التقرير النهائي

قطاع تنمية الاتصالات لجنة الدراسات 1

المسألة 1/1-22

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

فترة الدراسة الخامسة 2010-2014

قطاع تنمية الاتصالات

للاتصال بنا

الموقع الإلكتروني: www.itu.int/ITU-D/study_groups

المكتبة الإلكترونية للاتحاد: www.itu.int/pub/D-STG/

البريد الإلكتروني: devsg@itu.int

الهاتف: 5999 730 22 41+

المســـألة 1/1-22:

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

لجان دراسات قطاع تنمية الاتصالات

دعماً لجدول أعمال تقاسم المعارف وبناء القدرات لمكتب تنمية الاتصالات، تقوم لجان دراسات قطاع تنمية الاتصالات بدعم البلدان في تحقيق أهدافها الإنمائية. وعن طريق العمل كعامل حفز من خلال استحداث وتقاسم وتطبيق معارف تكنولوجيا المعلومات والاتصالات للحد من الفقر وتحقيق التنمية الاقتصادية والاجتماعية، تسهم لجان دراسات قطاع تنمية الاتصالات في تهيئة الظروف المؤاتية لكي تستخدم الدول الأعضاء المعارف لتحقيق أهدافها الإنمائية بشكل أفضل.

منصة المعارف

تستخدم النواتج التي يتفق عليها في لجان دراسات قطاع تنمية الاتصالات والمواد المرجعية ذات الصلة كمدخلات لتنفيذ السياسات والاستراتيجيات والمشاريع والمبادرات الخاصة في الدول الأعضاء في الاتحاد البالغة 193 دولة. وتعمل هذه الأنشطة أيضاً على تعزيز قاعدة المعارف المشتركة للأعضاء.

محور تبادل المعلومات وتقاسم المعارف

يجري تقاسم المعلومات بشأن المواضيع ذات الاهتمام المشترك من خلال اجتماعات وجهاً لوجه والمنتديات الإلكترونية والمشاركة عن بُعد في جو يشجع الحوار المفتوح وتبادل المعلومات.

مستودع المعلومات

تعد التقارير والمبادئ التوجيهية وأفضل الممارسات والتوصيات استناداً إلى المدخلات المقدمة من أعضاء اللجان لاستعراضها. وتجمع المعلومات عن طريق دراسات استقصائية ومساهمات ودراسات حالة وتتاح لإطلاع الأعضاء عليها بسهولة باستخدام أدوات إدارة المحتوى والنشر على الويب.

لجنة الدراسات 1

أسند إلى لجنة الدراسات 1 في الفترة 2010-2014 دراسة تسع مسائل في مجالات البيئة التمكينية والأمن السيبراني وتطبيقات تكنولوجيا المعلومات والاتصالات والقضايا المتصلة بالإنترنت. وركز العمل على السياسات والاستراتيجيات الوطنية للاتصالات التي تمكّن البلدان من الاستفادة إلى أقصى حد من القوة الدافعة للاتصالات/تكنولوجيا المعلومات والاتصالات بوصفها محركاً للنمو المستدام وخلق فرص العمل والتنمية الاقتصادية والاجتماعية والثقافية، مع مراعاة المسائل ذات الأولوية للبلدان النامية. وشمل العمل سياسات النفاذ إلى الاتصالات/تكنولوجيا المعلومات والاتصالات، لا سيما نفاذ الأشخاص ذوي الإعاقة وذوي الاحتياجات الخاصة، إضافة إلى أمن شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات. كما ركز أيضاً على سياسات ونماذج التعريفات لشبكات الجيل التالي ومسائل التقارب والنفاذ الشامل إلى خدمات النطاق العريض الثابتة والمتنقلة وتحليل الأثر وتطبيق مبادئ التكلفة والمحاسبة، مع مراعاة نتائج الدراسات التي يجريها قطاعا تقييس الاتصالات والاتصالات الراديوية، وأولويات البلدان النامية.

شارك في إعداد هذا التقرير عدة خبراء من إدارات وشركات مختلفة. ولا ينطوي ذكر شركات أو منتجات معينة على أي تأييد أو توصية من جانب الاتحاد الدولي الاتصالات.

© ITU 2014

جميع حقوق النشر محفوظة. لا يمكن استنساخ أي جزء من هذه المنشورة بأي شكل كان ولا بأي وسيلة إلا بإذن خطي من الاتحاد الدولي للاتصالات (ITU).

جدول المحتويات

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الأشكال

الجداول

المســـألة 22-1/1
تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

1 مقدمة إلى التقرير النهائي بشأن المسألة 22-1/1 المتعلقة بالأمن السيبراني

تعد لجنة الدراسات 1 لقطاع تنمية الاتصالات المعنية بالمسألة 22-1/1 تقارير عن أفضل الممارسات فيما يتعلق بمختلف جوانب الأمن السيبراني. وهذا هو التقرير النهائي للفريق المعني بالمسألة 22-1/1 لقطاع تنمية الاتصالات بشأن أنشطته على مدى دورة الدراسات الأخيرة التي امتدت أربع سنوات شملت الفترة 2010-2014. وكان المؤتمر العالمي لتنمية الاتصالات قد وضع في اجتماعه الذي عقد عام 2010 في حيدر آباد بالهند برنامج عمل المسألة 22/1. وعالج فريق المسألة 22-1/1 خلال السنوات الأربع الأخيرة جميع البنود التي تضمنها برنامج العمل ذلك، إما بشكل كامل أو جزئي.

ويتألف تقرير المسألة 22-1/1 النهائي هذا من عددٍ من تقارير أفضل الممارسات بشأن مختلف جوانب الأمن السيبراني. ومن بين ذلك (1) دليل إنشاء نظام لإدارة الأمن السيبراني الوطني؛ و(2) أفضل الممارسات لتكوين شراكات بين القطاعين العام والخاص دعماً لأهداف الأمن السيبراني وغاياته؛ و(3) بناء القدرة الوطنية على إدارة حوادث الأمن الحاسوبية؛ و(4) إدارة فريق وطني للاستجابة للحوادث الحاسوبية مع عوامل النجاح الحاسمة؛ و(5) أفضل الممارسات لحماية شبكات موردي خدمات الإنترنت. وعلاوةً على ذلك، يضم **الملحق هاء** بهذا التقرير مواد لدورات تدريب على بناء أفرقة الاستجابة للحوادث الحاسوبية وإدارتها. كما تلقت المسألة مساهمة تصف دراسة إضافية ودورة إلكترونية للأطفال من أكاديمية أوديسا الوطنية للاتصالات (n.a. A.S. Popov). كما تلقى الفريق كذلك تقارير من مكتب تنمية الاتصالات بشأن أنشطته على الصعيدين العالمي والإقليمي.

ويواصل الفريق المعني بالمسألة 22-1/1 العمل على عدد من التقارير الأخرى، منها على سبيل المثال تقرير عن أفضل الممارسات لمكافحة الرسائل الاقتحامية، وآخر بشأن استقصاء عن برامج التوعية التي تباشرها الدول الأعضاء وثالث يضم خلاصة وافية للتقارير التي أسهمت بها البلدان في المسألة 22-1/1 بشأن أنشطتها في مجال الأمن السيبراني. ومن المتوقع استكمال هذا العمل خلال دورة لجنة الدراسات التالية.

2 أفضل الممارسات المتعلقة بالأمن السيبراني – دليل إنشاء نظام لإدارة الأمن السيبراني الوطني

1.2 مقدمة

لإنشاء نظام لإدارة الأمن السيبراني الوطني أهمية تعجز الكلمات عن وصفها في عصر التقدم الرقمي هذا الذي تواجه البلدان فيه مخاطر ومواطن ضعف حقيقية في أنظمة معلومات حاسمة يمكن لجهات معادية استغلالها. وليس الفضاء السيبراني اليوم آمناً، بل هو بعيد عن ذلك، مما ينشئ حاجة ملحة إلى التحرك – على الصعيدين الوطني والدولي – لمجابهة جميع أنواع التهديدات السيبرانية. ومواجهة تحديات أمن الحواسيب هو دور الحكومات، التي يثقل كاهلها غياب هيكليات تنظيمية ومؤسسية ملائمة للتعامل مع الحوادث. ولذلك ينبغي أن تعمل القطاعات والوكالات الرائدة على تقييم موثوقية البنى التحتية ومواطن ضعفها وبيئات التهديدات من حولها ومن ثم إعمال تدابير واستجابات حمائية ملائمة لوقايتها. وقد سبق أن اقترح الاتحاد الدولي للاتصالات عملية متكاملة لوضع خطة للأمن السيبراني الوطني وتنفيذها. ويحدد هذا المقترح منهجية لتنفيذ خارطة طريق لإدارة الأمن السيبراني الوطني، مما يتضمن إطاراً لأفضل الممارسات ونموذج نضج لتقييم مختلف الجوانب ذات الصلة بالأمن السيبراني الوطني.

والمقصود من وثيقة "أفضل الممارسات للأمن السيبراني–دليل إنشاء نظام لإدارة الأمن السيبراني الوطني" هو عرض "نظام إدارة الأمن السيبراني الوطني"، وهو دليل تطوير للأمن السيبراني الوطني الفعال. وهو يكفل تنفيذ خارطة طريق وطنية لإدارة الأمن السيبراني من خلال المكونات الأربعة التالية:

"إطار الأمن السيبراني الوطني"، الذي يطرح 5 ميادين و34 عملية تغطي القضايا الرئيسية ذات الصلة بالأمن السيبراني على الصعيد الوطني، مثل معيار ISO 27002 بالنسبة إلى المؤسسات؛

1 "نموذج نضج الأمن السيبراني الوطني"، الذي يصنف عمليات "إطار الأمن السيبراني الوطني" حسب مستوى نضجها؛

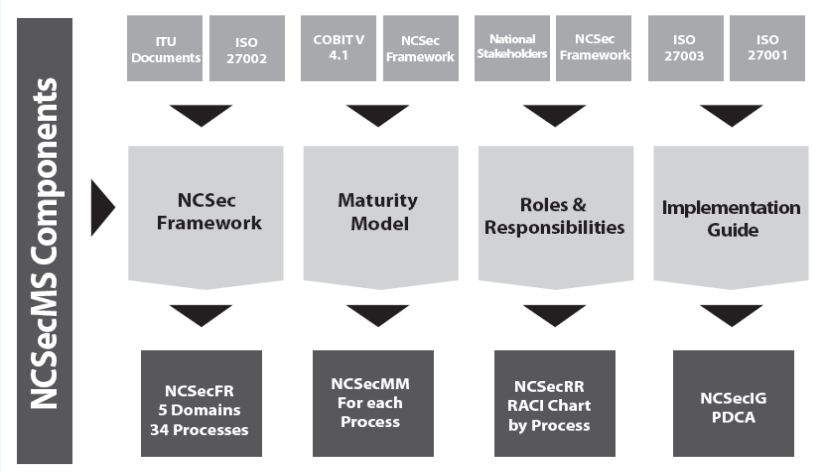
2 "مخطط الأدوار والمسؤوليات (RACI) للأمن السيبراني الوطني"، الذي يساعد في تحديد أدوار ومسؤوليات أصحاب المصلحة الرئيسيين المعنيين بالأمن السيبراني في بلدٍ ما أو منطقة ما؛

3 "دليل تنفيذ الأمن السيبراني الوطني"، وهو عبارة عن تعميم للمعيارين ISO 27001 وISO 27003 على الصعيد الوطني. وهو يبرز أفضل الممارسات التي يمكن للمؤسسات استخدامها لقياس وضع التأهب عندها.

2.2 نظام إدارة الأمن السيبراني الوطني

يمكن اعتبار نظام إدارة الأمن السيبراني الوطني أداة الهدف منها تسهيل تحقيق الأمن السيبراني الوطني على الصعيدين الوطني والإقليمي. وهو يتكون من أربع خطوات تضم المكونات التالية:

الشكل 1: نظام إدارة الأمن السيبراني الوطني



الخطوة 1: إطار الأمن السيبراني الوطني

يمثل مقترح أفضل الممارسات للأمن السيبراني الوطني إطاراً شاملاً يلبي الاحتياجات التي أعرب عنها الاتحاد الدولي للاتصالات في جدول الأعمال العالمي للأمن السيبراني الذي وضعه. وهذا الإطار مستوحى بالكامل من المعيار ISO 27002،[1] وهو مدونة ممارسة للهيكليات والسياسات التنظيمية المتعلقة بالأمن السيبراني على الصعيد الوطني، ويتألف من خمسة ميادين و34 عملية ويستهدف المساعدة في بناء التعاون الإقليمي والدولي للمراقبة والإنذار والاستجابة للحوادث.

[1] للحصول على مزيدٍ من المعلومات عن المعيار ISO 27002، انظر الملحق 1 بوثيقة المغرب 1/45.

الخطوة 2: نموذج نضج الأمن السيبراني الوطني

سيتيح نموذج نضج الأمن السيبراني الوطني تقييم الأمن في بلد أو إقليم كامل وبالتالي إجراء مقارنات بينها وبيان ما فيها من قوى وتهديدات. كما سيسهل تحديد مستوى النضج في بلدٍ ما، وبالتالي وضع هدف للنضج والتخطيط لتحسين مستوى النضج. وطالما كان هناك إطار وطني شامل محدد للأمن السيبراني، فإن نموذج نضج الأمن السيبراني الوطني يقترن بمقترح أفضل الممارسات للأمن السيبراني الوطني هذا، وهو المسمى إطار الأمن السيبراني الوطني. وهو مستوحى من نموذج نضج Cobit، وسيفرض تنفيذ نظام إدارة الأمن السيبراني الوطني، مظهراً بذلك ما يجب عمله لتحسين كل عملية على الصعيدين الوطني والإقليمي.

الخطوة 3: أدوار ومسؤوليات الأمن السيبراني الوطني

يمثل تخطيط المسؤوليات أسلوباً للوقوف على المجالات الوظيفية التي تضم عمليات يكتنفها الإبهام وإظهار الاختلافات وحلها من خلال عمل تعاوني عبر الوظائف. ويحدد "مخطط RACI الوطني" المقدَم من هو "مسؤول" أو "مساءل" أو "مستشار" أو "محاط علماً" من بين أصحاب المصلحة لكلٍ من عمليات الأمن السيبراني الوطني الأربع وثلاثين. ويحدد "مخطط RACI" بالتفصيل ما الذي يجب تفويض الغير فيه ومن يكون المفوض، وما هي نوعية المسؤولية التي ستناط بأحد أصحاب المصلحة دون غيره.

الخطوة 4: دليل تنفيذ الأمن السيبراني الوطني

يتيح دليل التنفيذ المقترن بالأمن السيبراني الوطني آلية تحكم عمليات فعالة لضمان حسن فهم التفاعل بين هذه العمليات، وذلك باستخدام نهجي ISO 27001 وISO 27003.[2]

نهج الحل

اعتُمد نهج الحل، الذي يراعي توجهات وقائع الاتحاد الدولي للاتصالات وأهدافها المستقرة بالفعل، لكلٍ من الخطوات الأربع المذكورة أعلاه من أجل التوصل إلى أهداف الاتحاد المناظرة، والتي تتمثل في وضع استراتيجيات لتكوين هيكليات وسياسات تنظيمية ملائمة بشأن الأمن السيبراني على الصعيدين الوطني والإقليمي ووضع استراتيجيات لإنشاء إطار شامل للمراقبة والإنذار والاستجابة في الحوادث.

- **بناء إطار للأمن السيبراني الوطني *(NCSecFR)***

انصب التركيز خلال هذه الخطوة على وثائق الاتحاد الدولي للاتصالات الموجودة والنهج القائم على عملية ISO 27002: لقد حاولنا تكييف نهج ISO 27002 حتى نتمكن من حسم أمر العمليات الرئيسية التي يستلزمها الأمن السيبراني الوطني ونعد إطار الأمن السيبراني الوطني. وبما أن ISO 27002 هو المعيار الدولي لأنظمة معلومات المؤسسات، فإن إطار الأمن السيبراني الوطني المقترح عبارة عن تعميم لهذا المعيار.

- ***نموذج نضج الأمن السيبراني الوطني (NCSecMM)***

إطار الأمن السيبراني الوطني (الخطوة 1) غير كافٍ، بل يجب إلحاق نموذج نضج به من أجل فرض تنفيذ إدارة الأمن السيبراني الوطني ومن ثم بيان ما يجب عمله في سبيل التحسين.

- ***نموذج الأدوار والمسؤوليات (NCSecRR)***

تُحدَد في هذه الخطوة المجالات الوظيفية التي تضم عمليات يكتنفها الإبهام وإظهار الاختلافات وحلها من خلال عمل تعاوني عبر الوظائف. ومن بالغ الأهمية أن يحدَد بالتفصيل ما الذي يجب تفويض الغير فيه ومن يكون المفوض، وما هي نوعية المسؤولية

[2] للحصول على مزيدٍ من المعلومات عن المعيارين ISO 27002 وISO 27003، انظر الملحق 1 (المغرب 1/45).

التي ستناط بأحد أصحاب المصلحة دون غيره. وهذا يعين المؤسسات والأفرقة على تحديد المسؤولية عن عناصر محددة على الصعيد الوطني وعلى صعيد عمليات إطار الأمن السيبراني الوطني.

- ***دليل التنفيذ (NCSecIG)***

من أولى الأولويات هيكلة كل وجه من أوجه إطار الأمن السيبراني الوطني. ومن المهم توفير تحكم عمليات فعال لضمان حسن فهم التفاعل بين هذه العمليات. وسيتيح دليل التنفيذ هيكلة كلٍ من العمليات باستخدام نهجي ISO 27003 وISO 27001: وسيوفر ISO 27003 مساعدة وتوجيهاً في تنفيذ نظام إدارة أمن معلومات، بما في ذلك التركيز على طريقة PDCA (التخطيط – التنفيذ – المراجعة – التحرك) فيما يتعلق بإنشاء النظام ومراجعته وتحسينه. وسيُستخدم ISO 27001، من خلال نموذج PDCA، لهيكلة كل عملية، بل ولهيكلة نموذج النضج نفسه. وسيُستخدم نهج PDCA تلقائياً ضمن عملية تنفيذ إطار الأمن السيبراني الوطني ونموذج النضج بأكملها.

3.2 إطار الأمن السيبراني الوطني

كيفية تلبية إطار الأمن السيبراني الوطني للاحتياجات

تنبني إدارة الأمن السيبراني أساساً على **إطار وطني** قادر على معالجة قضايا التهديدات السيبرانية والسيطرة عليها على صعيد وطني. كما ينبغي أن تكون مزودة بالقدرة، في الفضاء السيبراني غير المحدود، على إتاحة التعاون اللازم على صعيد إقليمي ودولي من أجل تحقيق أهدافها.

وقد يرتكز إطار نظام إدارة الأمن السيبراني الوطني بشكل أساسي على ما يلي:[3]

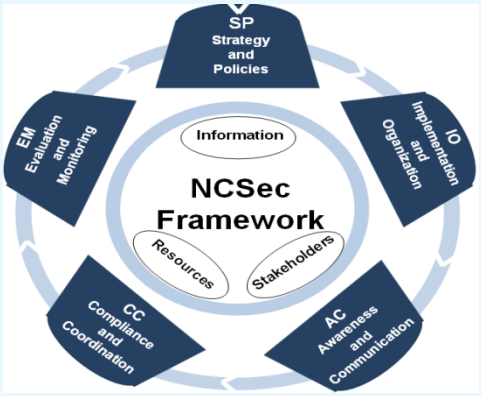
- الأساس القانوني الوطني؛
- تدابير تقنية؛
- هيكليات تنظيمية؛
- بناء القدرات؛
- التعاون الدولي.

وهذه العناصر متسقة مع الأهداف العامة لجدول الأعمال العالمي للأمن السيبراني وأركانه (أو مجالات عمله) الاستراتيجية الخمسة. وينبغي تنظيم الإطار المقترح بحيث يحقق أهداف مبادرة جدول الأعمال العالمي للأمن السيبراني كي يعالج التحديات العالمية ذات الصلة بمجالات العمل الخمسة.

[3] للحصول على مزيدٍ من المعلومات عن كلٍ من هذه العناصر الخمسة، انظر الملحق 1 (المغرب 1/45).

إطار الأمن السيبراني الوطني

الشكل 2: نموذج إطار الأمن السيبراني الوطني



إطار الأمن السيبراني الوطني: خمسة ميادين[4]

يتألف إطار الأمن السيبراني الوطني من 34 عملية مقسمة على خمسة ميادين.[5]

الميدان 1: الاستراتيجية والسياسات (SP)

يتناول هذا الميدان في العادة الأسئلة التالية:

- هل استراتيجية الأمن السيبراني الوطني محددة؟
- هل تضع الحكومة سياسات فعالة للأمن السيبراني الوطني؟
- هل فهم كلٌ من أصحاب المصلحة أهداف الأمن السيبراني الوطني؟
- ما مدى فهم عمليات إدارة المخاطر ودمجها في الإطار الشامل، خاصة بالنسبة إلى حماية البنى التحتية الحاسمة للمعلومات؟
- هل درجة تأهب كلٍ من أصحاب المصلحة على صعيد الأمن ملائمة لتنفيذ استراتيجية الأمن السيبراني الوطني؟

الميدان 2: التنفيذ والتنظيم (IO)

يتناول هذا الميدان في العادة أسئلة الإدارة التالية:

- هل سيحقق أصحاب المصلحة أهداف الأمن السيبراني الوطني بشكل سليم وقت تطبيق استراتيجية الأمن السيبراني الوطني؟
- هل تنفذ خدمات الأمن السيبراني الوطني بشكل يتسق مع استراتيجية الأمن السيبراني الوطني بالنسبة إلى كلٍ من القطاعات/أصحاب المصلحة؟
- هل بلغت تكاليف الأمن السيبراني الوطني الحد الأمثل؟
- هل يتمتع أصحاب المصلحة بالقدرة على استعمال الأنظمة السيبرانية بشكل إنتاجي وآمن؟
- هل يرجح أن ينفذ أصحاب المصلحة الجدد خدمات تتماشى مع استراتيجية الأمن السيبراني الوطني؟
- هل يرجح تطبيق أصحاب المصلحة الجدد لسياسات الأمن السيبراني الوطني في وقتها وضمن الميزانية المحددة لها؟

---

[4] للحصول على مزيدٍ من المعلومات عن الميادين الخمسة، انظر الملحق 1 (المغرب 1/45).

[5] للحصول على مزيدٍ من المعلومات بشأن هذه العمليات الأربع وثلاثين، انظر الملحق 1 (المغرب 1/45).

الميدان 3: الوعي والاتصال (AC)

يتناول هذا الميدان في العادة أسئلة الإدارة التالية:

- هل لدى قادة الحكومة على الصعيد الوطني قناعة بالحاجة إلى التحرك الوطني لمعالجة التهديدات ومواطن الضعف؟
- هل يوجد برنامج توعية شامل يروج له على الصعيد الوطني حتى يؤمِّن جميع المشاركين – الشركات والقوة العاملة العامة وعموم الجماهير – ما تحت يد كلٍ منهم من الفضاء السيبراني؟
- كيف تنفذ برامج ومبادرات التوعية والتواصل المتعلقة بالأمن لجميع أصحاب المصلحة؟
- هل يوجد أي دعم للمجتمع المدني مع إيلاء احتياجات الأطفال والمستخدمين الأفراد انتباهاً خاصاً؟

الميدان 4: الامتثال والتنسيق (CC)

يتناول هذا الميدان في العادة أسئلة الإدارة التالية:

- هل تكفل الهيكليات التنظيمية فعالية الضوابط وكفاءتها؟
- هل تراعَى ضوابط المخاطر والامتثال ويبلغ بها؟
- هل تنطوي مكونات الإطار على قدرٍ وافٍ من السرية والنزاهة والإتاحة؟

الميدان 5: التقييم والرصد (EM)

يتناول هذا الميدان في العادة أسئلة الإدارة التالية:

- هل يقاس أداء الأمن السيبراني الوطني لاكتشاف المشاكل في وقت مناسب؟
- هل يمكن ربط أداء الأمن السيبراني الوطني بالأهداف الاستراتيجية لإطار الأمن السيبراني الوطني الشامل؟
- هل تقاس المخاطر والضوابط والامتثال والأداء ويبلغ بها؟

والمكونات الرئيسية لإطار الأمن السيبراني الوطني هي كالتالي:[6]

- أهداف ضبط/مجالات تركيز إدارة الأمن السيبراني الوطني؛
- الموارد/الهيكليات التنظيمية للأمن السيبراني الوطني؛
- أصحاب المصلحة في الأمن السيبراني الوطني؛
- معلومات الأمن السيبراني الوطني، استناداً إلى تصنيف التهديدات التراتبي.[7]

نموذج نضج الأمن السيبراني الوطني

▪نموذج نضج إطار COBIT (المصدر: ISACA – ITGI)[8]

يتعين تطوير إطار للأمن الوطني السيبراني للتحسين من أجل الوصول إلى مستوىً ملائم من الإدارة والضبط. ويحقق هذا النهج التوازن بين التكاليف والفوائد على الأمد الطويل على نحو يعالج الأسئلة التالية:

- ماذا يفعل أقراننا في الصناعة، وأين مكانتنا بالنسبة إليهم؟
- ما هي الممارسات الجيدة المقبولة في الصناعة، وأين موضعنا فيما يتعلق بتلك الممارسات؟
- استناداً إلى هاتين المقارنتين، هل يمكن القول بأن ما نفعله كافٍ؟

---

[6] للحصول على مزيدٍ من المعلومات عن المكونات الرئيسية لإطار الأمن السيبراني الوطني، انظر الملحق 1 (المغرب 1/45).

[7] انظر الملحق 1 (المغرب 1/45) للاطلاع على معايير معلومات الأمن السيبراني الوطني.

[8] للحصول على مزيدٍ من المعلومات عن نموذج نضج إطار COBIT، انظر الملحق 1 (المغرب 1/45).

- كيف نتبين ما يتعين عمله للوصول إلى مستوىً كافٍ من الإدارة والضبط لعملياتنا في مجال تكنولوجيا المعلومات؟

وقد يكون من الصعب تقديم أجوبة شافية عن هذه الأسئلة. ولا يكف القائمون على إدارة تكنولوجيا المعلومات عن تلمس أدوات للقياس المرجعي والتقييم الذاتي تلبيةً للحاجة إلى معرفة ما ينبغي عمله بشكل فعال. وابتداءً من عمليات COBIT، يفترض أن يتمكن المسؤول عن العملية من القياس المرجعي بتدرج مقابل ذلك الهدف الضابط. وهذا يلبي ثلاثة احتياجات:

- قياس نسبي لموضع المؤسسة
- أسلوب لاتخاذ قرار بشكل فعال بشأن التوجه
- أداة لقياس التقدم مقابل نمذجة نضج الأهداف لإدارة عمليات تكنولوجيا المعلومات وضبطها تستند إلى طريقة لتقييم المؤسسة، بحيث يمكن تصنيفها من مستوى نضج غير قائم (صفر) إلى الحد الأمثل (5).

وفي COBIT، يوجد تعريف عام لمقياس نضج COBIT، وهو يشبه CMM إلا أنه مكيَّف على طبيعة عمليات إدارة تكنولوجيا المعلومات في COBIT. ويوجد نموذج محدد مستقى من هذا المقياس العام لكلٍ من عمليات COBIT الأربع وثلاثين. وأياً كان المقياس، ينبغي ألا تكون المقاييس مفرطة في التفصيل، حيث إن من شأن ذلك أن يجعل النظام صعب الاستخدام ويطرح درجة من الدقة غير مبررة لأن الغرض، بشكل عام، هو تبين مواضع الإشكاليات وكيفية تحديد أولويات التحسين. وليس الغرض مستوى التقيد بأهداف الضبط.

ويمكن من خلال استخدام نماذج النضج المطورة لكلٍ من عمليات تكنولوجيا المعلومات الأربع وثلاثين في COBIT أن تتبين الإدارة:

- الأداء الفعلي للمؤسسة – موضع المؤسسة اليوم
- وضع الصناعة الحالي – المقارنة
- هدف المؤسسة للتحسين – أين تريد المؤسسة أن تكون؟
- مسار النمو اللازم بين "كما هي" و"منشود"

ولجعل النتائج سهلة الاستعمال في جلسات إحاطة الإدارة، حيث تُعرض كوسيلة لتأييد منطق الأعمال للخطط المستقبلية، يجب توفير طريقة للعرض الرسومي[9].

وقد طُور إطار COBIT من أجل إدارة عمليات تكنولوجيا المعلومات مع التركيز بقوة على الضبط. ويجب أن تكون هذه المقاييس عملية في تطبيقها وسهلة الفهم إلى حدٍ معقول. وبما أن موضوع إدارة عمليات تكنولوجيا المعلومات ينطوي على قدر من التعقيد والذاتية، فإن أفضل مقاربة له تكون من خلال التقييمات الميسرة التي ترفع الوعي وتحظى بتوافق واسع النطاق وتحفز على التحسين. ويمكن تنفيذ هذه التقييمات إما مقابل توصيفات مستويات النضج بشكل كلي أو بمزيدٍ من التمحيص مقابل كلٍ من البيانات المستقلة للتوصيفات. وفي أيٍ من الحالتين، يتطلب الأمر خبرة في عملية المؤسسة الخاضعة للاستعراض.

وتكمن ميزة نهج نموذج النضج فيما يتيحه من سهولة وضع الإدارة نفسها على المقياس وتقديرها للعوامل المعنية إذا ظهرت حاجة إلى تحسين الأداء. ويتضمن المقياس درجة الصفر لأنه من الوارد جداً ألا توجد عملية أصلاً. ويستند المقياس 0-5 إلى مقياس نضج بسيط يبين كيفية تطور عمليةٍ ما من قدرة منعدمة إلى قدرة مثلى.

غير أن قدرة إدارة العمليات ليست مثل أداء العمليات. وربما لا يلزم تطبيق القدرة المطلوبة، على النحو الذي تحدده أهداف الأعمال وتكنولوجيا المعلومات، على نفس المستوى عبر بيئة تكنولوجيا المعلومات بأكملها، على سبيل المثال بشكل غير متسق أو على عدد محدود فقط من الأنظمة أو الوحدات. ويمثل قياس الأداء، كما تتناوله الفقرات التالية، ضرورة في سبيل الوقوف على الأداء الفعلي للمؤسسة بالنسبة إلى عمليات تكنولوجيا المعلومات فيها. والقدرة التي تطبق بشكل سليم تؤدي بالفعل إلى خفض المخاطر، ومع ذلك فلا غنى عن تقييم المؤسسة للضوابط اللازمة لضمان التخفيف من المخاطر واكتساب القيمة بما يتماشى مع مستوى الرغبة في المخاطرة وأهداف الأعمال. وتتوجه هذه الضوابط حسب أهداف ضبط COBIT. ويمثل نموذج

[9] انظر الشكل 2.1 في الملحق 1 (المغرب 1/45) للاطلاع على التفاصيل.

النضج أسلوباً لقياس مدى تطوير عمليات الإدارة، أي مدى قدراتها الفعلية. ويعتمد مدى التطوير أو القدرة التي ينبغي أن تكون عليه على أهداف تكنولوجيا المعلومات واحتياجات الأعمال الأساسية التي تدعمها. كما يعتمد إلى حد بعيد مدى تطبيق تلك القدرة فعلياً على العائد التي ترغب المؤسسة في تحقيقه من الاستثمار.

ويمكن التماس نقطة مرجعية استراتيجية من أجل تحسين مؤسسةٍ ما إدارة عمليات تكنولوجيا المعلومات وضبطها عن طريق النظر في المعايير الدولية الناشئة وأفضل الممارسات في فئتها. وقد تمثل ممارسات اليوم الناشئة مستوى الأداء المتوقع للغد، مما يجعلها مفيدة للتخطيط لتحقيق المكانة التي تريد المؤسسة بلوغها على المدى الزمني. وتُبنى نماذج النضج تصاعدياً بداية من النموذج النوعي العام[10] الذي يضاف إليه مبادئ من السمات التالية على نحو متزايد عبر المستويات:

- الوعي والاتصال
- السياسات والخطط والإجراءات
- الأدوات والأتمتة
- المهارات والخبرات
- المسؤولية والمساءلة
- وضع الأهداف والقياس

نهج الحل

ينطوي نموذج نضج الأمن السيبراني الوطني على ربط استراتيجية الأمن السيبراني الوطني بالأهداف الوطنية الاستراتيجية، وتوفير قياسات ومستويات لنموذج النضج من أجل قياس مدى تحققها ولتبين ما يقترن بذلك من مسؤوليات أصحاب المصلحة وعملية هدف الضبط. وهذا النهج مشتق من نموذج النضج الذي وضعه معهد هندسة البرمجيات لنضج قدرة تطوير البرمجيات.

ويسمح نموذج نضج الأمن السيبراني الوطني المقترح بتحديد مدى النضج في بلدٍ ما وبالتالي تحديد نضج مستهدف والتخطيط لتحسين مستوى النضج.

وهو يضم المستويات التالية:

- 0. منعدم
- 1. مبدئي
- 2. قابل للتكرار لكنه بديهي
- 3. محدد
- 4. خاضع للإدارة وقابل للقياس
- 5. أمثل

نموذج النضج حسب العملية

لكل من العمليات الخمس شروط يجب استيفاؤها لتحقيق أحد مستويات النضج الخمسة.[11]

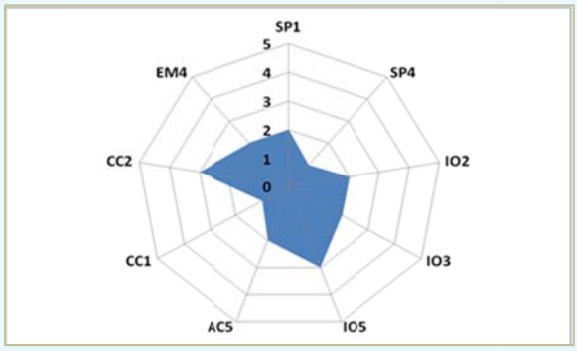
[10] انظر الشكل 3.1 في الملحق 1 (المغرب 1/45) للاطلاع على التفاصيل.

[11] انظر "3.3 نموذج النضج حسب العملية"، الملحق 1 (المغرب 1/45) للاطلاع على الشروط.

التقييم القُطري

لتقييم مستوى نضج بلدٍ ما بالنسبة إلى استراتيجيتها للأمن السيبراني الوطني، نقترح الاحتفاظ بعشر عمليات أساسية من أجل إجراء جرد في أي وقت معين، على النحو المبين في شكل "الرادار" أدناه، والذي يقارن بين بلدان مختلفة ويقيِّم تطور بلدٍ ما بين تاريخين.

الشكل 3: رادار لتقييم مستويات النضج



أدوار ومسؤوليات الأمن السيبراني الوطني

ينبغي ضمن الحاجة العامة لإرساء إدارة الأمن السيبراني الوطني إقران مخطط RACI بإطار عام. وقد سبق استعمال هذا النهج في COBIT وأثبت فعاليته (معهد إدارة تكنولوجيا المعلومات 2005).

4.2 مصفوفة RACI

يجب اتباع نهج فعال لتبين المجالات الوظيفية التي يكتنفها الإبهام من حيث المسؤوليات وإظهار الاختلافات وحلها من خلال عمل تعاوني عبر الوظائف. ويتيح تخطيط المسؤوليات للمديرين على مستويات تنظيمية أو في برامج واحدة أو مختلفة المشاركة بفعالية في مناقشات مركزة ومنهجية حول توصيفات الإجراءات ذات الصلة بالعمليات. ويجب إنجاز هذه الإجراءات في سبيل إخراج المنتج أو الخدمة في الصورة النهائية بنجاح. إلا أنه لا توجد نماذج "تخطيط مسؤوليات" مخصصة للأمن السيبراني الوطني.

وتخطيط المسؤوليات عملية تتكون من خمس خطوات (سميث وإيروين 2005): أولاً، يجب أن نحدد العمليات.[12] وثانياً ينبغي تحديد أصحاب المصلحة والموارد والمعلومات المفيدة للتخطيط. ومن ثم يمكن تطوير مخطط RACI عن طريق استيفاء خلايا المخطط. وينبغي بعد ذلك حل أي تداخلات. وأخيراً، ينبغي حل أي فجوات كذلك. وسنتبع هذه المنهجية من أجل تكوين جدول مخطط RACI وإعداده.

نهج مخطط RACI

نموذج RACI أداة بسيطة نسبياً تستعمل لتوضيح الأدوار والمسؤوليات والصلاحيات بين أصحاب المصلحة المعنيين بإدارة عمليات أو أدائها، خاصة خلال عمليات التغيير التنظيمي. ومن المفيد وصف ما ينبغي عمله ومن المسؤول عن عمله في سبيل إحداث عملية تحويل (كيلي 2006).

ومخطط RACI عبارة عن جدول يصف أدوار مختلف أصحاب المصلحة ومسؤولياتهم في مباشرة عمليةٍ ما. وضمن سياق إطار الأمن السيبراني الوطني، يوضح "مخطط RACI" أدوار مختلف أصحاب المصلحة ومسؤولياتهم على الصعيد الوطني. وهو يلحِق

[12] انظر "مصفوفة RACI حسب العملية"، الملحق 1 (المغرب 1/45).

بقائمة أصحاب المصلحة معلومات حول الأدوار التي يضطلعون بها بالنسبة إلى كل عملية من عمليات إطار الأمن السيبراني الوطني الأربع وثلاثين.

ويُلحق لكل عملية حرف واحد أو أكثر من حروف الاختصار "RACI" بكل صاحب مصلحة حسب أدواره ومسؤوليته. ويمثل هذا الاختصار ما يلي:

- مسؤول (R): من يبذل جهداً لإنجاز العملية، بما في ذلك الدعم، وهو توفير الموارد لاستكمال المهمة في تنفيذها.
- مساءل (A): من يساءلون في نهاية المطاف عن استكمال المهمة بشكل صحيح. وهذا يمثل صلاحية الموافقة النهائية. ويجب أن يصدر عن حامل صلاحية المساءلة موافقة على العمل الذي يقدمه حامل صلاحية المسؤولية قبل إجازته. ويجب ألا يكون هناك أكثر من مساءل واحد محدد لكل عملية.
- مستشار (C): من تلتمس آراؤهم في تواصل ثنائي الاتجاه. وهذا يمثل صلاحية من يطلب منه إبداء الرأي وعنده معلومات و/أو قدرات لازمة لاستكمال العمل.
- محاط علماً (I): من يحاطون علماً بمستجدات التقدم المحرز في تواصل أحادي الاتجاه. وهذا يمثل صلاحية من يجب إعلامه عن العمل وإخطاره بالنتائج دون أن تلزم استشارته.

وكثيراً ما يناط بصاحب دور "المساءلة" دور "المسؤولية" كذلك، إلا أنه يوصى بشكل عام ألا يسند لصاحب أي دور أكثر من نوع واحد من أنواع أدوار التشارك لكل عملية. وإذا ظهرت أنواع تشارك مزدوجة في مخطط RACI فإن ذلك يعني أن الأدوار لم تحلل على الحقيقة بعد. ويلزم عندئذٍ توضيح كل دور على كل مهمة.

منهجية RACI للأمن السيبراني الوطني

لن تختلف المنهجية المختارة في حالة مخطط RACI للأمن السيبراني الوطني كثيراً عن المنهجية التقليدية. وهي تنطوي على استيفاء خلايا المخطط بعد تحديد من يحمل كل من الأدوار الأربعة المذكورة بالنسبة إلى كل عملية. ويفضل كمبدأ عام ألا يكون لأي عملية أكثر من مسؤول واحد، وإلا فإن فجوة تنشأ عندما توجد عملية لا مسؤول لها، بينما ينشأ تداخل في حالة حمل أصحاب مصلحة متعددون مسؤولية عمليةٍ ما.

ونبدأ بدور المساءل. والمبادئ التوجيهية لتعيين الأدوار هي كالتالي:

- تعيين نقطة (دور موقع) مساءلة (A) واحدة لكل عملية؛
- تخصيص المسؤولية (R) على المستوى الأقرب للإجراء أو المعرفة اللازمة للمهمة والتحقق من ملاءمة أي مسؤوليات متقاسمة؛
- التكفل باستشارة (C) أصحاب المصلحة الملائمين وإحاطتهم علماً (I)، لكن مع تقييد هذين الدورين ضمن حدود المباشَرة الضرورية فقط.

5.2 دليل تنفيذ الأمن السيبراني الوطني

الغرض من دليل التنفيذ هو مساعدة أي من/جميع أصحاب المصلحة في الأمن السيبراني الوطني على تطبيق نظام تتبع يتماشى مع إطار الأمن السيبراني الوطني ونموذج نضج الأمن السيبراني الوطني وتخطيط مسؤوليات الأمن السيبراني الوطني.

وسيستخدم دليل التنفيذ هذا أي من/جميع أصحاب المصلحة من إطار الأمن السيبراني الوطني الذين يريدون تطبيق نظام تتبع إدارة الأمن السيبراني الوطني، ومن أمثلة ذلك الحكومة والقطاع الخاص والبنية التحتية الحاسمة والهيئات الأكاديمية والمجتمع المدني.

ويمثل أي من أفراد أصحاب المصلحة المذكورين آنفاً متلقياً مستهدفاً لهذا المبدأ التوجيهي. وعلاوةً على ذلك، يمكن للدول الأعضاء في الاتحاد الدولي للاتصالات استعمال دليل التنفيذ هذا دعماً لجهود التنفيذ التي يبذلها أصحاب المصلحة المحليين، وذلك ضمن عملية تقييم ذاتي.

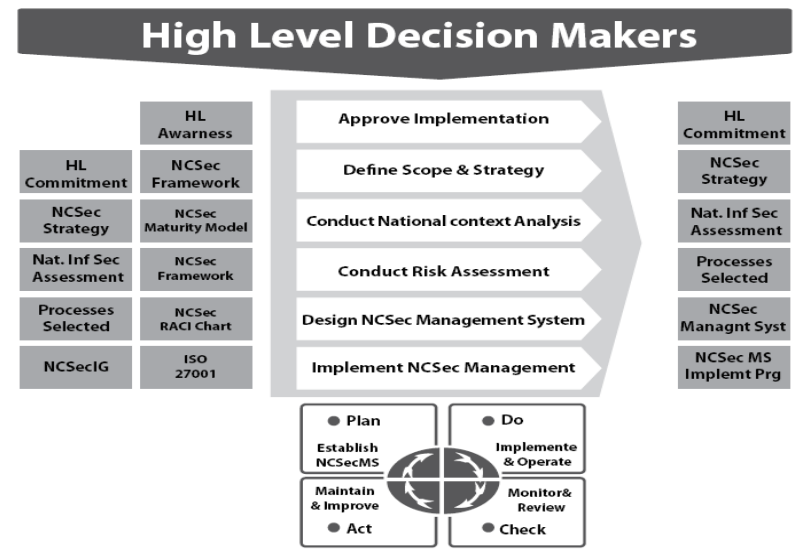
الخطوات الرئيسية

يتكون دليل التنفيذ من ست خطوات أساسية تستند جميعها إلى نهج PDCA:

الشكل 4: خطوات دليل التنفيذ

نهج الحل

الشكل 5: نهج الحل لدليل تنفيذ مشروع الأمن السيبراني الوطني



6.2 دليل التنفيذ

- **الموافقة على التنفيذ**

أ – استعراض للموافقة على للتنفيذ

ب – تحديد الأهداف والمتطلبات الوطنية للأمن السيبراني

ج – تحديد النطاق المبدئي لإدارة الأمن السيبراني الوطني

د – الحصول على موافقة صانع قرار رفيع المستوى

- **تعريف النطاق والاستراتيجية**

أ – استعراض بشأن تحديد نظام إدارة الأمن السيبراني الوطني واستراتيجيته

ب – تعيين حدود الفضاء الأمن السيبراني الوطني

ج – استكمال الحدود لنطاق نظام إدارة الأمن السيبراني الوطني

د – وضع استراتيجية الأمن السيبراني الوطني

- **إجراء تحليل السياق الوطني**

أ – استعراض بشأن إجراء تحليل السياق الوطني

ب – تحديد متطلبات أمن المعلومات

ج – تحديد حماية البنية التحتية الحاسمة للمعلومات

د – إنشاء تقييم لأمن المعلومات الوطني

- **تصميم نظام إدارة الأمن السيبراني الوطني**

أ – استعراض بشأن تصميم نظام إدارة الأمن السيبراني الوطني

ب – تحديد الهيكليات التنظيمية

ج – تصميم الرصد والقياس

د – إخراج برنامج تنفيذ نظام إدارة الأمن السيبراني

- **تنفيذ نظام إدارة الأمن السيبراني الوطني**

أ – استعراض بشأن تنفيذ نظام إدارة الأمن السيبراني الوطني

ب – إعداد نظام إدارة التنفيذ

ج – مباشرة مشروعات التنفيذ

د – توثيق الإجراءات والضوابط

7.2 الخلاصة

يمكن استعمال نظام إدارة الأمن السيبراني الوطني المذكورة أعلاه، القابل للتطبيق على إدارة الأمن السيبراني على الصعيدين الوطني والإقليمي، في أي بلد أو إقليم بأكمله للوقوف على مدى إتقان إدارة الأمن السيبراني من خلال التقييم الذاتي المستند إلى نموذج نضج محدد بشكل جيد. ومن شأن إطار إدارة الأمن السيبراني الوطني أن يسمح للبلدان والأقاليم بالوصول إلى مستويات ملائمة من الإدارة والضبط من خلال التحسين المستمر، مع مراعاة فوائد التكاليف لأهداف الأمد القصير والطويل.

3 الفصل الثالث: الشراكات بين القطاعين العام والخاص دعماً لأهداف الأمن السيبراني وغاياته

1.3 مقدمة

يتناول هذا التقرير الذي يدور حول أفضل الممارسات فعالية الشراكات بين القطاعين العام والخاص في معالجة مجموعة التحديات المعقدة المقترنة بأمن البنية التحتية المعلوماتية الحاسمة وإدارة مخاطرها.

وتتسم مهمة إدارة المخاطر التي تحيق بالبنية التحتية الحاسمة بتعقيد هائل، إلا أن لها أهمية حيوية كذلك. فمن شأن انتهاك البنية التحتية الحاسمة أو استغلالها بشكل ضار أن يكون له عواقب وخيمة على الصعيد المحلي أو الإقليمي بل والعالمي. وقد

ازدادت بشكل متوالٍ جسامة مخاطر الأمن السيبراني المتعلقة بالبنية التحتية المعلوماتية الحاسمة مع تزايد اعتماد البلدان والصناعات والأشخاص على أنظمة المعلومات وشبكاتها لدعم الوظائف المعتادة المتعلقة بعموم البنية التحتية الحاسمة. فإن تركت المخاطر المهددة لأنظمة وشبكات المعلومات هذه على حدتها، استتبعت عواقب وخيمة محتملة على الأمن القومي والحيوية الاقتصادية والرفاهة الاجتماعية.

وتمثل إدارة المخاطر المحيقة بالبنية التحتية الحاسمة على صعيد وطني أو عالمي تحدياً مستعصياً للحكومات، خاصة ما تعلق منها بالأمن السيبراني، الذي ينطوي على تحديات أمنية متعلقة بالبنية تحتية المادية والمنطقية. ففي المقام الأول، البنية التحتية الحاسمة موجودة في كل مكان، وبها العديد من نقاط ضعف ومداخل الخطر. ثم إن التهديدات المحيقة بالبنية التحتية لا حصر لها، حيث تمثل الهجمات الإجرامية أو الإرهابية المتعمدة والأخطار الطبيعية والحوادث وعلاقات الاعتماد ضمن البنية التحتية وحالات الانقطاع في سلاسل الإمداد وتهديدات أخرى عديدة سبباً وجيهاً للقلق. كما أن من شأن العواقب المباشرة وغير المباشرة أن تجمع بين أثر تدميري وصعوبة في التقدير والتوقع بدقة. ويضاف إلى ذلك أن تحديد حجم المخاطر وأولويات جهود إدارتها وتوزيع الموارد المحدودة قد يمثل تحدياً مفزعاً ومعقداً، خاصة على النطاق الواسع (على صعيد إقليمي أو وطني أو عالمي). وعلى جانب آخر، يسير التواصل البيني في عالمنا على مسار تزايدي متوالٍ، ومن الوارد أن تتجاوز المخاطر المحيقة بالبنية التحتية الحدودَ الجغرافية والولايات القضائية. ولهذا الاعتبار الأخير أهمية خاصةً في مجال البنية التحتية المعلوماتية الحاسمة، حيث يحتمل إطلاق الهجمات السيبرانية من أي مكان تقريباً وبشكل معضل للتحريات الجنائية. وأخيراً، فبينما كانت المسؤولية عن الأمن القومي تقع تقليدياً على كاهل الحكومة، فإن القطاع الخاص يستحوذ على قدر عظيم من ملكية البنية التحتية وإدارتها.

ولا تقف هذه الشواغل وغيرها عند حد اقتضاء حلول مبتكرة لإدارة المخاطر، بل تستلزم أيضاً مستوىً أعلى من التعاون والتنسيق والعمل المشترك بين الدول، وبين الحكومات والشركات والمؤسسات الأكاديمية والمنظمات غير الحكومية والدولية وغيرها من المنظمات التي لها مصلحة في حماية البنية التحتية الحاسمة. ويمكن القول ببساطة أن الشراكات بين القطاعين العام والخاص تحقق في كثير من الأحيان قدراً من النجاح حيث تفشل الجهود المنفردة.

وما من موضع يمثل فيه هذا الأمر أهمية أكثر مما يمثل في مجال البنية التحتية المعلوماتية الحاسمة، حيث تشكل قضايا الجرائم السيبرانية وحماية البيانات وأمن أنظمة التحكم وحماية الشبكات والاستجابة للحوادث السيبرانية والاستعادة تحديات متزايدة للحكومة والصناعة على حدٍ سواء. وكثيراً ما تتجاوز مجابهة هذه التحديات وغيرها من تحديات الأمن السيبراني قدرة كلٍ من الحكومة أو القطاع الخاص بشكل منفرد. ويقتضي تحقيق أفضل المصالح الدولية والوطنية والتجارية، بل والفردية، تقاسم مسؤولية تعزيز وضع الأمن السيبراني العالمي بين القطاعين العام والخاص والمجتمع الدولي.

2.3 مبادئ الشراكة

الخصائص الأساسية للشراكات الناجحة

سبقت الإشارة تكراراً إلى فعالية الحلول التعاونية للتحديات المعقدة والمستشرية. وقد طُبقت بنجاح شراكات بين القطاعين الحكومي والخاص على نطاق واسع من القضايا تتراوح بين مسائل أكاديمية وعلمية إلى تحديات اجتماعية واقتصادية وإلى النزاعات المسلحة وجهود مكافحة الإرهاب.

والشراكة هي علاقة يدخل فيها أفراد أو جماعات بغية تحقيق هدف محدد، وتتسم عامةً بالمنفعة المتبادلة والعمل والمشترك وتقاسم كلٍ من المسؤولية والمساءلة.

والمشاركون ينشئون الشراكات لرؤيتهم قيمة في العلاقة ولتوقعهم جنيٍ قدر ما من المنافع. كما يدرك الأعضاء أن تحقيق الغاية من الشراكة دون علاقة العمل المشترك هذه سيكون أصعب أو متعذراً بالكلية.

ويوجد عدد من الخصائص الأساسية المشتركة لشراكات القطاعين الناجحة، وتتباين أهميتها حسب طبيعة الشراكة والظروف المحيطة بها. ومن هذه الخصائص بشكل عام ما يلي:

- للشراكة منفعة متبادلة.
- الشراكة طوعية.

- للشركاء فهم موحد (وموثق) لأهداف الشراكة ونطاقها.
- يتفق الشركاء على إجراءات بأولويات لتحقيق تلك الأهداف.
- تحد الأدوار والمسؤوليات خطوط واضحة.
- تتسم الشراكة بالاتساع والشمول، وتنحصر معوقات الدخول فيها ضمن الحدود الدنيا.
- يسهم كل عضو بقدرات تعين الشراكة على المضي قدماً نحو تحقيق الهدف المشترك أو الغاية المشتركة.
- يُحتفظ لكل شريك باستقلاليته وسيادته – فالشراكة علاقة بين أكْفاء ثقات.
- يعمل الشركاء معاً بفعالية وكفاءة.
- تتسم الشراكة بشفافية ضمنية.
- يتاح للشراكة قدر من الموارد كافٍ لتحقيق الغرض منها.
- الاستثمار موزع بين الشركاء بإنصاف، ويشمل ذلك تقاسم التكاليف والأعباء.

وبما أن المسؤولية عن جوانب مختلفة – ومتداخلة أحياناً – من أمن البنية التحتية المعلوماتية الحاسمة توزع في كثير من الأحيان بين منظمات حكومية متعددة، فإن لاستمرار التواصل بين الجهات الحكومية أهمية بالنسبة إلى جهود إدارة المخاطر المشتركة بين القطاعين العام والخاص وبالنسبة إلى الشراكات الناجحة بين القطاعين بشكل عام.

3.3 عرض القيمة

تدرك الحكومات بشكل عام أن حماية مواطنيها من العواقب المدمرة المحتملة المقترنة بسوء استغلال البنية التحتية الحاسمة أو تعطيلها تكاد تكون مستحيلة دون مشاركة موسعة وطوعية من القطاع الخاص. فالقطاع الخاص يمتلك معظم البنية التحتية ويقوم على تشغيلها وصيانتها، مما يجعل خبرات القطاع الخاص وتعاونه والتنسيق معه وموارده وتفاعله بشكل جامع ضرورة بالنسبة إلى الجهود الحكومية في سبيل إدارة المخاطر المتعلقة بالنية التحتية الحاسمة.

ولتحقيق تفاعل القطاع الخاص مع الشراكات الأمنية أسباب أكثر تنوعاً، حيث تعنى الشركات أساساً بحماية عملائها وإدارة المخاطر المتعلقة بمؤسساتهم. وقد تعجز الشركات عن تحقيق أهدافها الكلية من إدارة المخاطر التجارية – والتي قد ترتبط ارتباطاً وثيقاً بالمخاطر الأمنية – دون مساعدة من شركاء آخرين من أحد القطاعين العام أو الخاص أو كليهما. وكثيراً ما تتقاطع مصالح الأمن العام مع الأنشطة المتركزة على منع الضرر عن البيانات أو المنتجات أو الممتلكات وغير ذلك من خسائر الكيانات التجارية. وعلى نفس المنوال، كثيراً ما يكون لاستمرار الأعمال وحماية الموظفين والاستثمارات مقوِّم أمني. ويقع على كاهل الشركات المسجلة في البورصة أيضاً التزام بالاستجابة لحاملي أسهمها، الذين يفرضون في كثير من الأحيان ضغوطاً على الشركات كي تتخذ إجراءات حيال قضايا معينة دعماً للصالح العام، مما يشمل قضايا متعلقة بالأمن وقضايا ذات حساسية سياسية (مثل تغير المناخ). وقد ينبع الضغط كذلك ضمن الشركات مع استشعار المسؤولين فيها المسؤولية المدنية. ومن الوارد أن تُمنح الشركات التي يثبت عملها مع الحكومة بشكل يتسم بالتعاون وحسن النوايا أوجه حماية من الناحية القانونية ومن ناحية مسؤولياتها، علاوة على تخفيضات في أقساطها التأمينية.

كما تمثل الشراكات الطوعية بديلاً جذاباً عن التنظيم، ومن شأن هذه وعوامل أخرى معها أن تحفز الشركات الخاصة على إصباغ علاقاتها بالجهات الحكومية بالتعاون والعمل المشترك لا بالمنازعة أو التركيز على الامتثال, ومن شأن إقامة علاقات عمل وثيقة مع الجهات الحكومية أن يتيح للشركات مزيداً من الشفافية في اطلاعها على السياسات الحكومية وقدرة معززة على التأثير في عملية صنع القرار الحكومي ضماناً لخروج السياسات على نحوٍ مقبول وفعال وقابل للتطبيق.

وليست الشراكات غايات في حد ذاتها، بل يقاس نجاح أي شراكة بمدى تحقيقها لأهداف المشاركين. ودائماً ما تتطلب الشراكات من الأفراد والمؤسسات اتخاذ إجراءات محددة أو تخصيص موارد للوفاء بالأهداف ذات الصلة. وفيما يتعلق بأمن البنية التحتية المعلوماتية الحاسمة ومرونتها، فإن غاية نجاح الشراكة بين القطاعين تتمثل في فعالية تلك الشراكة في إدارة المخاطر السيبرانية.

وتكمن الفائدة الأساسية من الشراكات في تمكينها الأفراد والمؤسسات من تحقيق أهداف أو اكتساب قدرات يكون منالها أصعب أو مستحيل في غياب الشراكة. وتتوصل مجموعات من المؤسسات في كثير في الأحيان إلى حلول أكثر فعالية لمشاكل صعبة ومعقدة مقارنةً بالمؤسسات التي تعمل بشكل منفرد، خاصة عندما تتعدد في تلك المشاكل علاقات الاعتماد البيني أو المنظمات أو البلدان. ومن شأن الشراكة المركزة أن تؤدي إلى توزيع أكثر فعالية للمسؤوليات حسب القدرات والخبرات، وإلى تقاسم الموارد وتطبيقها، وإلى تقاسم المعلومات والبيانات، وإلى تسخير قدر أعظم من رأس المال الفكري في سبيل تحقيق الأهداف المشتركة للمجموعة على نحوٍ أفضل.

ويمكن للمؤسسات المشاركِة في شراكات القطاعين العام والخاص الرامية إلى تدعيم أمن البنية التحتية الحاسمة – بما في ذلك أمن البنية التحتية المعلوماتية الحاسمة – أن تحقق تحسينات معتبرة في قدراتها على إدارة المخاطر نتيجةً للعمل المشترك والتعاون. وتشمل هذه ما يلي:

- تبين التهديدات ومواطن الضعف بشكل أفضل؛
- إعداد التقارير وتقاسم المعلومات المتعلقة بالتهديدات والإنذار على نحوٍ أفضل، وتعزيز قدرات الإنذار المبكر والمنع التخفيف من عواقب التهديدات؛
- تحسين إدارة الحوادث والاستجابة والتعافي؛
- تبادل الخبرات المتعلقة بمجالات التقنية والأمن والمخاطر وإدارة الطوارئ وغير ذلك من الخبرات؛
- تحسين النفاذ إلى أدوات تدريبية وتعليمية؛
- رفع درجة التأهب من خلال عمليات أمنية منسقة ومنفذة بشكل مشترك؛
- زيادة القدرة الكلية على إدارة المخاطر من خلال التشارك في تطوير أدوات ومعايير وممارسات فضلى في مجال إدارة المخاطر المشتركة ونشرها على نطاق واسع؛
- إنشاء مجتمعات وشبكات أمن قوية تشمل قطاعات البنية التحتية الحاسمة والأعمال وتتجاوز الحدود القُطرية؛
- زيادة الثقة والشفافية والحد من المنازعات بين الجهات الحكومية والقطاع الخاص؛
- إنشاء أدوات وعمليات لتقاسم المعلومات وسياسات أقوى تدعم تقاسم المعلومات؛
- تحسين أوجه الفعالية وتعزيز التنسيق والحد من الازدواجية بين الجهات الحكومية على جميع الأصعدة، وبين الجهات الحكومية والقطاع الخاص؛
- رفع مستوى فهم المخاطر المحيقة بالبنية التحتية الحاسمة (تهديدات جميع المخاطر ومواطن الضعف والعواقب) ومستوى المعرفة التفصيلية لعلاقات الاعتماد الدولية؛
- تجنب التنظيم باهظ التكلفة للجزء الأكبر من البنية التحتية الحاسمة؛
- الحد من قنوات المعلومات والولايات الحصرية الضيقة بين الجهات الحكومية وبين شركاء القطاعين العام والخاص؛
- رفع القدرة على قياس التقدم المحرز في التخفيف من المخاطر وفعالية البرامج على امتداد مشهد البنية التحتية الحاسمة؛
- زيادة فعالية تحديد الأولويات وتقسيم الجهود في مجال البحث والتطوير عبر الجهات الحكومية والقطاع الخاص؛
- زيادة الابتكار في نُهُج إدارة المخاطر المحيقة بالبنية التحتية الحاسمة.

وبما أن اعتماد المجتمعات على البنية التحتية المعلوماتية الحاسمة في تزايد مستمر، وبينما كان الأمن المحلي والقومي يقع تقليدياً ضمن نطاق سلطة الحكومات الوطنية، فإن التحدي الماثل في تأمين البنية التحتية المعلوماتية الحاسمة يتطلب شراكة موسعة ومستدامة بين الحكومة والشركات الخاصة التي تمتلك الكثير من بنيتنا التحتية وتشغلها وتديرها.

4.3 الشراكات وإدارة المخاطر الأمنية

يؤدي كلٌ من القطاع الحكومي والقطاع الخاص أدواراً مهمة في دورة إدارة المخاطر الأمنية، وينبغي لهما العمل معاً للوصول بجهود الحد من المخاطر إلى الوضع الأمثل.

ويستطيع القطاع الخاص استثمار ما اجتمع له من الخبرات الغزيرة لمعالجة قضايا صعبة، كما أنه يدخل على المعادلة عوامل المرونة وسرعة الاستجابة والابتكار. وما لأحد أن يتفوق على مالكي البنية التحتية المعلوماتية الحاسمة ومشغليها في فهم داخليات تشغيل بناهم التحتية وفي معرفة نماذج أعمالهم وقدراتهم الأساسية وما يخضعوا له من القيود المادية والمالية. كما يمثل القطاع الخاص في كثير من الأحيان خط الدفاع الأول بالنسبة إلى حماية البنية التحتية المعلوماتية الحاسمة ومجابهة ما تتعرض له من تهديدات، علاوةً على أداء دور المستجيب الأول لجهود التخفيف من عواقب الحوادث السيبرانية والتعافي منها في كثير من الأحيان. ولأن القطاع الخاص يمتلك في بلدان كثيرة قدراً عظيماً من البنية التحتية الحاسمة ويشغلها، فإن الصناعات الخاصة تكون عادةً الأكثر تعرضاً للمخاطر من خلال الاعتماد على البنية التحتية المعلوماتية الحاسمة أو استخدامها (مثل البنية التحتية الحاسمة التي تعتمد في عملها على تكنولوجيا المعلومات). والصناعة هي التي توفر كذلك الأدوات والمنتجات التي يستعان بها على إدارة المخاطر السيبرانية.

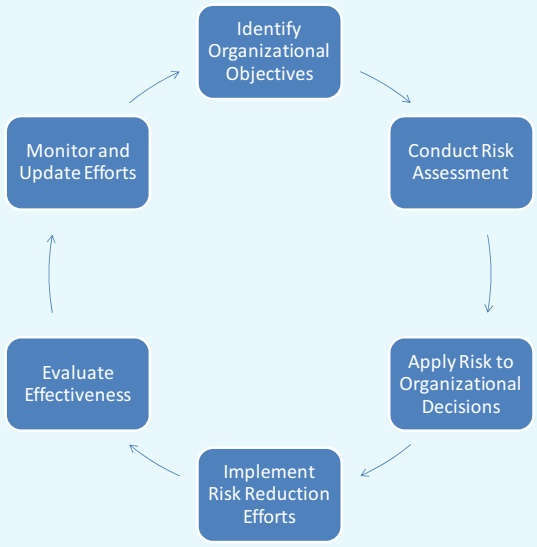
أما الحكومة فلها كذلك أن تسهم بشكل معتبر في شراكات الأمن، حيث توظف الجهات الحكومية قدراً معتبراً من الموارد النقدية والمعدات والموارد البشرية. كما تمتلك الحكومات الجهاز الاستخباراتي التقليدي، وتستطيع العمل مع القطاع الخاص وخدمات الاستخبارات الأجنبية على وضع صورة شاملة للتهديدات تتجاوز قدرات أي شركة خاصة منفردة. وعلى جانب آخر، تتولى الحكومة سن القوانين واللوائح التنظيمية، وتستأثر بحل السلطات، مما يتيح لها التأثير إلى حدٍ بعيد في أولويات الأمن وتوزيع الموارد لمساعدة الصناعة. وأخيراً، تستطيع الحكومة أداء دور التحكيم الفعال والموثوق ودور المنسق بين الشركات، التي من شأنها خلاف ذلك أن تحجم عن تقاسم معلومات حساسة في بيئة سوق تنافسية. وتتحمل الحكومة أيضاً مسؤولية مقارنة المخاطر على مستوى المرافق أو الأقاليم أو القطاعات مقابل مشهد المخاطر على الصعيد الوطني بل والعالمي. وفي بعض الحالات، تستطيع الحكومة جمع بيانات ذات صلة بالمخاطر وحمايتها من الكشف على العموم – مما يتضمن بيانات قد تكون مملوكة ملكية خاصة أو معلومات ذات حساسية تنافسية لشركات خاصة – في سبيل تبين التوجهات ومواطن الضعف المشتركة والمخاطر النسبية على أصول البنية التحتية المعلوماتية الحاسمة وأنظمتها وشبكاتها ووظائفها.[13]

والحكومة تؤدي تاريخياً دوراً مهيمناً في جمع المعلومات الاستخباراتية وتبين التهديدات، ولهذا أهمية خاصة بالنسبة إلى التهديدات المادية الأكثر تقليدية. أما فيما يتعلق بالتهديدات السيبرانية (مقارنةً بالتهديدات المادية)، فإن القطاع الخاص يؤدي الآن دوراً أبرز بكثير في تبين التهديدات والتخفيف منها والإنذار.

وفي نهاية المطاف، فإن فعالية شراكات القطاعين العام والخاص المتركزة على أمن البنية التحتية المعلوماتية الحاسمة يقاس بالدرجة التي تبلغها الشراكة في إدارة المخاطر والتخفيف منها. ويبين الشكل 6 أدناه دورة حياة تقليدية لإدارة المخاطر الأمنية يمكن تطبيقها بشكل واسع على معظم الأوضاع.

[13] في الولايات المتحدة، على سبيل المثال، يقدم القطاع الخاص طوعاً معلومات تتعلق بالتهديدات ومواطن الضعف ومعلومات أخرى إلى الحكومة عبر برنامج معلومات البنية التحتية الحاسمة المحمية. وهذا برنامج لحماية المعلومات يرفع من مستوى تقاسم المعلومات بين القطاع الخاص والحكومة. وتستخدم وزارة الأمن الداخلي الأمريكية هذا البرنامج لتحليل البنية التحتية الحاسمة والأنظمة المحمية وتأمينها، ولتبين مواطن الضعف وإعداد تقييمات المخاطر، ولتحسين تدابير التأهب للاستعادة. ولا يمكن استخدام البرنامج لأغراض تنظيمية، وهو محمي من مختلف اشتراطات الكشف على العموم.

الشكل 6: دورة حياة إدارة المخاطر



ومن بالغ الأهمية عند تناول المخاطر الأمنية على البنية التحتية المعلوماتية الحاسمة أن يتوصل أصحاب أدوار الصدارة في إدارة المخاطر إلى توافق بشأن النواتج المرغوبة من جهودهم المشتركة. وينبغي أن تتفق الحكومة والصناعة بشكل واضح على أهداف إدارة المخاطر وغاياتها التي ترمي جهودهما المشتركة إلى معالجتها.[14] ويرسي شركاء الحكومة والقطاع الخاص الذين يعملون معا أهدافاً محددة لإدارة المخاطر التي سيسعون بشكل مشترك في تحقيقها ويلزمون أنفسهم بها. وفي معرض تقييم المخاطر والحد منها (أو إدارتها على أي نحو آخر)، تنشأ أولويات جديدة ويعاد ضبط الأهداف بحيث تستوعب ما يطرأ على بيئة المخاطر من تغيرات.

وبعد توصل الأطراف معاً إلى تحديد أهداف إدارة المخاطر، يتطلب تبين المخاطر الأمنية وتقييمها مزيداً من العمل المشترك بين الحكومة والقطاع الخاص. ويسهم كلٌ من القطاعين الحكومي والخاص بقدرات معتبرة في هذه المرحلة من دورة إدارة المخاطر.

ويكون من الملائم في بعض الحالات أن يعمل المحللون الحكوميون بشكل مباشر مع القطاع الخاص (مع مديري المرافق أو الأنظمة والمسؤولين عنها على سبيل المثال) لإجراء تقييمات للمخاطر. ولأن الملاك من القطاع الخاص هم الأدرى بأنظمتهم وشبكاتهم، فلا غنىً عن مشاركتهم في سبيل ضمان اتسام عملية التقييم بالشمول والقوة. وتستطيع الجهات الحكومية أيضاً مساعدة الملاك والمشغلين من القطاع الخاص في تحديد المخاطر على مستوى المرفق أو المؤسسة عن طريق تزويدهم بأدوات تقييم وتقييم ذاتي (ومنهجيات وأساليب تحليلية). ومن شأن هذه المنتجات أن تجميع بين توفير التكلفة والوقت، وأن تتيح للشركات تقييم المخاطر على مستوى المرفق والمؤسسة.[15]

[14] في الولايات المتحدة، على سبيل المثال، تعمل الحكومة الفيدرالية مع شركاء من حكومات الولايات ومن القطاعين العام والخاص على الصعيد المحلي والإقليمي والدولي على إرساء أهداف تشمل القطاع كله، ولا يقتصر ذلك على قطاع تكنولوجيا المعلومات، بل يطبق أيضاً على 17 قطاعاً آخر في مجال البنية التحتية الحاسمة، وهذه القطاعات جميعاً تعتمد بدرجات متفاوتة على البنية التحتية المعلوماتية الحاسمة.

[15] على سبيل المثال، طورت إدارة الأمن السيبراني القومي التابعة لوزارة الأمن الداخلي الأمريكية أداة تقييم الأمن السيبراني كي يقيِّم المستخدمون وضع الأمن السيبراني لشبكاتهم السيبرانية وأنظمة التحكم الصناعي لديهم. وتوجه برمجيات هذه الأداة المستخدمين خلال عملية تنفذ على خطوات لتقييم ممارساتهم الأمنية المتعلقة بأنظمة التحكم وشبكات تكنولوجيا المعلومات مقابل معايير معترف بها على مستوى الصناعة. وتقدم الأداة قائمة بالتوصيات مرتبة حسب أولوياتها لرفع المستوى الأمني لأنظمة المؤسسة السيبرانية على الصعيد المؤسسي وعلى صعيد التحكم الصناعي (http://www.us-cert.gov/control_systems/satool.html).

وبعد تقييم المخاطر التي تتعرض لها البنية التحتية المعلوماتية الحاسمة، تستطيع الحكومة إدخال نتائج المخاطر المجمعة والمرتبة حسب أولوياتها في عمليتها الجامعة المتعلقة بالميزانيات والسياسات وصنع القرارات. كما تستطيع شركات القطاع الخاص تنفيذ عمليات تحليل وصنع قرارات شبيهة على المستوى المؤسسي.

ويمتلك القطاع الخاص في كثير من البلدان معظم البنية التحتية المعلوماتية الحاسمة أو يقوم على تشغيلها، ومؤدى هذه الحقيقة البسيطة هو أن عبء تنفيذ جهود الحد من المخاطر يقع إلى حد بعيد على عاتق الشركات الخاصة. والشراكة بحكم تعريفها علاقة طوعية يتفق الأطراف بمقتضاها على العمل معاً تحقيقاً لمصلحة مشتركة، مما يعني أن الحكومة لا تستطيع في العادة إجبار مؤسسات القطاع الخاص على اعتماد برامج لإدارة المخاطر أو الحد منها.

ومع ذلك، تُعتبر المخاطر المحيقة بأمن البنية التحتية الحاسمة أو سلامتها في بعض الحالات جسيمة بقدر يجعل الحكومة تشترط الإشراف التنظيمي،[16] بينما تنجح في حالات أخرى برامج تأمين البنية التحتية الحاسمة والبنية التحتية المعلوماتية الحاسمة الطوعية. وإدراكاً لمحدودية الموارد التي يواجهها كثير من الشركات الخاصة عندما تكون بصدد اتخاذ قرارات بشأن كيفية إدارة المخاطر الأمنية على البنية التحتية، وخاصة المخاطر ذات الاحتمالات المنخفضة والعواقب الوخيمة، فمن المستحسن أن تعمل الجهات الحكومية بشكل وثيق مع شركاء القطاع الخاص على تطوير وتوفير مجموعة من منتجات وأدوات إدارة المخاطر تنبني على كلٍ من أولويات احتياجات القطاع الخاص والمخاطر. ومن هذه أدوات لتقييم المخاطر وتحليلها، وممارسات فضلى ومعايير، وآليات تقاسم المعلومات، ومنتجات للتوعية الأمنية، وتدريبات تأهب، ومنتجات لإدارة الحوادث، وموارد تدريبية وتعليمية، وقائمة لا حصر لها من الأدوات والمبادرات والمنتجات والبرامج الأخرى. ومن شأن العمل المشترك على تطوير هذه الأدوات والمنتجات أن يحقق قدراً أعظم من التيقن بخروج هذه المنتجات على نحو فعال من حيث التكلفة ونافع، وبتوافر موارد لتحسين جهود التأهب والمنع والحماية والمرونة والاستجابة والاستعادة بالنسبة إلى البنية التحتية المعلوماتية الحاسمة لكلٍ من الحكومة والقطاع الخاص. كما تستطيع الحكومة العمل مع شركائها من القطاع الخاص على تنفيذ أنشطة انتشار لرفع مستوى التثقيف والتوعية بقضايا الأمن والمنتجات المتاحة.

وفي معرض تطبيق البرامج الرامية إلى الحد من المخاطر، يعمل القطاعين الحكومي والخاص معاً على تقييم أداء هذه البرامج وفعاليتها، وعلى قياس التقدم الشامل المحرز مقابل الأهداف الموضوعة لإدارة المخاطر. ويدخل في تقييم المبادرات المحددة وبرنامج المخاطر الشامل عدد من العوامل، منها على سبيل المثال لا الحصر التكلفة والوقت ومستوى الجهد المبذول والمرونة، وتقاس مقابل مستوى المخاطر الخاضع للتقييم والمخاطر المستجدة أو المتغيرة. ومع تطوير مقاييس والإبلاغ بها، توضع أولويات جديدة ويعاد ترتيب الأولويات القائمة استناداً إلى وضع المخاطر المتغير.

5.3 بيان ختامي

تمثل الشراكات بين القطاعين العام والخاص عنصراً ضرورياً في سبيل بناء برنامج أمني للبنية التحتية المعلوماتية الحاسمة ناجح وتحقيق الاستدامة فيه. وتتجاوز إدارة المخاطر المحيقة بالبنية التحتية المعلوماتية الحاسمة وما تدعمه من وظائف حيوية في مجال الأمن القومي والمجالين الاقتصادي والاجتماعي بفعالية وشمول قدرات أي من الحكومة والقطاع الخاص بشكل منفرد. ولهذا فإن الشراكات التي تتسم بالتعاون والالتزام تجمع موارد الكل وتحسن تقاسم المعلومات والاتصالات وتعزز الاستجابة للحوادث وتحسن قدرة الشركاء على إدارة المخاطر على جميع المستويات وفي جميع مراحل دورة حياة إدارة المخاطر. وقد أنشأت الولايات المتحدة على مدى العقد الماضي نموذجاً للشراكة بين القطاعين يوفر قاعدة صلبة لبرنامجها الخاص بأمن البنية التحتية المعلوماتية الحاسمة الوطنية. ومع توسع هذه الشراكة بين القطاعين وغيرها وامتدادها عبر الحدود الوطنية والجغرافية، فإن النواتج الاستراتيجية والتشغيلية لمثل هذه العلاقات ستؤدي إلى تعزيز القدرات الأمنية على الصعيد الوطني وإنشاء معمارية عالمية بالفعل لإدارة المخاطر التي تتعرض لها البنية التحتية المعلوماتية الحاسمة.

[16] على سبيل المثال، تفرض حكومة الولايات المتحدة لوائح تنظيمية أمنية للمفاعلات النووية التجارية وبعض المرافق الكيماوية ذات المخاطر العالية.

6.3 دراسة حالة: الشراكات بين القطاعين العام والخاص في الولايات المتحدة

ليست الشراكة بين الحكومة والصناعة بالأمر الجديد، إلا أن العقود الأخيرة شهدت اعترافاً متزايداً من جانب الحكومات بما تستلزمه برامج تأمين البنية التحتية الحاسمة الناجحة من مشاركة موسعة ومستدامة ونشطة من مالكي البنية التحتية ومشغليها, وفي التسعينيات من القرن العشرين، بدأت الحكومة الأمريكية في بذل جهود منسقة في سبيل تكوين شراكات مستدامة بين القطاعين العام والخاص تستهدف تحديداً تحسين أمن البنية التحتية الحاسمة.

التزام بالشراكات الأمنية

وقع الرئيس بيل كلينتون عام 1998 على القرار الرئاسي بتعليمات رقم 63، الذي أقر لأول مرة بالحاجة إلى تعزيز الشراكات الأمنية الموسعة والمستمرة بين الحكومة والقطاع الخاص الرامية إلى تأمين البنية التحتية الحاسمة. وقد اعترف القرار 63 بأهمية البنية التحتية الحاسمة بالنسبة إلى أمن الولايات المتحدة ورفاهتها الاقتصادية، ووضع لحماية البنية التحتية من أي هجمة إرهابية أولوية فيدرالية. واتسم إطار الشراكات الذي أرساه القرار 63 بالطوعية، حيث نص على أنه ينبغي للشراكات أن تكون "... صادقة ومتبادلة وتعاونية."[17] وقد تضمنت العناصر الأساسية في القرار 63 ذكراً لستة قطاعات بنية تحتية "حاسمة" على وجه التحديد، وإنشاءً للمركز الوطني لحماية البنية التحتية بغرض تقاسم المعلومات بين الجهات الحكومية كافة وبين الحكومة والقطاع الخاص، وتعزيزاً لمراكز القطاع الخاص المعنية بتقاسم المعلومات وتحليلها، وإنشاءً للمجلس الوطني لتأمين البنية التحتية الذي ضم قيادات من صناعات القطاع الخاص ومسؤولين حكوميين على مستوى الولايات والمستوى المحلي.

وقد شهد الزخم الموجه لهذه الجهود إثر هجمات 11 سبتمبر تعجيلاً هائلاً، حيث أبرزت الهجمات مواطن الضعف وأهمية البنية التحتية الحاسمة بالنسبة إلى رفاهة أمريكا. وفي ديسمبر 2003، أصدر الرئيس جورج بوش تعليمات الأمن الداخلي الرئاسية رقم 7 بشأن تحديد البنية التحتية الحاسمة وأولوياتها وحمايتها، حيث كانت التعليمات رقم 7 تهذيباً وتحديثاً للقرار 63 سالف الذكر، كما أنها زادت إطار الشراكة المذكور في ذلك القرار تحديداً وكلفت وزير الأمن الداخلي الجديد بمسؤوليات محددة في سبيل تحقيق أمن البنية التحتية الحاسمة وحمايتها من جميع الأخطار.

وقد وسعت التعليمات رقم 7 قائمة قطاعات البنية التحتية الحاسمة وأبرزت مجدداً أهمية الشراكات الطوعية بين الحكومة ومالكي البنية التحتية ومشغليها، مما يشمل القطاع الخاص. وقد وجهت الوزير إلى إقامة شراكة مع القطاع الخاص ترمي إلى "تحديد البنية التحتية الحاسمة والموارد الرئيسية وتحديد أولوياتها وتنسيق حمايتها، وإلى تسهيل تقاسم المعلومات حول التهديدات المادية والسيبرانية ومواطن الضعف والحوادث وتدابير الحماية المحتملة وأفضل الممارسات."[18] كما ألزمت التعليمات رقم 7 وزير الأمن الداخلي بوضع خطة قومية لحماية البنية التحتية الحاسمة، مما تمخض عم الخطة القومية لحماية البنية التحتية، التي خضعت للتحديث آخر مرة في عام 2009.

وتقدم هذه الخطة القومية الإطار الموحِد الرامي إلى جمع الجهود المشتتة في سبيل حماية مرونة البنية التحتية الحاسمة في الولايات المتحد وتحسينها. وتقنن الخطة أطر إدارة المخاطر والشراكة بين القطاعين العام والخاص، وتعرِّف 18 قطاعاً للبنية التحتية الحاسمة، وتحدد الوزارة والوكالات الحكومية المسؤولة بشكل أساسي عن إدارة الشراكات بين القطاعين في كل قطاع. وعلاوةً على إطار الشراكة، أعفى الكونغرس الأمريكي بعض مناقشات الشراكة وأنشطتها من بعض قوانين الكشف على العموم لضمان التبادل الحر والمفتوح لمعلومات أمن البنية التحتية بين الحكومة والقطاع الخاص.

نموذج شراكة القطاعات

وُضع نموذج شراكة القطاعات وإطار إدارة المخاطر المشار إليه في الخطة القومية لحماية البنية والتحتية، بل وهذه الخطة ذاتها، بالتشاور والعمل المشترك بشكل وثيق مع القطاع الخاص.

وتقود وزارة الأمن الداخلي الأمريكي وشركاؤها – بما في ذلك القطاع الخاص – الآن جهوداً لإدارة مخاطر البنية التحتية الحاسمة من خلال المجلس الاستشاري لشراكات البنية التحتية الحاسمة، الذي يؤدي دور الكيان المدير لهذه الشراكات. ويضم

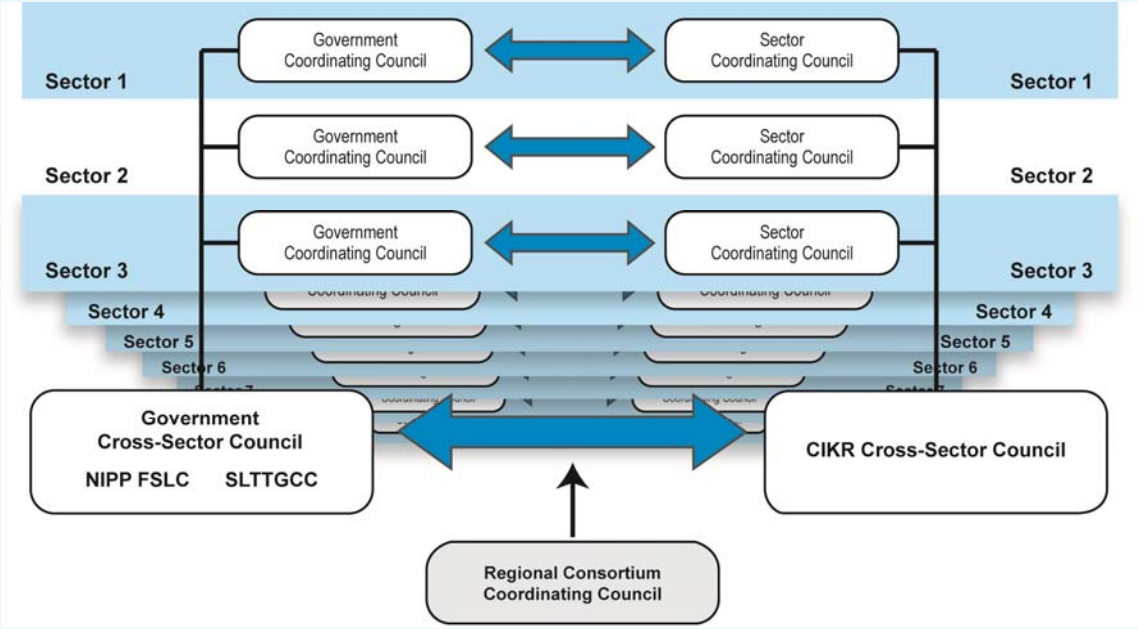
[17] http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
[18] http://www.fas.org/irp/offdocs/nspd/hspd-7.html

المجلس الاستشاري ممثلين من القطاع العام والقطاع الخاص من 18 قطاعاً للبنية التحتية الحاسمة وجهات حكومية على مستوى الولايات والمستوى المحلي واتحادات إقليمية. وترتبط هذه المؤسسات بدورها بالعديد من شبكات الشراكة الأخرى تشكل معاً نظاماً قومياً من التحالفات والعلاقات ذات المنفعة المتبادلة التي تعزز الوضع الكلي المتعلق بالمخاطر المحيقة بالبنية التحتية.

ويتيح المجلس الاستشاري منتدىً تعمل في ظله الحكومة الفيدرالية الأمريكية والقطاع الخاص معاً على تحسين مرونة البنية التحتية الحاسمة وحمايتها. وهو يتألف مما يربو على 700 عضو مؤسسي حكومي وخاص، مما يتضمن أكثر من 200 اتحاد تجاري تمثل شركات من جميع الأحجام. ويتشارك أعضاء المجلس الاستشاري لإنشاء استراتيجيات وبرامج ومنتجات تكوِّن قدرات حماية البنية التحتية ومرونتها في وجه مجموعة من تهديدات الأمن الداخلي، مما يضم الحوادث والجرائم والإرهاب والأمراض الوبائية والكوارث الطبيعية. ويطور الأعضاء مبادرات للحد من المخاطر على قطاعات بعينها في مجال البنية التحتية وفيما بين القطاعات كذلك.

وإطار المجلس الاستشاري مصمم بحيث يشجع على الحوار المفتوح ويسهله مع موازنة احتياجات مهمة الأمن الداخلي في نفس الوقت. ويتضمن إطار شراكة القطاعات مجالس معنية بقطاعات محددة وأخرى تعنى بقطاعات متعددة، مما يسهل التواصل والتنسيق بين الشركاء بشأن نطاق عريض من أنشطة الحماية والمرونة. ويبين الشكل 7 الإطار المذكور.

الشكل 7: نموذج المجلس الاستشاري لشراكة القطاعات



وضمن المجلس الاستشاري، تعمل مجالس تنسيق حكومي في كل قطاع مع مجالس تنسيق قطاعي، وهي كيانات ذاتية الحكم أنشأها مالكو البنية التحتية الحاسمة ومشغلوها. ومجالس التنسيق القطاعي هي كيان القطاع الخاص الأساسي المعني بالعمل مع الحكومة الأمريكية على تنسيق الأنشطة في أي قطاع من قطاعات البنية التحتية بعينه. وتختلف العضوية المحددة حسب القطاع، إلا أنها تضم قاعدة عريضة من الملاك والمشغلين والاتحادات التجارية. أما مجالس التنسيق الحكومي فهي المجالس النظيرة لمجالس التنسيق القطاعي على مستوى الحكومة الفيدرالية، وهي تسهل التنسيق بين الوكالات والتخطيط وتنفيذ مبادرات الحماية والمرونة الحكومية.

ويعمل مجلس تنسيق حكومات الولايات والمحليات والقبائل والأقاليم بشكل وثيق مع مجالس التنسيق الحكومي والقطاعي عبر جميع القطاعات، ويمثل الشركاء الحكوميين خارج النطاق الفيدرالي. والأعضاء متنوعون جغرافياً ويقدمون معرفة وخبرات مؤسسية واسعة النطاق من تخصصات مهنية شتى. أما مجلس تنسيق الاتحاد الإقليمي فيتيح منتدىً لمعالجة قضايا البنية التحتية الحاسمة على صعيد إقليمي. ويتضمن الأعضاء مؤسسات عامة وخاصة وإقليمية تعمل على تسهيل العمل المشترك اللازم لتنفيذ مهمة البنية التحتية الحاسمة بين الشركاء الإقليميين.

ويتألف مجلس البنية التحتية الحاسمة والموارد الرئيسية بين القطاعات من قيادات مجالس التنسيق القطاعي كافة، وهو يوفر تنسيقاً استراتيجياً على مستوىً رفيع مع الوكالات الفيدرالية وينشر أفضل الممارسات عبر قطاعات البنية التحتية ويقدم الاستشارات المتعلقة بجهود وضع سياسات وخطط الأمن الداخلي القومي ويشارك فيها. أما المجلس الفيدرالي لقيادات المستوى الرفيع فهو ينسق جهود الحد من المخاطر المحيقة بالبنية التحتية الحاسمة عبر الحكومة الفيدرالية ويعلن عنها، وهو النظير الحكومي لمجلس البنية التحتية الحاسمة والموارد الرئيسية بين القطاعات. ومن أعضائه الوكالات المعنية تحديداً بكل قطاع – بما في ذلك وزارة الأمن الداخلي – وعدد من الوزارات والوكالات الفيدرالية الأخرى.

وتدعم هذه البنية من الشراكات وتحسنها شراكات أخرى بين القطاعين العام والخاص على مستوى القضايا المحددة والمستوى دون الوطني والمستوى الدولي. فعلى سبيل المثال، يجمع فريق العمل المعني بالأمن السيبراني عبر القطاعات في إطار المجلس الاستشاري لشراكات البنية التحتية الحاسمة بين جهات القطاعين العام والخاص في سبيل العمل المشترك نحو معالجة المخاطر السيبرانية عبر قطاعات البنية التحتية الحاسمة. ومن خلال فريق العمل هذا، تقدم وزارة الأمن الداخلي للشركاء خبرات وإرشاداً وتساعدهم في فهم المخاطر السيبرانية والتخفيف منها وفي وضع تدابير حماية فعالة وملائمة. ويتضمن هذا إجراء مشروعات تجريبية نظامية عبر القطاعات مع شركاء القطاعات لمعالجة مجموعة من قضايا إدارة مخاطر الأمن السيبراني.

وتلقى الشراكات كذلك دعماً من آليات لتقاسم المعلومات وتحليلها مملوكة لكلٍ من الجهات الحكومية والقطاع الخاص مثل شبكة معلومات الأمن الداخلي والمركز الوطني للتنسيق بشأن البنية التحتية ومركز تقاسم معلومات تكنولوجيا المعلومات وتحليلها ومركز تقاسم معلومات تكنولوجيا المعلومات وتحليلها متعدد الولايات والمركز الوطني للأمن السيبراني وتكامل الاتصالات، مما يعزز القدرات الوطنية على الاستكشاف والمنع والاستعادة والاستجابة.

وقد أضفت هذه الشراكات، بالتنسيق مع شراكات أخرى بين القطاعين العام والخاص في أرجاء الولايات المتحدة كافة، قوة عظيمة على جهود الشركات والمجتمعات وحكومات الولايات المنفردة، كما أنها تدعم معاً جهداً منسقاً على الصعيد الوطني يرمي إلى جعل البنية التحتية آمنة ومرنة. وفي نهاية المطاف، أدت هذه الشراكات إلى تمكين الشركات والجهات الحكومية من إدارة التكاليف بكفاءة ومن فهم المخاطر المحيقة بالبنية التحتية على نحوٍ أفضل ومن بناء مؤسسة تتمتع بمزيدٍ من القوة والأمن.

7.3 دراسة حالة: بعض الشراكات بين القطاعين العام والخاص بالولايات المتحدة في مجال الأمن السيبراني

الشهر الوطني للتوعية بالأمن السيبراني

يمثل الشهر الوطني للتوعية بالأمن السيبراني وحملة "قف. فكِّر. اتصل." نموذجاً ممتازاً لبرنامج انتشار وتعليم وتوعية مشترك بين القطاعين العام والخاص قائم على العمل المشترك والتنسيق. وتثقف هذه الحملة عموم الشعب الأمريكي وتشركه وتمكنه من تولي أمر سلامتهم وأمنهم على الإنترنت، كما تشجع اتخاذ المزيد من الحيطة والعادات الذكية في سبيل رفع مستوى الأمن أثناء التوصيل بالإنترنت. ويقام الشهر الوطني للتوعية في شهر أكتوبر من كل عام ليكون منبراً تعليمياً يستطيع شركاء القطاعين العام والخاص من خلاله رفع الوعي بقضايا الأمن السيبراني عبر الولايات المتحدة.

ولا يركز شهر التوعية على التهديدات ومواطن الضعف السيبرانية التي يلزم الأفراد والشركات والجهات الحكومية التنبه إليها فحسب، بل على كثير من الخطوات التي يستطيع المواطنون العاديون اتخاذها للحد من المخاطر السيبرانية على أنفسهم وأمتهم كذلك. ولا غنى عن شراكة قوية بين القطاعين في مثل هذا الجهد لضرورة توافر مواردهما وخبراتهما معاً في سبيل حمل رسالة شهر التوعية إلى مجموعة واسعة من جماعات أصحاب المصالح التي تستهدفها الحملة.

وقد ساهم نطاق عريض من شركاء القطاع الخاص بالتعاون والتشارك مع وزارة الأمن الداخلي الأمريكية وغيرها من الوكالات الفيدرالية في جهود تعليمية موجهة. وتضمنت الفعاليات مؤتمرات تحت قيادة القطاع الخاص عن الأمن السيبراني وجهود تعليم وانتشار واسعة لكلٍ من موظفي الشركات الداخليين والعملاء.

كما شاركت وزارة الأمن الداخلي وغيرها من الوكالات الفيدرالية، مثل وكالة الأمن القومي ووزارة العدل، بشكل موسع في الأنشطة المحيطة بشهر التوعية. وكان لمساهمة القطاع الخاص ضرورة مساوية في سبيل تحقيق الانتشار اللازم والتعبير عن

الوجاهة واسعة النطاق للوعي المحسَّن بالأمن السيبراني. ونتيجة لهذا العمل المشترك بين القطاعين العام والخاص، بلغ العدد المقدر لمن وصلت إليهم حملة شهر التوعية الأخيرة 175 مليون شخص.[19]

سلسلة تدريبات العاصفة السيبرانية

للشراكات بين القطاعين العام والخاص في الولايات متحدة أهمية محورية أيضاً بالنسبة إلى جهود التأهب والاستجابة والاستعادة، كما يبين ذلك العمل المشترك المشاهد خلال سلسلة تدريبات العاصفة السيبرانية.

وتختبر سلسلة تدريبات العاصفة السيبرانية، التي أطلقت في أوائل عام 2006، أسلوب عمل الحكومة والقطاع الخاص معاً على الاستجابة لمجموعة متنوعة من الهجمات السيبرانية. وأبرز تدريب العاصفة السيبرانية الثالث في سبتمبر 2010 العمل المشترك والتعاون بين القطاعين وركز على ذلك. وكان من المشاركين في تدريب العاصفة السيبرانية الثالث سبع وزارات هي وزارات التجارة والدفاع والطاقة والأمن الداخلي والعدل والنقل والخزانة و11 ولاية و12 شريكاً دولياً و60 شركة قطاع خاص من قطاعات تتعلق بالبنية التحتية الحاسمة مثل قطاع الأعمال المصرفية والمالية والقطاع الكيماوي وقطاع الاتصالات وقطاع السدود وقطاع قاعدة الدفاع الصناعية وقطاع تكنولوجيا المعلومات والقطاع النووي وقطاع النقل وقطاع المياه، علاوةً على مجالس التنسيق القطاعي ومراكز تقاسم المعلومات وتحليلها. وأبرزت سيناريوهات الهجمات التي اتبعت خلال العاصفة السيبرانية 3 الأهمية الحاسمة للشراكة بين القطاعين عن طريق تهيئة بيئة تطلبت من الحكومة العمل مباشرة مع شركات القطاع الخاص المتأثرة بالهجمات وشركات القطاع الخاص التي تقدم حلولاً للتخفيف من آثار الهجمات.

كما انطوت العاصفة السيبرانية 3 على تجربة للخطة القومية للاستجابة للحوادث السيبرانية التي تحدد بشكل رسمي الأدوار والمسؤوليات والصلاحيات والعمل المشترك للاستجابة للحوادث السيبرانية وقدرات الإدارة، ولا يقتصر ذلك على نطاق الحكومة الفيدرالية، بل يتجاوزه إلى القطاع الخاص أيضاً. ومن الجوانب الأساسية لهذه الخطة القومية فريق التنسيق السيبراني الموحد، وهو جهاز تنسيقي يضم صناع قرار على مستوى رفيع من القطاعين العام والخاص لكلٍ من متطلبات الحالة المستقرة والحوادث، وهو فريق عمل تابع للمجلس الاستشاري لشراكات البنية التحتية الحاسمة ضمن قطاع الاتصالات (انظر القسم 2.5).

كما كانت العاصفة السيبرانية 3 الفرصة الأولى لتوظيف واختبار قدرات المركز الوطني للأمن السيبراني وتكامل الاتصالات، وهو مركز يعمل على مدار الساعة ويحمل مسؤولية إعداد صورة تشغيل مشتركة للوضع السيبراني والاتصالات عبر حكومة الولايات المتحدة الفيدرالية والقطاع الخاص، وقد أدى المركز في جميع مراحل تدريب العاصفة السيبرانية دور النقطة المركزية للعمل المشترك والوعي الظرفي لجميع الفاعلين من القطاعين، مسهلاً التنسيق اللازم لتخفيف آثار مختلف الهجمات متعددة القطاعات والحماية منها.

ويعتمد نجاح هذا المركز إلى حدٍ بعيد على المساهمات الطوعية من الشركاء فيه وقدراتهم ومواردهم. ويشارك المركز في مقره فريق التنسيق السيبراني الموحد ومراكز الحكومة الفيدرالية الستة المعنية بالأمن السيبراني ومركز التنسيق الوطني وفريق الاستجابة للطوارئ الحاسوبية المعني بأنظمة التحكم الصناعي ومكتب وزارة الأمن الداخلي المعني بالاستخبار والتحليل وإدارات ووكالات فيدرالية أخرى وإدارات حكومية على مستوى الولايات والمحليات والقبائل والأقاليم وشركاء من القطاع الخاص وشركاء دوليون.

وتكفل وزارة الأمن الداخلي من خلال سلسلة من الاتفاقات تَمكنها من الاستفادة إلى أقصى حد من خبراء القطاع الخاص عن طريق تسكينهم في طابق المركز الوطني هذا، وهذا يتيح للحكومة ومحللي تكنولوجيا المعلومات من القطاع الخاص التنسيق وتقاسم المعلومات والاستجابة للحوادث السيبرانية والتعافي منها بمزيدٍ من الفعالية.

المجلس الاستشاري الدولي

من النماذج الأخرى للشراكة بين القطاعين في الولايات المتحدة المجلس الاستشاري الدولي التابع لوزارة الخارجية الأمريكية الذي يسهل التعاون وتقاسم المعلومات في مجال الأمن التشغيلي بين وزارة الخارجية والقطاع الخاص الأمريكي على الصعيد العالمي.

[19] http://www.staysafeonline.org/resource-document/ncsam-2010-short-report

ويجمع القطاع الخاص بين دور المتلقي الأول لتقارير المجلس ونشراته التي تغطي قضايا أمنية على النطاق العالمي ودور المشارك الحاسم في هيكل إدارة المجلس والمساهم المهم في منتجات المجلس. ويتولى المجلس التنفيذي لهذا المجلس الاستشاري (30 من 34 عضواً فيه من شركات القطاع الخاص) جدول أعمال المنظمة ويجتمع ربع سنوياً لمعالجة القضايا الأمنية القائمة، مما يتضمن الجريمة عبر الوطنية وأمن معلومات الشركات.

ويستثمر المجلس خبرات القطاع الخاص التقنية في سبيل بدء مشروعات خاصة واستكمالها. ومن بين الشركات التي أدت دوراً استشارياً تقنياً للمجلس التنفيذي شركات M3 وCIGNA وGoogle وVerizon. وتتضمن عضوية المجلس الاستشاري الدولي حالياً ما يزيد على 500 7 شركة وهيئة أكاديمية ومنظمة دينية ومؤسسة غير حكومية من الولايات المتحدة. ويتيح العمل المشترك والتعاون بين القطاع الخاص ووزارة الخارجية للمركز الاستشاري الدولي تزويد المشاركين فيه بمعلومات قيمة ووعي ظرفي واستراتيجيات للحد من المخاطر، معالجاً نطاقاً عريضاً من شواغل المخاطر المادية والسيبرانية. ويعالج المجلس الاستشاري الدولي تحديداً المخاطر السيبرانية العالمية من خلال نشراته للتوعية السيبرانية، علاوةً على منتجات أخرى.

أفرقة الاستجابة للطوارئ الحاسوبية

تستثمر أفرقة الاستجابة للطوارئ الحاسوبية موارد القطاعين العام والخاص كي توفر قدرات شبه لحظية للرصد السيبراني والوعي الظرفي، إضافةً إلى قدرات التنبيه والإنذار السيبرانية لنطاق عريض من أصحاب المصلحة، ومنهم موفرو تكنولوجيا المعلومات وجهات حكومية على المستوى الفيدرالي ومستوى الولايات والمحليات وشركات وهيئات أكاديمية ومواطنين أفراد. ومع انتشار أفرقة الاستجابة للطوارئ الحاسوبية (أو أفرقة الاستجابة للحوادث الحاسوبية)، تزداد جهود العمل المشترك بينها على الصعيد العالمي لمعالجة طبيعة المخاطر السيبرانية التي لا حدود لها.

وفي الولايات المتحدة، يعمل فريق الاستجابة للطوارئ الحاسوبية الوطني بشكل وثيق مع منظمات حكومية أخرى ومع القطاع الخاص لتنسيق الاستجابات لتهديدات الأمن السيبراني. كما يوفر مركز تنسيق أفرقة الاستجابة للطوارئ الحاسوبية في جامعة كارنيجي ميلون بشكل مستقل تقارير ويطور أفضل الممارسات لبناء قدرات الأمن السيبراني على الأمد الطويل.

ويقدم فريق الاستجابة للطوارئ الحاسوبية الأمريكي مجموعة من الخدمات تشمل نشرات إعلامية تتعلق بالقضايا الأمنية ومواطن الضعف والاستغلال القائمة، ويعمل مع موردي البرمجيات لإنشاء إضافات برمجية لمعالجة مواطن الضعف الأمني والاستجابة للأحداث السيبرانية وإرساء أفضل الممارسات لاستخدام الحواسيب الشخصية. كما يمثل الفريق منصة انطلاق للعمل المشترك المتواصل بين القطاعين، حيث يوفر آلية لتواصل الشركات والأفراد مع الحكومة الفيدرالية بشكل مباشر.

ويثبت نموذج فريق الاستجابة للطوارئ الحاسوبية الأمريكي وانتشار أفرقة أخرى شبيهة حول العالم قدراتها على على تهيئة العمل المشترك بين القطاعين في مجال الأمن السيبراني على نحو يجمع بين قابلية الإدارة والتركيز مع إمكانية التوسع عبر الحدود الوطنية لتعزيز الأمن السيبراني عالمياً من خلال توصيلات بينية قوية. وتوصل الأنظمة والعمليات السيبرانية بين المستخدمين في جميع أنحاء العالم، كما أنها توهن الحدود بين البلدان والولايات القضائية وتقلل من أهميتها. وتقتضي سرعة الفضاء السيبراني وسيولته التعاون بين القطاعين العام والخاص على صعيد عالمي بتوفير الأمن السيبراني بشكل وافٍ للأشخاص والحكومات والشركات والبنية التحتية التي تعتمد عليه. وسيكون هذا التعاون ضرورياً كحد أدنى لمعالجة تحديات العزو والإنفاذ المتأصلة في ساحة الفضاء السيبراني التي لا تفصح عن هويات ولا تقف عند حدود. وتتخذ أفرقة الاستجابة للطوارئ الحاسوبية مكانة تتيح لها أن تشكل جزءاً لا يتجزأ من جهود الأمن السيبراني العالمية في المستقبل لأنها أظهرت بالفعل إطاراً إنتاجياً يرى فيه القطاعات العام والخاص، ومجتمعات وطنية وإقليمية أخرى مختلفة، بعضهم البعض كأصحاب مصلحة متبادلة في نظام إيكولوجي سيبراني يرجون جميعاً رفع مستوى الأمن فيه.

وتمثل الشراكات بين القطاعين العام والخاص عنصراً ضرورياً في سبيل بناء برنامج أمني للبنية التحتية المعلوماتية الحاسمة ناجح وتحقيق الاستدامة فيه. وتتجاوز إدارة المخاطر المحيقة بالبنية التحتية المعلوماتية الحاسمة وما تدعمه من وظائف حيوية في مجال الأمن القومي والمجالين الاقتصادي والاجتماعي بفعالية وشمول قدرات أي من الحكومة أو القطاع الخاص بشكل منفرد. ولهذا فإن الشراكات التي تتسم بالتعاون والالتزام تجمع موارد الجميع وتحسن تقاسم المعلومات والاتصالات وتعزز الاستجابة للحوادث وتحسن قدرة الشركاء على إدارة المخاطر على جميع المستويات وفي جميع مراحل دورة حياة إدارة المخاطر. وقد أنشأت الولايات المتحدة على مدى العقد الماضي نموذجاً للشراكة بين القطاعين توفر قاعدة صلبة لبرنامجها الخاص بأمن البنية

التحتية المعلوماتية الحاسمة الوطنية. سومع توسع هذه الشراكة بين القطاعين وغيرها وامتدادها عبر الحدود الوطنية والجغرافية، فإن النواتج الاستراتيجية والتشغيلية لمثل هذه العلاقات ستؤدي إلى تعزيز القدرات الأمنية على الصعيد الوطني وإنشاء معمارية عالمية حقاً لإدارة المخاطر التي تتعرض لها البنية التحتية المعلوماتية الحاسمة.

4 أفضل الممارسات المتعلقة بالأمن السيبراني الوطني: بناء قدرة وطنية لإدارة حوادث الأمن الحاسوبي

1.4 مقدمة

يتطلب ضمان سلامة الأمن القومي والحيوية الاقتصادية اعترافاً بأن حكومة أي بلد لا تسيطر على جميع المخاطر ولا تستطيع وحدها الحد منها، بل المسؤولية عن ذلك موزعة بين الحكومة الوطنية والمحلية بمختلف فروعها ومالكي البنية التحتية الحاسمة ومشغليها والهيئات الأكاديمية والمواطنين جميعاً. ويجب تبين المخاطر الجديدة والناشئة وتحليلها والحد منها بفعالية في سبيل ضمان أمن المواطنين وسلامتهم في حياتهم اليومية. وقد تنطوي أنشطة إدارة المخاطر هذه على ضمان استمرارية أعمال الحكومة وحماية مرافق توليد الكهرباء وخدمات الاستجابة للطوارئ وضمان موثوقية سلسلة الإمداد وغير ذلك. ويعتمد كل من هذه الوظائف اعتماداً كبيراً على تكنولوجيا المعلومات في أي اقتصاد حديث. ويتزايد إدراك قادة البلدان أن أمن المعلومات وتكنولوجيا المعلومات يصب في مصلحة الأمن القومي وأنه ينبغي تقنينه في القوانين والاستراتيجية القومية. وتقع ضمن أساسيات استراتيجيات تحسين هذا النوع من الأمن قدرات تشغيلية محددة، مثل أنشطة إدارة الحوادث التي يضطلع بها في العادة فريق وطني يعنى بالاستجابة للحوادث الحاسوبية.

2.4 أهمية وضع استراتيجية وطنية للأمن السيبراني

الوضع الأمثل أن يكون إعداد استراتيجية وطنية للأمن السيبراني الخطوة الأولى في إنشاء برنامج وطني للأمن السيبراني. وينبغي أن يوضح أي إطار سياسات وطني أهمية الأمن السيبراني وأن يعين أصحاب المصلحة على فهم أدوارهم وأن يحدد الأهداف والأولويات. وينبغي أن تجمع الاستراتيجية الوطنية بين أساسيات الأمن (مثل التوعية) وأن تبرز أهمية العلاقات التعاونية بين أصحاب المصلحة على الصعيد الوطني. ومن الممكن كذلك أن تقاوم الاستراتيجية الوطنية مقام كواليس إنشاء القوانين ذات الصلة بالأمن السيبراني، وذلك على سبيل المثال في مجالات الجرائم الحاسوبية وحماية الملكية الفكرية والخصوصية. وأخيراً، ينبغي للاستراتيجية أن تحقق التوازن بين الحاجة إلى الأمن والحاجة إلى احترام حقوق المواطنين والقيم الثقافية للبلاد وأعرافها.

وينبغي كذلك أن تعبر الاستراتيجية عن الحاجة إلى قدرات تشغيلية محددة، كما ينبغي تعمد تحقيق الاتساق بين الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية مع تلك الأهداف الاستراتيجية المتعلقة بالأمن السيبراني الوطني حتى يسهم عمل الفريق في تحقيقها. وبينما يمثل وضع استراتيجية وطنية كخطوة أولى الحالة المثلى، فلا يكون ذلك متيسراً في كثير من الأحوال، وقد يرجع ذلك إلى صعوبة التوصل إلى توافق بين عدد كبير من أصحاب المصلحة على استراتيجية معينة. ويمكن بدلاً من ذلك أن يرى قادة البلاد أن بناء قدرة لإدارة الحوادث يمثل حاجة أكثر إلحاحاً من وضع استراتيجية متكاملة تماماً. ويمكن في مثل هذه الحالات أن تسير جهود وضع استراتيجية فعالة بالتوازي مع بناء قدرة إدارة الحوادث. وعلى أي حال، ينبغي أن تعمل الجهة الراعية للفريق الوطني المعني بالاستجابة للحوادث الحاسوبية مع الحكومة في سبيل ضمان مراعاة الاحتياجات والأولويات الوطنية في جميع مراحل عملية بناء فريق وطني للاستجابة للحوادث الحاسوبية وإدارته.

3.4 أصحاب المصلحة الرئيسيون في الأمن السيبراني الوطني

يتعلق الأمن السيبراني الوطني بعدد كبير من أصحاب المصلحة. ويصف هذا القسم بشكل عام أدوار أصحاب المصلحة التقليديين على الصعيد الوطني ومسؤولياتهم، وكيف يمكن لهم الإسهام في برنامج وطني لإدارة الأمن السيبراني. وليست هذه الأدوار حكراً على عمليات الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية، لكن من الوارد أن يتفاعل كثير من أصحاب المصلحة المشار إليهم هنا بشكل مباشر مع ذلك الفريق. وعلاوةً على ذلك، من شأن الفريق الوطني المعني بالاستجابة

للحوادث الحاسوبية أن يضفي على دوره تحسيناً ويعين على تطوير ثقافة أمنية عن طريق التفاعل بشكل استباقي مع أصحاب المصلحة هؤلاء.

وللحكومة أدوار ومسؤوليات عديدة في سبيل تعزيز الأمن السيبراني الوطني. ويتصدر هذه الأدوار تحديد الاستراتيجية الوطنية وتهيئة إطار السياسات الذي يصف المعمارية التي يقوم عليها تكوين الجهود الوطنية وتشغيلها. ثم تأتي بعد ذلك مسؤولية الحكومة عن المشاركة مع جميع أصحاب المصلحة في جهود تبين المخاطر وتحليلها والحد منها. وللحكومة أيضاً دور أساسي تؤديه في ساحة العلاقات الدولية والأمن السيبراني، خاصة في مجالي المعاهدات المتعلقة بالأمن السيبراني وتحقيق الاتساق في القوانين الوطنية المتعلقة بالجرائم السيبرانية.

الجناح التنفيذي للحكومة

عادةً ما تقع على الجناح التنفيذي للحكومة في معظم البلدان مسؤولية إنفاذ القوانين وضمان الأمن. وقد يشمل ذلك الجهاز العسكري أيضاً. ويتولى الجناح التنفيذي في كثير من الأحيان رعاية برنامج الأمن السيبراني الوطني. ويجب على القسم التنفيذي من الحكومة التكفل باستمرارية مقومات برنامج الأمن السيبراني وتوافر الموارد الملائمة له (أن يوفر له على سبيل المثال ما يلزم من اعتماد وموظفين وتمويل وغير ذلك).

الجناح التشريعي للحكومة

يعمل الذراع التشريعي للحكومة على توفير قوانين فعالة تعزز ثقافة الأمن السيبراني. وسواء كان ذلك من خلال تخصيص الموارد أو التمويل، أو تشريعات توجب تنفيذ الاستراتيجية الوطنية، أو قوانين الخصوصية أو منع الضرر، أو قوانين تعرِّف السلوك الإجرامي، فيجب أن يكفل المشرع توافر الأسس اللازمة لإنجاح البرنامج الوطني للأمن السيبراني.

القضاء

للجهاز القضائي والمؤسسات القانونية في البلاد دور مهم تؤديه في إطار الاستراتيجية الوطنية للأمن السيبراني. ويتعلق هذا الدور تحديداً بتحقيق الوضوح والاتساق في أجزاء القانون التي من شأنها التأثير في الأمن السيبراني. ومن أمثلة ذلك قانون الخصوصية. ويستطيع المجتمع القانوني أيضاً، عن طريق العمل مع النظراء على الصعيد العالمي، الإعانة على الحد من قدرة المجرمين وغيرهم من المعتدين على استغلال الاختلافات القانونية بين الولايات القضائية.

جهاز إنفاذ القانون

يكفل جهاز إنفاذ القانون وضع التشريعات المتعلقة بالأمن السيبراني موضع الإنفاذ. ويمكن لهذا الجهاز أيضاً أن يكون مصدراً مهماً للمعلومات الاستخباراتية المتعلقة بالأنشطة الضارة ومواطن الضعف المستغَلة وأساليب الهجوم. ويتيح تقاسم هذه المعلومات لمالكي البنية التحتية الحاسمة ومشغليها الاستفادة من خبرات الغير في سبيل تحسين ممارسات الأمن السيبراني وإدارته. وأخيراً، يستطيع جهاز إنفاذ القانون تحسين الأمن السيبراني عن طريق التعاون مع النظراء في بلدان أخرى في مجال ملاحقة الفاعلين الإجراميين الذين يؤثرون في الأنظمة وتوقيفهم بغض النظر عن الحدود الجغرافية.

المجتمع الاستخباراتي

يؤدي المجتمع الاستخباراتي دور رصد وإنذار مهماً للبنية التحتية التقنية. فعادةً ما ترصد المؤسسات الاستخباراتية مختلف مصادر المعلومات تلمساً لأي تهديدات للبنية التحتية للبلاد أو مواطن ضعف فيها. وينبغي أن تخضع هذه المعلومات لعملية ترشيح وأن تقدم إلى الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية، وإلى مالكي البنية التحتية حسب الاقتضاء. ويعين هذا على ضمان توقع الهجمات وإدراكها والتصدي لها بكفاءة.

مالكو البنية التحتية الحاسمة ومشغلوها

يمكن تعريف البنية التحتية الحاسمة بشكل عام كما يلي:

الأنظمة والأصول، سواء كانت مادية أو افتراضية، التي تبلغ من الأهمية الحيوية بالنسبة إلى البلاد مبلغاً يجعل من شأن تعطيل تلك الأنظمة والأصول أو تدميرها أن يكون له أثر سلبي على الأمن أو الأمن الاقتصادي الوطني أو الصحة أو السلامة العامة على الصعيد الوطني، أو أي تركيبة من هذه الأمور.

ومالكو البنية التحتية الحاسمة ومشغلوها من أصحاب المصلحة ذوي الأهمية البالغة في الاستراتيجية العامة للأمن السيبراني للبلاد. فعادةً ما يكون لدى مشغلي البنية التحتية فهم لكيفية تأثير التهديدات الأمنية ومواطن الضعف في قطاعهم. كما تقع على كاهل مشغلي البنية التحتية أداء المهمة اليومية المتمثلة في تنفيذ التوصيات أو الالتزامات الأمنية الصادرة عن الحكومة الوطنية وغيرها من السلطات. ويجب عليهم تحقيق التوازن بين الحاجة إلى الأمن وما قد يتعارض مع ذلك أحياناً من أهداف الكفاءة والربحية.

ونظراً لوضعهم الفريد، يحوز مالكو البنية التحتية ومشغلوها معلومات قيمة للغاية تتراوح بين المشاكل البرمجية الفعلية وما قد تتعرض له من هجمات سيبرانية إلى فعالية التدابير المضادة أو استراتيجيات الحد من المخاطر. كما أنهم من أوائل مستخدمي المعلومات المتعلقة بمواطن الضعف الأمنية. وأخيراً، نظراً لخبراتهم العملية في تنفيذ المعايير الأمنية والامتثال للقانون، فقد يكون للمالكين والمشغلين إسهام قيِّم في وضع لوائح وتشريعات فعالة وواقعية.

الموردون

يسهم موردو تكنولوجيات المعلومات وخدماتها في الأمن السيبراني الوطني من خلال ممارسات التطوير والجهود المستمرة للحد من مواطن الضعف. ويمكن في كثير من الأحيان أن يكون الموردون مصدراً لمعلومات تتعلق بمواطن الضعف، حيث إنهم يحرصون دوماً على تزويد المستخدمين بأحدث المعلومات والحلول التقنية للحد من مواطن الضعف المعروفة. ويتشارك الموردون، في الوضع الأمثل، مع الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية ويساعدون على توسيع قدرات التحليل وحل المشاكل التي تحتاج إليها تلك الأفرقة من أجل الاستجابة للحوادث. ومن شأن تقاسم المعلومات بين الموردين وكبار عملائهم والفريق الوطني المعني بالاستجابة للحوادث الحاسوبية أن ينشئ علاقة شراكة تؤدي باستمرار إلى تحسين المستوى الأمني للتكنولوجيات والخدمات.

الهيئات الأكاديمية

تؤدي المؤسسات التعليمية دوراً أساسياً في تطوير رأس المال البشري والمهارات التقنية اللازمة لحل المشاكل المعقدة، مثل جوانب الأمن السيبراني. ويجري الأكاديميون أبحاثاً تؤدي إلى تحسين الجوانب التقنية والقانونية والسياساتية للأمن السيبراني. وأخيراً، فقد رعت المؤسسات التعليمية في كثير من البلاد الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية واستضافتها.

الحكومات الأجنبية

يجب على الدول الاعتناء بالمساعدة على منع أي هجمات سيبرانية على دول الجوار والحلفاء. وينبغي لعددٍ من الأسباب، بما في ذلك شواغل تتعلق بالاقتصاد وبالسياسة وبالنية التحتية، إقامة شراكات لتناول المخاطر وعلاقات الاعتماد البينية على الصعيد العالمي بالنقاش. كما يمكن للحلفاء ودول الجوار توفير مصدر قيِّم للمعلومات الاستخبارية وتعزيز عمليات المنع والتأهب السيبراني إقليمياً.

المواطنون

يعتمد المواطنون على جميع أصحاب المصلحة من أجل تحقيق الأمن الوطني واستقرار البنية التحتية الحاسمة. وللمواطنين في أي بلد مصلحة في تحقيق الأداء الموثوق للاستراتيجية الوطنية للأمن السيبراني، كما أنهم يشكلون جزءاً لا يتجزأ من تلك الاستراتيجية.

4.4 الدور الخاص للفريق الوطني المعني بالاستجابة للحوادث الحاسوبية

تمثل الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وما شابهها من مؤسسات، في الوضع الأمثل، مكونات حاسمة من الاستراتيجية الوطنية للأمن السيبراني.[20] وأول ذلك أن هذه الأفرقة الوطنية توفر القدرة على الاستجابة للحوادث الأمنية الحاسوبية التي تعتبر ذات أهمية قومية[21]. ولأنها تجمع معلومات عن حوادث الأمن الحاسوبي وتحللها بشكل يومي، فإن هذه الأفرقة الوطنية تمثل مصدراً ممتازاً للدروس المستفادة وغير ذلك من المعلومات التي من شأنها أن تساعد أصحاب المصلحة على الحد من المخاطر. كما يمكن للأفرقة الوطنية أن تكون عاملاً مساعداً في سبيل عقد حوار وطني مثمر بشأن الأمن السيبراني والوعي عن طريق التفاعل مع أصحاب المصلحة من القطاعين الخاص والحكومي. وفيما يلي تناول لدور الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية، وإن لم يكن من المتوقع أن تؤدي كل مؤسسة جميع هذه الوظائف ولا أن تنفذ جميع هذه المهام. ومع ذلك فإن هذه الأدوار تمثل الكيفية التي يدعم بها فريق وطني معني بالاستجابة للحوادث الحاسوبية في العادة الأمن السيبراني الوطني.

5.4 تحليل حوادث الأمن الحاسوبي لتبين مجموعات الاقتحام

تعرَّف مجموعة الاقتحام بأنها مجموعة من حوادث الأمن الحاسوبي التي يتشابه فاعلوها أو أساليبها. وقد يتطلب تبين تورط فاعلين متشابهين مجموعة متنوعة من الأساليب التحليلية، وهو يرتبط ارتباطاً وثيقاً بمسألة الأسلوب. وقد ينطوي الوقوف على تطابق الأسلوب في هجمات مختلفة مسائل وسيط الهجوم (بريد إلكتروني أو صفحات إلكترونية احتيالية وما إلى ذلك) أو أوجه تشابه بين عينات من البرمجيات الضارة أو توجيه المعلومات المسروقة (من خلال عناوين إنترنت بديلة محددة على سبيل المثال).

ويمثل تبين مجموعات الاقتحام في الأساس شكلاً محسَّناً من تحليل العلاقات البينية التي يعرفها الكثير ممن يتعاملون مع حوادث الأمن الحاسوبي. وبشكل عام، تقسَّم أنشطة الحوادث إلى فئات مختلفة مثل:

- نشاط إجرامي
- نشاط من تنفيذ بلدان أخرى
- غير محدد

ويمكن بعد ذلك تقديم هذه المعلومات والتحليلات إلى سلطات وطنية أخرى لاتخاذ إجراء حسب شواغل الأمن لدى الدولة وأهدافها.

استخدام معلومات حساسة تتعلق بجهاز إنفاذ الأمن أو الاستخبارات

نظراً للمهمة القومية التي تؤديها الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وعلاقتها الوثيقة في كثير من الأحيان مع الحكومة الوطنية وعملها بشكل يومي على حماية معلومات حساسة، فقد تستخدم معلومات حساسة من مؤسسات وطنية معنية بالاستخبارات أو إنفاذ القانون فيما تجري من تحليلات. ومن شأن استخدام هذا النوع من المعلومات أن يعزز عمل هذه الأفرقة الوطنية، لكن ذلك يقتضي أيضاً وجود علاقات قوية قائمة على الثقة بينها وبين الحكومة، علاوةً على تدابير قوية لتأمين المعلومات.

[20] انظر **الملحق ألف** للاطلاع على مزيدٍ من الموارد عن التخطيط لفريق وطني معني بالاستجابة للحوادث الحاسوبية وتكوينه.

[21] يتناول القسم 1.3.3 بشكل أشمل مسألة تحديد الحوادث التي ترقى إلى مستوى الأهمية الوطنية.

مَورد للحكومة الوطنية بشأن قضايا الأمن السيبراني

من شأن أي فريق وطني معني بالاستجابة للحوادث الحاسوبية أن يمثل مورداً قيِّماً للحكومة الوطنية بشأن القضايا التقنية والسياساتية والقانونية المتعلقة بالأمن السيبراني. وقد يكون قادراً على تقديم الاستشارات للحكومة بشأن ملاءمة أو أمن الأنظمة التي تقدم الحكومة على تركيبها أو تنفيذها. وعلاوة على ذلك، من شأن الفريق الوطني أن يمد الجهات الحكومية بتنبيهات ونشرات تقنية وممارسات فضلى وغير ذلك من الاستشارات.

تقييم التأهب السيبراني وإدارة الأزمات على الصعيد الوطني

من شأن الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية أن يساعد القادة الوطنيين وأصحاب المصلحة الأساسيين على اختبار مستوى تحمل البلاد للهجمات والأزمات السيبرانية وقياسه. وقد تتخذ هذه المساعدة شكل توفير دعم تقني وأساليب تحليلية للتخطيط لتدريبات وتنفيذها أو تقديم الاستشارات بشأن وضع التهديدات السيبرانية الحالية أو واقعية التدريبات.

التنبيه والإنذار على الصعيد الوطني

تؤدي معظم الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية القائمة وظيفة إنذار تتعلق بتنبيه المجتمعات الوطنية الأساسية إلى مشاكل تتراوح بين مواطن ضعف محددة في برمجيات أو أنظمة إلى الأساليب الإجرامية الناشئة وتهديدات البرمجيات الضارة.

بناء قدرات أفرقة الاستجابة للحوادث الحاسوبية في المؤسسات

للأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية دور أساسي تؤديه في بناء قدرات الأمن السيبراني. وبشكل محدد، تستطيع هذه الأفرقة الوطنية مساعدة أفرقة الاستجابة للحوادث الحاسوبية العاملة في مؤسسات البلاد بأشكال شتى، منها الاستشارة والتدريب وأفضل الممارسات، أو بالتوظيف في بعض الحالات.

نقطة اتصال موثوقة ومنسق وطني

كثيراً ما تؤدي الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية دور نقطة اتصال موثوقة على المستوى الوطني بالنسبة إلى قضايا الأمن السيبراني. فعلى سبيل المثال، تتعامل الأفرقة الوطنية في كثيرٍ من الأحيان مع طلبات واردة من بلدان أخرى أو من مؤسسات أجنبية تتعلق بنشاط ضار نابع من حواسيب أو أنظمة واقعةً في بلادها. وعلى نفس المنوال، كثيراً ما تؤدي الأفرقة الوطنية دوراً تنسيقياً للمؤسسات المحلية التي تحاول حل حوادث متعلقة بالأمن السيبراني. وفي العادة لا يتولى الفريق الوطني في إطار هذا الدور تحليل الحوادث ولا حلها بنفسه، بل يساعد في توجيه المؤسسات التي تواجه الحوادث إلى معلومات أو خدمات أو كيانات أخرى تستطيع مساعدتها.

6.4 تكوين ثقافة الأمن السيبراني

يستطيع الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية المساعدة في تكوين ثقافة الأمن السيبراني في البلاد. وينطوي تكوين ثقافة الأمن السيبراني على كثيرٍ من الأنشطة منها توعية المواطنين الأفراد وتثقيفهم بشأن مخاطر التوصيل بالإنترنت، وتثقيف أصحاب المصلحة على الصعيد الوطني بأثر الأنشطة الافتراضية على مؤسساتهم وعواقب أنشطتهم على الأمن السيبراني والمعلوماتي.

7.4 الأهداف الاستراتيجية وأهداف التمكين لقدرات إدارة الحوادث

يعرض هذا القسم الأهداف الاستراتيجية وأهداف التمكين التي ينبغي النظر فيها في معرض تكوين فريق وطني يعنى بالاستجابة للحوادث الحاسوبية. وتقدم هذه المعلومات استعراضاً للاعتبارات والأهداف اللازمة لضمان دعم الاستراتيجية الوطنية للأمن السيبراني ولتحقيق الاتساق بين الفريق الوطني والاستراتيجية الوطنية. وأهدف التمكين هي خطوات محددة لتحقيق الأهداف الاستراتيجية[22]. وللأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية أربعة أهداف استراتيجية هي كالتالي:

1) تخطيط وبناء قدرة مركزية لإدارة حوادث أمن الحواسيب (الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية)
2) تهيئة الوعي الظرفي المشترك
3) إدارة الحوادث السيبرانية
4) دعم الاستراتيجية الوطنية للأمن السيبراني.

ويوضح كلٌ من هذه الأهداف الاستراتيجية العناصر الأساسية للفريق الوطني المعني بالاستجابة للحوادث الحاسوبية ويجب على الجهة الراعية للفريق الوطني وزنه بعناية. والأهداف الاستراتيجية عبارة عن متطلبات ضرورية طويلة الأمد تعين على بناء قدرة الاستجابة للحوادث السيبرانية وتعزيز المعلومات والأمن السيبراني على صعيد وطني. ويتبع كلاً من الأهداف الاستراتيجية أهداف تمكين. وتساعد أهداف التمكين الجهة التي يتبعها الفريق على بناء القدرة. وهي توضح بمزيد من التفصيل الاعتبارات والأنشطة اللازمة لتنفيذ الأهداف الاستراتيجية. وتختلف الإرشادات المتاحة لكل هدف حسب نضج الموضوع، حيث يكون لبعض الموضوعات، مثل معالجة الحوادث، تاريخ قوي، بينما تمثل موضوعات أخرى، مثل تنفيذ استراتيجية وطنية للأمن السيبراني من خلال الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية، تخصصات ناشئة.

وليس من مقاصد هذه الوثيقة توفير تعليمات تنفيذية محددة، بل تبرز المتطلبات الفريدة لبناء القدرات في مجال إدارة الحوادث السيبرانية. وأخيراً، يُختتم كل هدف استراتيجي بقائمة بالمراجع الإضافية والموارد التدريبية. وليست هذه المصادر شاملة، بل تزود القارئ بخطوة تالية على مسار الموارد التدريبية والإعلامية.[23]

الهدف الاستراتيجي: تخطيط وبناء قدرة مركزية لإدارة حوادث أمن الحواسيب (الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية)

قبل أن يمكن إدارة أول حادثة أمن سيبراني، يجب أولاً بناء القدرة نفسها بشكل تنظيمي مثل شكل الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية. ويتيح وجود مصدر وحيد أو نقطة وحيدة للاتصال بشأن حوادث الأمن الحاسوبي وقضايا الأمن السيبراني عدة فوائد. فالمؤسسة الواحدة توفر لأصحاب المصلحة مصدراً معروفاً للمعلومات. كما يستطيع الفريق الوطني تزويد الحكومة بقناة للتراسل المترابط المتسق بشأن قضايا الأمن السيبراني. وفي وجود فريق وطني واحد، يكون لدى الإدارات الحكومية مصدر للمعلومات التقنية لدعم مجالاتها الوظيفية كل على حدة. وأخيراً، فإن الفريق الوطني يستطيع إذكاء النقاش حول الأمن السيبراني وتسهيل التعاون الدولي بشأن هذه القضية. وربما تقتضي اعتبارات معينة في بعض البلدان وجود عدة أفرقة وطنية، أو حتى توزيع قدرة إدارة الحوادث على عدة مؤسسات، وقد يكون ذلك ملائماً تماماً. وتتيح هذه الوثيقة إرشادات أياً كان الشكل التنظيمي المطبق تعييناً.

وينبغي تأسيس قدرة فريق وطني معني بالاستجابة للحوادث الحاسوبية وتشغيلها وفقاً لمبادئ أساسية معينة. وتعين هذه المبادئ القادة على اتخاذ قرارات مقابل الموارد المحدودة والمشاكل التي تكون في كثير من الأحيان معقدة. والمبادئ الأساسية بالنسبة إلى قدرة الإدارة الوطنية هي:

- الامتياز التقني. ينبغي أن تكون قدرة الفريق الوطني على أحسن نحو يمكن تطويره في ظل الموارد المتاحة. وهذا مهم لأن الفريق الوطني يجتهد في احتلال مكانة القائد الموثوق في مجال قضايا الأمن الحاسوبي على مستوى البلاد. وربما تكون

[22] انظر **الملحق باء** للاطلاع على مزيدٍ من الموارد المتعلقة بتهيئة الوعي الظرفي وإدارة الحوادث.

[23] انظر **الملحق جيم** للاطلاع على موارد إضافية لدعم الاستراتيجية الوطنية للأمن السيبراني.

نقطة الاجتهاد في تحقيق الامتياز بدهية، إلا أن لها مقتضيات معينة في سبيل بناء قدرة في ظل مقيدات الموارد. فهي تقتضي، على سبيل المثال، تفضيل بناء قدرة واحدة أو اثنتين بشكل فائق على محاولة تكوين مجموعة من القدرات دون توافر ما يلزم لذلك من موظفين وتمويل. فينبغي أن يكون التركيز على الكفاءة التقنية.

- الثقة. يكاد يكون من الحتمي بحكم التعريف أن يتعامل الفريق الوطني مع معلومات حساسة أو من شأنها أن تسبب حرجاً لأصحاب المصلحة. فيجب إذاً اكتساب الثقة والحفاظ عليها. ويمثل حسن التعامل مع المعلومات السرية وحمايتها مكوناً مهماً لبناء هذه الثقة وإدارتها.
- كفاءة الموارد. المقصود بكفاءة الموارد توظيف الموارد المتاحة بشكل فعال. وسيخضع هذا الاعتبار للتناول بمزيدٍ من التفصيل لاحقاً، لكنه يقتضي تقييماً مستمراً لتبين التهديدات والحوادث التي تشكل أهمية فعلية بالنسبة إلى الاستراتيجية العامة الفريق الوطني وبالنسبة إلى المجتمع الذي يخدمه كذلك.
- التعاون. ينبغي للفريق الوطني التعاون على أشمل وجه ممكن مع أصحاب المصلحة في البلاد ومع أفرقة وطنية في بلدان أخرى أيضاً من أجل تبادل المعلومات وتنسيق حل المشاكل التي تكون في كثير من الأحيان معقدة للغاية.

ومن المقومات الرئيسية لنجاح الفريق الوطني أن يحظى برعاية وموارد بشكلٍ وافٍ. والمقصود من أهداف التمكين الواردة هنا مساعدة الجهة الراعية لقدرة إدارة الحوادث الوطنية على بناء هذه القدرة على أقوى وجه ممكن. ويجدر النظر في أهداف التمكين التالية في معرض التخطيط لقدرة إدارة الحوادث الوطنية وتكوينها.

هدف التمكين: تحديد الجهات الراعية والمستضيفة

ينبغي أن تحدد الجهة الراعية للفريق الوطني جهات رعاية أخرى وجهات استضافة محتملة للفريق الوطني. وقد تتمكن جهات الرعاية الأخرى من توفير مزيدٍ من التمويل والدعم لمشروع الفريق الوطني. كما يجب بطبيعة الحال تحديد مقر مادي – أو جهة مستضيفة – للفريق الوطني. وقد تولت هذه الاستضافة في بعض البلدان مؤسسات أكاديمية. وكثر استضافة جامعات للأفرقة الوطنية نظراً للاتساق البالغ بين رسالة الجامعة الأساسية – ألا وهي خدمة المجتمع وإجراء أبحاث وتحليلات عل مشاكل صعبة – مع رسالة الفريق الوطني. ومع ذلك ففي حالة استضافة جامعة للفريق الوطني، ربما لا يتاح له موارد كافية أو صلاحية إنفاذ الإجراءات، بل يحقق نجاحه في هذه الحالة عن طريق التأثير في آخرين من خلال أعماله المحمودة.

وقد تهتم مؤسسات وجهات حكومية مختلفة بدعم الفريق الوطني أو استضافته. وبينما تلقى أي مساعدة الترحيب، فإن تلقي دعم من مجموعة معينة من أصحاب المصلحة قد يحمل في طياته أسباب تعثر. وينبغي أن يكون الفريق الوطني مكرَّساً لخدمة المجتمع بأكمله دون انحياز ولا محاباة لأحد أصحاب المصلحة دون غيره. ومن شأن تلقي الفريق الوطني دعماً من كيان يرتبط ارتباطاً وثيقاً بأحد أصحاب المصلحة أو إحدى الصناعات تعييناً أن يقيد قدرته المتصورة على خدمة المجتمع بأكمله. وينبغي النظر في هذا الاحتمال، على سبيل المثال، في حالة تولي مؤسسة ربحية معينة تشغيل فريق وطني. وفي حالات أخرى، من شأن اضطلاع مؤسسات رعاية معينة بدور في ذلك أن يثبط مستفيدين أساسيين عن تقاسم المعلومات. فقد يحجم بعض المستفيدين، على سبيل المثال، عن تقاسم المعلومات إذا كانت جهة رعاية الفريق الوطني الرئيسية إحدى مؤسسات إنفاذ القانون. وعلاوةً على ذلك، ينبغي أن تكون الجهة المستضيفة للفريق الوطني ممولة بشكل كافٍ لضمان الاستقرار المالي من أجل استمرارية العمل.

هدف التمكين: تحديد القيود

ينبغي للجهة الراعية أن تحدد القيود التي من شأنها أن تحد من تكوين الفريق الوطني وتشغيله. ومن القيود المعتادة الميزانية وتوافر الموظفين المهرة والبنية التحتية المتاحة لدعم عمليات الفريق الوطني. ولمسألة القيود أثر بالغ في تمكن الحكومة الوطنية من تكوين قدرة إدارة الحوادث، وتكون في العادة محركاً رئيسياً للقرارات التي تتخذ بشأن اختيار الخدمات التي ستقدم للمجتمع. فربما لا يكون من العملي أو المستحسن، على سبيل المثال، تكوين قدرة خاصة بتحليل البرامج الضارة أو الفحص العميق للرزم لدى الفريق الوطني. وقد تملي القيود اتباع نهج يتسم بمزيدٍ من الواقعية ويتمثل في تكوين علاقات مع مؤسسات أخرى محلية أو دولية لديها تلك القدرة.

وتتعلق القيود تعلقاً شديداً بثلاثة من مبادئ التشغيل الأساسية المبينة أعلاه، ألا وهي الامتياز التقني والثقة وكفاءة الموارد. فالامتياز التقني يتطلب فهماً واضحاً لما يتاح من الموظفين والتمويل من أجل دعم أنشطة معينة للفريق الوطني. وقد يقتضي ذلك التركيز على بضعة خدمات أساسية تنفذ بإتقان بدلاً من محاولة تقديم مجموعة واسعة من الخدمات. ومن شأن القيود كذلك أن تزيد إلى حدٍ بعيد من أهمية التمكن من تنسيق إدارة الحوادث بدلاً من محاولة استيفاء جميع مهام إدارة الحوادث داخلياً. ويتطلب اكتساب ثقة الفاعلين الرئيسيين استقراراً تشغيلياً وتوظيفياً، علاوةً على التمكن من حماية المعلومات الحساسة – وكل ذلك يتأثر بشكل مباشر بمحدودية الموارد. وأخيراً، تتطلب كفاءة الموارد إدراك ما هي الموارد المتاحة.

هدف التمكين: تحديد هيكلية الفريق الوطني المعني بالاستجابة الحوادث الحاسوبية

من الممكن تشغيل الفريق الوطني، في ضوء وظيفته في مجال الأمن السيبراني الوطني، بأشكال متعددة، منها شكل الوكالة المستقلة ذات الشراكات التشغيلية المحدودة وشكل المشروع المشترك مع موفري الاتصالات الوطنيين وشكل التبعية الضمنية للاستراتيجية الوطنية الدفاع العسكري. ويجب النظر في عددٍ من العوامل ضماناً لحسن هيكلة وظائف الاكتشاف والتنسيق في الحوادث والاستجابة لها هيكلةً ملائمة. والمقصود من الاعتبارات الهيكلية المذكورة فيما يلي أن تكون استرشادية لا شاملة:

- ما هو المستوى الحكومي الذي يدار عليه الفريق الوطني؟
- ما هي الجهة الممولة للفريق الوطني وما هي الجهة التي تعتمد ميزانيته؟
- هل يوجد كيان مستقل يشرف على الفريق الوطني؟
- ما هي مجموعة الأدوار والمسؤوليات التي حُددت لشركات تشغيل الفريق الوطني؟

كما توجد عدة اعتبارات من شأنها أن تفيد في البت في مسألة الشكل التنظيمي، علاوةً على المبادئ الأساسية:

- ما هي الهيكلية التي تسمح للفريق الوطني بالتخفيف من قلق أصحاب المصلحة بشأن تقاسم المعلومات على أحسن وجه؟ هل توجد أي هيكليات تنظيمية محتملة من شأنها أن تحد من قدرة الفريق الوطني المتصورة على خدمة مجتمعه دون انحياز؟
- هل من شأن أشكال هيكلة أنظمة البلاد وبنيتها التحتية أن تجعل من المفيد وجود عدة أفرقة وطنية من حيث تقاسم المعلومات أو إعداد تقارير بشأن العلاقات؟
- في حالة تكوين أفرقة وطنية متعددة، كيف ينبغي تقاسم المعلومات بينها؟ وهل يحتمل أن تعجز الأفرقة الوطنية المتعددة عن تقاسم المعلومات بشكل فعال عبر قطاعات البنية التحتية؟ وما هي تكاليف المعاملات المقترنة بوجود مؤسسات متعددة؟ وكيف توزن مقابل فوائد المقياس في حالة وجود فريق وطني واحد؟[24]
- هل لمختلف الأشكال التنظيمية المحتملة أي مقتضيات من حيث التوظيف وإدارة رأس المال البشري؟

هدف التمكين: تحديد صلاحيات الفريق الوطني المعني بالاستجابة الحوادث الحاسوبية

يجب على الجهة التي يتبعها الفريق الوطني أو التي ترعاه البت في منح الفريق الوطني صلاحية حظر أو فرض إجراءات أو تدابير أمنية معينة من عدمه. وقد تنطوي صلاحية الفريق الوطني على الإلزام بالإبلاغ عن الحوادث الأمنية أو اعتماد تدابير أمنية معينة

[24] ملاحظة حول العمل المشترك على الصعيد الإقليمي: قد تعتبر جهة رعاية الفريق الوطني أن تقاسم الموارد والتكاليف مع بلدان مجاورة لتكوين قدرة إقليمية لإدارة حوادث الأمن الحاسوبي يؤدي إلى تكوين "فريق إقليمي معني بإدارة الحوادث الحاسوبية". وقد يكون هذا أسلوباً فعالاً لمعالجة المشكلة المتأصلة المتمثلة في الوفاء بمتطلبات كثيرة بموارد محدودة. وتتجاوز دراسة مثل هذا الترتيب نطاق هذا التقرير، غير أن هذا الحل ينطوي على عدة تضحيات. فبما أن الفريق الوطني يتولى، فيما يتولى، الموازنة بين الحاجة إلى الاستجابة للتحديات العالمية والقانون الداخلي للبلاد وثقافتها وهيكلياتها الوطنية، فقد تضعف قدرة الفريق الإقليمي على تحقيق قيمة لبلدان متعددة. ثم أن الأمن السيبراني يشكل جزءاً من الاستراتيجية الأمنية العامة لأي بلد، مما قد يضع بين أيدي الأفرقة الإقليمية معلومات لها تبعات مهمة بالنسبة إلى الأمن القومي. وقد تكبل أيدي الفريق الإقليمي عن الحصول على هذه المعلومات من بعض أصحاب المصلحة الوطنيين نظراً لشواغل تتعلق بتقاسم هذه المعلومات في محفل متعدد الأقطار. وعلى أي حال، فإن نجاح أي فريق إقليمي من هذا النوع يتطلب درجة عالية من الارتياح والألفة بين البلدان – أو هيكلية إدارة متعددة الأقطار فعالة.

أو كلا الأمرين. وعلاوةً على ذلك، من الوارد أن تختلف صلاحية الفريق الوطني اعتماداً على تعامله مع مواطنين أفراد وصناعات أو إدارات حكومية. وقد يكون من الملائم تماماً أن يحتفظ الفريق الوطني أو الجهة التي ترعاه سلطة على إدارات حكومية مختلفة دون أن يكون له أي سلطة على آحاد المواطنين.

وبينما تتخذ هذه القرارات بما يتسق مع قوانين البلاد وثقافتها، فكثيراً ما يحدث أن يعمل الفريق الوطني بشكل أكثر فعالية عندما يكون دوره استشاري محض، حيث يكون أصحاب المصلحة الرئيسيين على الصعيد الوطني أكثر استعداداً لتقاسم المعلومات ومناقشة مواطن الضعف الأمني بشكل كامل، بل وأقدر – حسب البيئة القانونية – على ذلك، إذا كان المحفل ذا طابع تعاوني لا يكون الفريق الوطني فيه كياناً تنظيمياً أو مانعاً.

هدف التمكين: تحديد خدمات الفريق الوطني المعني بالاستجابة الحوادث الحاسوبية

يتمثل الحد الأدنى من الوظائف الأساسية للفريق الوطني في القدرة على الاستجابة لتهديدات الأمن السيبراني وحوادثه التي تشكل أهمية لأصحاب المصلحة الوطنيين. وتنفذ الأفرقة الوطنية المختلفة القائمة حالياً مجموعة متنوعة من الوظائف من بينها ما يلي:

خدمات التعامل مع الحوادث	تقييمات مواطن الضعف
تحليل الحوادث	خدمات بحثية
خدمات تحريات جنائية	تدريب/تثقيف/توعية
خدمات رصد الشبكات	تنسيق الاستجابات
تحليل البرمجيات الضارة	

وتكون هذه الوظائف محدودة على المستوى الوطني بالقيود المبينة في هدف التمكين 2.1.3 (التمويل والقوة العاملة والموارد المادية على سبيل المثال). ويجب على الجهة الراعية للفريق الوطني تحديد الأنشطة الواقعية من بين هذه المذكورة في ضوء القيود القائمة. ويكون أقوى القيود في العادة رأس المال البشري (أي القوة العاملة). ولأن الفريق الوطني يؤدي دور القائد على الصعيد الوطني في مجال إدارة حوادث الأمن السيبراني وتحليلها، فينبغي أن يكون المبدأ الموجه لاختيار وظائف معينة هو الامتياز. وقد يكون أفضل سبيل لأي فريق وطني بعينه كي يستوفي دوره ما كان من خلال التنسيق الوثيق مع أفرقة وطنية أخرى لديها قدرات تقنية أعلى، أو قد يكون لديها بالفعل قنوات تواصل موثوقة.

هدف التمكين: تحديد أصحاب مصلحة إضافيين

ينبغي لجهة رعاية القدرة الوطنية لإدارة الحوادث تبين المؤسسات الأخرى التي يحتمل أن تقدم مدخلات أو يكون لها مصلحة في إنشاء فريق وطني يعنى بالاستجابة للحوادث الحاسوبية. وتظهر في القسم الثاني من هذه الوثيقة قائمة مفصلة بأصحاب المصلحة التقليديين في السياسات الوطنية المتعلقة بالأمن السيبراني. وإضافة إلى ذلك، من الوارد أن يهتم بعض أصحاب المصلحة بأداء دور أنشط في تكوين الفريق الوطني وتشغيله. ويكون من هؤلاء في العادة:

- جهاز إنفاذ القانون
- موردو التكنولوجيا
- مستخدمون حكوميون (وكالات ووزارات حكومية وما إلى ذلك)
- مجتمعات بحثية
- جهات إدارة.

وينبغي للفريق الوطني أن يدرك الكيفية التي يكمل أصحاب المصلحة المحددون بها عمليات الفريق الوطني ويندمجون فيها، وأن يضع خطة لضمان تصميم التواصل ثنائي الاتجاهات ضمن عملياته.

الهدف الاستراتيجي: تهيئة الوعي الظرفي المشترك

تتمثل الوظيفة الأساسية للفريق الوطني في القدرة على إدارة تهديدات الأمن السيبراني وحوادثه التي تشكل أهمية لأصحاب المصلحة الوطنيين. ويعين تحقيق الامتياز في إدارة الحوادث الفريق الوطني على تكوين علاقات مع أصحاب المصلحة وتحقيق أهداف استراتيجية أخرى، مثل دعم الاستراتيجية الوطنية للأمن السيبراني. وتتمثل الخطوة الأولى في إدارة الحوادث في تهيئة فهم أو وعي بمن هم المستفيدون الرئيسيون للفريق الوطني وما هي أنواع الأنظمة التي يستخدمونها (تكنولوجيا المعلومات والاتصالات) وما هي أنواع الحوادث التي تواجههم. ويشار إلى هذا الفهم العام في العادة بمسمى الوعي الظرفي المشترك.

ومن شأن إحجام المجتمع عن إبلاغ الفريق الوطني بالحوادث أن يؤدي إلى إهدار ما اجتمع له من الموظفين ولو كانوا أقدرهم ومن البنية التحتية التقنية ولو كانت أفضلها. ولذلك فإن أول أهداف التمكين يركز على هذه القضية.

هدف التمكين: تكوين علاقات قائمة على الثقة والحفاظ عليها

تجمع الأفرقة الوطنية معلومات حساسات عن مشاكل المستفيدين على الصعيد الوطني وشواغلهم ومواطن الضعف لديهم. وهي تستخدم هذه المعلومات في كثير من الأحيان لاستخلاص دروس مستفادة ونشر تقارير إعلامية، وهذه عملية تحمل في طياتها المخاطرة بكشف معلومات أكثر مما ينبغي إذا لم تنفذ بعناية. كما تنشر الأفرقة الوطنية لأصحاب المصلحة معلومات عامة عن التهديدات ومواطن الضعف وأفضل الممارسات. ويقتضي تبادل المعلومات ثنائي الاتجاه هذا تكوين علاقات قائمة على الثقة مع أصحاب المصلحة، حيث إن من شأن انعدام التيقن من حماية المعلومات الحساسة وتصنيفها بشكلٍ وافٍ أن يؤدي إلى إحجام أصحاب المصلحة عن تقاسم معلوماتهم الحساسة التي تمثل للفريق الوطني أهمية حاسمة. ويمكن القول ببساطة أن إدارة الحوادث الأمنية تصعب إذا أحجم الضحايا عن إبلاغ الفريق الوطني بها.

ويكتسب الفريق الوطني إمكانية النفاذ إلى المعلومات التي لا غنى لعملياته عنها من خلال تكوين علاقات وشراكات مع مالكي البنية التحتية الحاسمة ومشغليها وغيرهم من المستفيدين الأساسيين. وتقام هذه العلاقات والشراكات مع الفريق الوطني مباشرة وفيما بين المستفيدين كذلك. ومن الممكن أن يؤدي الفريق الوطني دور قناة التواصل الموثوقة بين المستفيدين الأساسيين.

ويمثل ضمان سرية معلومات أصحاب المصلحة مشكلة تأمين معلومات. وهذا يتطلب إجراء تقييمات مخاطر أمنية على مستوى الفريق الوطني وتنفيذ التوصيات الناتجة. وتتراوح سياسات تعزيز تأمين المعلومات من التحري عن الموظفين على نحوٍ سليم إلى إلزام الموظفين بالتوقيع على اتفاقات امتناع عن الكشف وما شابه ذلك من الوسائل القانونية، مما يجعل الحفاظ على السرية شرطاً للتوظف. ومن السبل الأساسية الأخرى لضمان حصر النفاذ إلى المعلومات على الأشخاص الذين يحتاجون إليها لتأدية المهام المنوطة بهم تصنيف المعلومات على مستويات سرية مختلفة. وبغض النظر عما يطبق من التدابير والسياسات الأمنية المحددة، ينبغي على الفريق الوطني معالجة شواغل أصحاب المصلحة في هذا المجال بشكل استباقي وأن يلتزم أقصى درجات الشفافية الممكنة بشأن الخطوات الأمنية المتخذة. وتضم هذه السلسلة لاحقاً تناولاً بمزيدٍ من التفصيل للسياسات التي تسهل تقاسم المعلومات وتأمينها في بيئة فريق وطني معني بالاستجابة للحوادث الحاسوبية.

هدف التمكين: تنسيق تقاسم المعلومات بين المستفيدين المحليين

من أهم العوامل في تكوين قدرة وطنية تسهيل تقاسم المعلومات بشكل موثوق وفعال. ومن الأدوار الأساسية التي يؤديها الفريق الوطني الحصول على معلومات عن الحوادث من المجتمع ثم العودة عليه بنشر معلومات متعلقة بالاستجابة في توقيت مناسب وبشكل وجيه. ويتضمن هذا النوع من المعلومات بشكل عام ما يلي:

- المعلومات الواردة بشأن الحوادث الأمنية والمجمعة من خلال وسائل متنوعة
- نشرات أمنية تضم معلومات توعوية بشأن التهديدات ومواطن الضعف السيبرانية
- إنذارات وتنبيهات سيبرانية عامة ومحددة وعاجلة (تقنية وغير تقنية)
- أفضل الممارسات لمنع المشاكل والأحداث والحوادث السيبرانية
- معلومات عامة عن الفريق الوطني (مثل الهيكل التنظيمي للفريق والجهات الراعية له والخدمات التي يقدمها وبيانات الاتصال بالهاتف أو البريد الإلكتروني وغير ذلك).
- موارد ومواد مرجعية (مثل الأدوات الأمنية والمؤسسات الشريكة).

ويمكن استخدام المعلومات التي يجمعها الفريق الوطني من أجل الحد من المخاطر عن طريق تقديم الدعم للمؤسسات التي تعرضت لهجمات. وقد يتخذ هذا الدعم شكل الدعم التقني المباشر أو قد ينطوي على العمل مع أطراف ثالثة التماساً لإصلاحات ومعالجات، أو لتوعية الجماهير والصناعات الخاصة. ومن المقومات الرئيسية لتقاسم المعلومات عدم جواز تقاسم المعلومات الحساسة الواردة من مستفيدين مع غيرهم إلا بعد طمس أي آثار معرفة للهوية منها خلال عملية التحليل وبما يتفق مع سياسات الفريق الوطني.

ويتطلب طمس الهوية استشعاراً لظروف معينة تتعلق بالحوادث الحاسوبية ذاتها أو بالمستفيدين الأساسيين. فعلى سبيل المثال، قد يحذف من تقرير منشور عن حادثة أسماء الضحايا أو الشركة المستفيدة المعنية. ومع ذلك، فإذا كان التقرير يتناول حادثة معروفة نشرت الصحافة أخبارها فقد تفشل محاولات حماية السرية. ومن المبادئ الأساسية في حماية المعلومات الامتناع عن تعميم معلومات أو نشر تقارير إلا بعد الحصول على موافقة الأطراف المعنية.

ومن المكونات الرئيسية لتقاسم المعلومات حيازة أدوات وأساليب وطرائق تتيح للفريق الوطني التواصل مع مجتمعه. ومن أمثلة ذلك ما يلي:

- موقع إلكتروني لتناقل المعلومات ونشرها على المستويين العام (متاح لنفاذ عموم الجماهير) والحساس (بوابة مؤمَّنة تتطلب استيقاناً) بين الفريق الوطني ومجتمعه.
- قوائم بريدية ونشرات إعلامية وتقارير وتوجهات تحليلية
- تنفيذ شبكات معلومات مؤمَّنة لعمليات الفريق الوطني.

هدف التمكين: دمج معلومات المخاطر الواردة من المجتمع

تستفيد الأفرقة الوطنية من المعلومات المتقاسمة بشكل مفتوح من الصناعات الخاصة والهيئات الأكاديمية والجهات الحكومية. فعندما تجري المؤسسات تقييمات مخاطر وافية ثم تتقاسم النتائج مع الفريق الوطنية، يزداد الوعي الظرفي. ومن شأن معلومات المخاطر الواردة من المجتمع أن تعين الفريق الوطني على فهم الأثر المحتمل لمواطن الضعف الأمني ومشاكل الأنظمة في أصول وبنية تحتية مهمة، مما يساعد الفريق الوطني في رفع مستوى التركيز لعملية إدارة الحوادث التي يطبقها وتحسينها.

ويكون الفريق الوطني في معرض أداء دوره المتمثل في الاستجابة للحوادث مساهماً أساسياً في تكوين الوعي الظرفي. ومن خلال تحليل التوجهات في الحوادث التي تخضع للإدارة، يكتسب الفريق الوطني مزيداً من الإدراك لوضع الأمن السيبراني ضمن المجتمع الذي يخدمه. ويوظف الفريق الوطني هذه المعرفة ومنظوره الخاص بشأن المشاكل من أجل إعداد صورة صادقة وواقعية للوعي الظرفي على الصعيد الوطني. وهذا يعين الفريق الوطني على وضع استراتيجيات دفاعية استباقية، علاوةً على ما يلزم إجراؤه من تحسينات في الممارسات والسلوكيات ضمن المجتمع.

هدف التمكين: جمع معلومات حول حوادث الأمن الحاسوبي

يجب أن يكون أي فريق وطني يعنى بالاستجابة للحوادث الحاسوبية قادراً على جمع معلومات حول حوادث الأمن الحاسوبي وأحداثه، وذلك عن طريق تلقي بلاغات عن حوادث مشتبه فيها أو مؤكدة تتطلب تنسيقاً أو استجابة. وتجمع هذه الأفرقة الوطنية معلومات حول الحوادث من خلال وسيلتين أساسيتين، هما علاقات الثقة التي يقيمها والبنية التحتية التقنية اللازمة لمعالجة البلاغات الواردة. وبينما يتخذ الإبلاغ عن الحوادث في كثير من الأحيان الشكل الطوعي وتسهله الثقة، فقد يكون إلزامياً في بعض الحالات.

ويتلقى الفريق الوطني بلاغات عن حوادث الأمن الحاسوبي من خلال وسائل تقنية متنوعة، ومن أمثلة ذلك الخطوط الساخنة التي تعمل على مدار الساعة والبوابات الإلكترونية. ومن الممكن إتاحة النفاذ إلى البوابات الإلكترونية من أي حاسوب لعموم الجماهير أو تأمينها من أجل تبادل معلومات حساسة. ويتطلب إثبات البلاغات المتعلقة بحوادث الأمن الحاسوبي من المجتمع اكتشاف الأنشطة غير الطبيعية وتبينها وتتبعها من خلال استخدام طرائق تقنية وأخرى غير تقنية. ويُعرَّف النشاط غير الطبيعي على أنه نشاط ينحرف عن عرفٍ ما موضوع لتشغيل النظام. وفي كثير من الحالات، قد يستلزم جمع معلومات عن حوادث الأمن الحاسوبي أولاً تثقيف المجتمعات بشأن اكتشاف هذا النوع من الأنشطة.

الهدف الاستراتيجي: إدارة الحوادث

يحظى الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية، بحكم أدائه دور نقطة الاتصال الموثوقة بشأن الأمن السيبراني على الصعيد الوطني، بمكانة فريدة من القدرة على إدارة الحوادث التي تثير الاهتمام في البلاد. ولتحقيق ذلك، ينمي الكثير من هذه الأفرقة الوطنية قدرات نشطة معينة مثل الاستجابة للحوادث واحتوائها وإعادة تكوين الخدمات. ومن المهم تذكر أن الفريق الوطني في كثير من الحالات لن يتولى معالجة جميع الحوادث وتحليلها بنفسه. فقد يؤدي الفريق الوطني دوراً تسهيلياً وتنسيقياً للتحليل والاستجابة، ويكون ذلك بسبب محدودية الموارد أو بسبب وجود المعرفة بالمشكلة المعنية تحديداً لدى جهة أخرى، كأن تكون لدى فريق وطني آخر أو أحد موردي التكنولوجيا.

هدف التمكين: تحديد الحوادث والتهديدات محل الاهتمام على الصعيد الوطني

في ظل شح الموارد، ربما يكون تحديد الحوادث والتهديدات التي تهم الفريق الوطني أصعب مهمة تواجهه. وتتسم عملية تبين المواضع التي ينبغي للفريق الوطني تركيز انتباهه عليها بالتدرج والتطور. ويجد الفريق الوطني نفسه عقب التشكيل الأولي لقدرة إدارة الحوادث في مواجهة سيل جارف من الأسئلة وطلبات المساعدة، مما يحتم على الفريق الوطني الموازنة بين شح الوقت والموارد من جهة ورغبته في خدمة المجتمع وتكوين علاقات مع أصحاب المصلحة من جهة أخرى.

ويمكن للجهة الراعية خلال عملية تكوين قدرة الفريق الوطني الاستعانة بعدد من الموارد على تحديد مجالات التركيز الأولية للفريق الوطني، ومن ذلك:

- أنظمة المعلومات والحوادث التي تؤثر في قطاعات البنية التحتية الحاسمة المحددة في السياسة الوطنية للأمن السيبراني، إن وجدت. وينبغي أن يكون هذا المحرك الأساسي خلف مجالات تركيز الفريق الوطني. ويمثل توفير الإرشاد للفريق الوطني أحد الأسباب الرئيسية لوجود سياسة وطنية منسقة.
- الحوادث والتهديدات لتي من شأنها التأثير في أنظمة قطاع واحد أو أكثر من قطاعات البنية التحتية الحاسمة.
- أنواع الحوادث أو الأنشطة التي قد تثير قلق السلطات الوطنية بشكل خاص لاحتمال تأثيرها بشكل مباشر في الأمن القومي أو أدائها إلى كشف معلومات حساسة أو جلبها حرجاً على البلاد أو بسبب عوامل فريدة أخرى.
- الحوادث التي تؤثر بشكل كبير في أغلبية مستخدمي الحواسيب في عموم الجماهير.
- معارف موظفي الفريق وخبراتهم.
- أنواع التهديدات التي يعتبرها محللو الحوادث ضمن الفريق الوطني أو مجتمع الاستجابة للحوادث جزءاً من تهديدات أكبر أو متطورة.
- المعارف والحنكة المستفادة من أفرقة وطنية أخرى.

ومن شأن الوعي بالأنظمة المستخدمة حالياً لدى مستفيدي الفريق الوطني الأساسيين أن يعين الفريق على تركيز تحليلاته للحوادث. ويتراكم هذا الوعي مع مرور الزمان من خلال معالجة الحوادث والتفاعل مع المجتمع.

هدف التمكين: تحليل حوادث الأمن السيبراني

يجب أن تحوز جميع الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية القدرة على الاستجابة للحوادث السيبرانية وتزويد المجتمع بتحليلات ودعم. ولا يتصور أن تحوز جميع الأفرقة الوطنية نفس المجموعة من القدرات المحددة لأداء هذا العمل. فعلى سبيل المثال، لن تحرز جميع الأفرقة الوطنية نفس المستوى من الشراكات الخارجية مع خبراء تكنولوجيا المعلومات ومجتمعات تطوير البرمجيات وباحثي المجال الأمني، ولن يكون لدى جميع الأفرقة الوطنية أفرقة داخلية تتولى تنفيذ تحليلات على مستوى لغة البرمجة للبرمجيات الضارة والبرمجيات العادية ومضاهاة الهجمات والخروقات. ومع ذلك، ينبغي كحد أدنى أن تحلل الأفرقة الوطنية بلاغات المشاكل التماساً لخصائص مشتركة لتبين أهميتها وقياس مستوى التهديد الذي تمثله المشكلة بدقة. وقد تتضمن تلك الخصائص المشتركة أشياء مثل وسيط الهجوم وأهداف الهجمات. وقد تنطوي هذه الخصائص المشتركة في بعض الحالات على معلومات محددة للهوية أو للمصدر من شأنها أن تفيد الجهات الأمنية الوطنية.

هدف التمكين: تطوير عملية تدفق عمل فعالة

لا مناص لأي فريق وطني يعنى بالاستجابة للحوادث الحاسوبية من تلقي معلومات من مصادر متعددة بشأن تلك الحوادث. وقد يكون ورود هذه الإخطارات عبر البريد الإلكتروني أو نماذج إلكترونية على الإنترنت أو الهاتف أو الفاكس أو عملية مؤتمتة (بمعنى الإخطار بالأحداث من أنظمة معلوماتية مؤتمتة أو محاسيس). وينبغي توقع ورود بلاغات شخصية (أي تلك الواردة من أفراد لا من أنظمة معلومات) من مصادر معروفة وغير معروفة. ومن المصادر المعروفة شركاء التشغيل وشبكات تقاسم المعلومات والأعضاء الموثوقين في صناعة خاصة وأصحاب المصلحة الحكوميون وخبراء معتبرون في مجال التخصص (باحثون وعلماء وما شابه). وأما المصادر غير المعروفة فمنها البلاغات الواردة من مواطنين ومن مؤسسات أخرى غير مرتبطة بأي علاقة. ومن أمثلة ذلك "الخط الساخن"، وهو رقم هاتف منشور أو خدمة تراسل فوري معلن عنها مما يتيح لجميع الأطراف إبلاغ الفريق الوطني بالحوادث على مدار اليوم والسنة. وتتنوع هذه الحوادث في خطورتها وأهميتها.

وينبغي للفريق الوطني كي يتعامل مع البلاغات بكفاءة وإنصاف أن يضع عملية واضحة ومتسقة لتدفق العمل. ومن الخطوات التقليدية في هذا المضمار ما يلي:

- اكتشاف الحوادث.
- جمع أدلة الحوادث وتوثيقها.
- تحليل الأحداث وتصنيفها.
- الاستجابة للحوادث والتعافي منها.
- التعلم من الحوادث.

هدف التمكين: إنذار المجتمع

يصدر الفريق الوطني إنذارات للمجتمع لعدد من الأسباب. ويتيح الإنذار بتهديدٍ ما في التوقيت المناسب تحقيق الحماية الاستباقية للأنظمة علاوةً على التعافي من الحوادث. وتؤدي الإنذارات والتنبيهات إلى رفع قدرة المستفيدين المتأثرين على الاستعداد لمجابهة الهجمات واكتشاف التهديدات ومواطن الضعف، مما يحد من الأثر المحتمل للمخاطر. ومن شأن إنذار المجتمع بشأن المشاكل ذات الصلة أن ينمي علاقات قويمة ويعزز ممارسات خاصة من أجل تحقيق الوعي الظرفي. ومن شأنه كذلك أن يبرهن على فائدة "القيمة المضافة" التي تجنى من الفريق الوطني.

ويوظف الفريق الوطني علاقاته مع أصحاب المصلحة وأفرقة وطنية خرى، علاوة على ما يجمع من بلاغات بحوادث وتحليلاته لها، في سبيل التعرف على التهديدات ومواطن الضعف وتبين المعلومات التي يلزم توزيعها على المجتمع. ويجب على الفريق الوطني تصميم إنذاراته على نحوٍ يحقق غرض إعلام أفراد المجتمع وتشجيعهم على التحرك دفاعاً عن أنفسهم. ومع ذلك فيتعين على الفريق الوطني الموازنة بينَ الحاجة إلى نشر المعلومات بسرعة وحساسية المعلومات ونسق الإنذار. ويجب إرسال هذه الإنذارات إلى المجتمع بشكل يقيم فيها الصدق والنزاهة والخصوصية متى ما لزمت. وعلاوةً على ذلك، تتطلب بعض الإنذارات إخفاء هوية مصدر المعلومات، خاصة إذا وردت المعلومات المتعلقة بالتهديد من مصدر استخباراتي. ويجب التزام الحيطة ضماناً لتقاسم المعلومات ذات الصلة بالتهديدات بفعالية مع حجبها في نفس الوقت عمن لا تلزمه معرفتها. ويعمد الكثير من الأفرقة الوطنية إلى إزالة المعلومات التي من شأنها الإفصاح عن مصدر البيانات المتعلقة بالتهديدات ومواطن الضعف، حيث تقصر البيان على موطن الضعف المكتشَف أو تخفي بيانات محددة متعلقة بالتهديدات.

وتكون الإنذارات الواردة من الفريق الوطني إلى أصحاب المصلحة والمجتمع الوطني بشكل عام أكثر فعالية إذا أرسلت من خلال قنوات تواصل موثوقة وسرية سبقت إقامتها بالفعل. وقد تتخذ هذه "القنوات" شكل أفراد معينين أو مكاتب معينة في مؤسسات أساسية. وقد ثبت أن العمل من خلال آليات تواصل سرية مقامة سابقاً يمثل استراتيجية ناجحة للغاية لبناء علاقات ثقة. وتتفق الأفرقة الوطنية وأصحاب المصلحة والمستفيدون الرئيسيون ذوي الصلة على طريقة التواصل وشروط معالجة المعلومات وغير ذلك من أوجه الحماية باعتبار ذلك كله أساساً لعلاقات الثقة. ويرتبط هدف التمكين هذا ارتباطاً وثيقاً بإقامة قنوات اتصال موثوقة.

هدف التمكين: تعميم أفضل ممارسات الأمن السيبراني

يجمع الفريق الوطني معلومات عن المشاكل الأمنية من خلال سبل متنوعة، ويشكل ما يجتمع لديه من معرفة تاريخية مصدراً ممتازاً لما يعرف باسم "الدروس المستفادة". ومن شأن الدروس المستخلصة من الحوادث أن تشكل أساساً لتنمية المهارات الموجهة والوعي الأمني العام. وعلاوةً على ذلك، كثيراً ما تؤدي هذه الدروس المستفادة إلى تحسين الوعي الظرفي والاستفادة من إدارة المخاطر السيبرانية بشكل عام. ومن الممكن أن يعلن الفريق الوطني عن أفضل الممارسات التي قننها من خلال نشر وثائق عامة عن أفضل ممارسات الأمن السيبراني وإرشادات الاستجابة للحوادث ومنعها والتدريب والإجراءات التنظيمية الموصى بها ودراسات الحالة المنشورة عن اعتماد الممارسات. فعلى سبيل المثال، يمكن للفريق الوطني أن يعِد ممارسات فضلى بشأن:

- كيفية تأمين تكنولوجيات محددة من هجمات وتهديدات أمن سيبراني معروفة.
- كيفية تطوير خطط وإجراءات وبروتوكولات للاستجابة في حالات الطوارئ واختبارها والتدرب عليها.
- كيفية التنسيق مع الفريق الوطني بشأن الأبحاث الأمنية (مثل تبين مواطن الضعف وتحليل الأسباب الجذرية والأبحاث المجتمعية المتعلقة بالتهديدات والهجمات).

الهدف الاستراتيجي: دعم الاستراتيجية الوطنية للأمن السيبراني

يمثل الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية مكوناً تشغيلياً مهماً في النهج القومي لتنفيذ استراتيجية الأمن السيبراني. فالفريق الوطني يشارك ضمن سياق أوسع للإدارة الوطنية للحوادث ضد مجموعة متنوعة من التهديدات (أي الصناعية والطبيعية، المادية والسيبرانية). ويمكن الاستفادة من الفريق الوطني في:

- الوقوف على المتطلبات الاستراتيجية الإضافية الخاصة بالأمن السيبراني على الصعيد الوطني
- تحديد ما يلزم من ممارسات تقنية وتحسينات تعليمية وتنمية مهارات للممارسين في مجال الأمن السيبراني وأبحاث وتطوير
- تبين فرص تحسين سياسات الأمن السيبراني وقوانينه ولوائحه التنظيمية
- تعميم الدروس المستفادة من خبرات في مجال الأمن السيبراني التي تؤثر في النهج القومي للأمن السيبراني ذاته
- تحسين قياس الأضرار والتكاليف المقترنة بالحوادث السيبرانية.

وربما يكون أهم مجال للاستفادة من الفريق الوطني في استراتيجية الأمن السيبراني هو تعزيز ثقافة أمن سيبراني وطنية. فمن خلال جمع مختلف أصحاب المصلحة، يستطيع الفريق الوطني إعانة أصحاب المصلحة على التوصل إلى فهم أفضل لقضايا الأمن السيبراني وأهمية هذا المجال بالنسبة إلى مجتمعاتهم المختلفة.

هدف التمكين: ترجمة الخبرات والمعلومات بغية تحسين إدارة الحوادث السيبرانية ووضع السياسات السيبرانية على الصعيد الوطني

بينما تواصل مؤسسات من جميع الأحجام مباشرة إدارة الحوادث السيبرانية داخلياً، فإن الفريق الوطني يتحمل وحده المسؤولية الأساسية عن معالجة الشواغل العامة على الصعيد الوطني. وتؤدي ترجمة خبرات الفريق الوطني إلى صورة تفيد صناع السياسات وأصحاب المصلحة ومجتمع الممارسين في المجال الأمني إلى تحسين الأمن السيبراني على الصعيد الوطني بشكل عام. وتقتضي ترجمة الخبرات النظر في الكيفيات التي يمكن أن يكون لعمل الفريق الوطني وخبرات المجتمع بها مقتضيات أوسع بالنسبة إلى القوانين والسياسات الوطنية. ومن شأن هذه الترجمة أن تفرز دروساً مستفادةً وأن ترفع مستوى تجنب المشاكل والحد من المخاطر على الصعيد الوطني، علاوةً على التأثير في اللوائح التنظيمية والإرشادات والمبادرات والتوجيهات على المستوى القومي.

وقد يكون من أمثلة هذه الخبرات حوادث تتعلق بمواطن ضعف تؤثر في نظام تفكر الحكومة الوطنية في نشره عبر إدارتها ووكالاتها ووزاراتها، حيث إن فهم المخاطر المتأصلة يفضي إلى البت في اعتماد تكنولوجيا معينة من عدمه. ومن الأمثلة الأخرى اعتوار شيء من الإبهام أو عدم الاتساق قانون الخصوصية على نحوٍ يعوق تقاسم المعلومات بين أصحاب المصلحة من القطاع الخاص. وتتضمن مصادر هذه الدروس المستفادة كلاً من خبرات الفريق الوطني وخبرات أصحاب المصلحة.

هدف التمكين: بناء قدرة الأمن السيبراني على الصعيد الوطني

يحظى الفريق الوطني بمكانة فريدة من حيث التمكن من أداء دور نقطة الاتصال الموثوقة على الصعيد الوطني. ويمكن للفريق الوطني توظيف ذلك التميز للتنسيق مع جميع مالكي تكنولوجيا المعلومات والاتصالات ومشغليها (من القطاع العام و/أو الخاص) في سبيل تكوين منظور متفرد في شموله لمشهد الأمن السيبراني الوطني. ويتيح هذا للفريق الوطني دعم الاستراتيجية الوطنية للأمن السيبراني وإدارة الحوادث المثيرة للاهتمام على الصعيد الوطني ودعم العمليات الحكومية بأقصى قدر من الفعالية. ويبني الفريق الوطني في العادة قدرة الأمن السيبراني عن طريق نشر أفضل الممارسات وتقديم خدمات وإرشادات وتدريب وتثقيف وتوعية لتكوين أفرقة وطنية أخرى مشابهة.

ويستطيع الفريق الوطني تنمية ثقافة أمن سيبراني على الصعيد الوطني. وينبغي تصميم منشورات الفريق الوطني وخدماته الاستشارية بحيث تبني القدرة الوطنية الجماعية، لا توجيه ذلك إلى الوفاء بحاجات تخصصية محددة. ويتعين على الفريق الوطني أن يمتنع عن العمل في سبيل تحقيق مصالح أحد أصحاب المصلحة تحديداً دون غيره. ويمكن للفريق الوطني أن يؤدي دور الجسر القيِّم بين أصحاب المصلحة وصناع السياسات الوطنية. وقد يعتمد مدى قدرة الفريق الوطني على الوفاء بهذا الدور على عوامل قانونية وهيكلية.

هدف التمكين: استثمار شراكات القطاعين العام والخاص في سبيل تحسين الوعي والفعالية

تمثل حماية البنية التحتية الحاسمة والفضاء السيبراني مسؤولية مشتركة يمكن القيام بها على خير وجه من خلال العمل المشترك بين الحكومة والقطاع الخاص، الذي يمتلك في كثيرٍ من الأحيان جزء كبير من البنية التحتية ويشغله. ويتطلب نجاح العمل المشترك بين الحكومة والصناعة ثلاثة عناصر مهمة: (1) عرض قيمة واضح و(2) أدوار ومسؤوليات تحدها خطوط واضحة و(3) تقاسم المعلومات في الاتجاهين. ويعتمد نجاح الشراكة على بيان الفوائد المتبادلة لشركاء الجهات الحكومية والصناعة. ومن بين الفوائد العائدة على جميع الشركاء:

- رفع الوعي الظرفي من خلال تقاسم المعلومات بشكل قوي ثنائي الاتجاه
- النفاذ إلى معلومات بشأن تهديدات المحيقة بالبنية التحتية الحاسمة يمكن التحرك على أساسها
- زيادة الاستقرار القطاعي المصاحب لإدارة المخاطر بشكل استباقي.

ويتطلب بناء قدرات الفريق الوطني التشغيلية والاستراتيجية مشاركة نشطة من جميع شركائه. وينبغي للجهات الحكومية والصناعة اعتماد نهج في إدارة المخاطر يتيح للحكومة والقطاع الخاص تحديد البنية التحتية السيبرانية وتحليل التهديدات وتقييم مواطن الضعف وتقدير العواقب ووضع خطط التخفيف.

هدف التمكين: المشاركة في تطوير مجموعات ومجتمعات تقاسم المعلومات والتشجيع على ذلك

تمثل مشاركة الفريق الوطني في مجموعات ومجتمعات تقاسم المعلومات سبيلاً مهماً لتحسين الوعي الظرفي وتكوين علاقات قائمة على الثقة. وينبغي في الوضع الأمثل أن يكون تقاسم المعلومات في هذا السياق ثنائي الاتجاه بين الفريق الوطني ومجتمعه. وفيما يتعلق بمشغلي البنية التحتية تعييناً، ينبغي أن تتدفق معلومات الحوادث والمخاطر إلى الفريق الوطني من الصناعة بينما ينشر الفريق بدوره معلومات التهديدات ومواطن الضعف والتخفيف. ويستطيع كل من الحكومة والفريق الوطني تحسين تدفق المعلومات هذا عن طريق التعاون فيما بينهما على تطوير إطار نظامي لمعالجة الحوادث، مما يتضمن القضايا المحيطة بتقاسم المعلومات. وينبغي أن يتضمن هذا الإطار سياسات وإجراءات لتقاسم المعلومات والإبلاغ عن الحوادث وحماية المعلومات الخاصة الحساسة (للحكومة والصناعة) ونشرها وآليات لنقل المعلومات ونشرها.

ويوجد عدد من أنواع مجموعات تقاسم المعلومات المختلفة. وحين يتبين الفريق الوطني حاجة إلى منتدى معين لتقاسم المعلومات فينبغي له قيادة جهود إنشاء ذلك المنتدى.

وتتألف مجموعات الصناعة من شركات متفرقة تعمل في نفس القطاع، مثل موردي الكهرباء المتعددين في بلد ما. وتكون هذه المجموعات في كثيرٍ من الأحيان مصدراً قيِّماً للمعلومات عن مواطن الضعف والحوادث في صناعةٍ ما بعينها، ومن شأنها أن تمثل منتديات مثمرة لتحفيز النقاش حول الأمن السيبراني. ورغم الفوائد الجمة لمجموعات الصناعة، يحجم المشاركون أحياناً عن تقاسم المعلومات الخاصة أو الحساسة في مجموعة تضم منافسين لهم.

أما مجتمعات الاهتمام فهي بشكل عام مجموعات لها تركيز تكنولوجي ضيق النطاق. وتكون هذه المجموعات مكونات أصيلة في آلية تقاسم المعلومات لما تتمتع به في كثير من الأحيان من معارف ومهارات وخبرات تقنية متعمقة تعين على دراسة المشاكل والخروج بحلول. وكثيراً ما يكون المشاركون في هذه المجموعات أفراداً مشهود لهم بالمهارة التقنية وباحثين رائدين في مجالي الأمن السيبراني وعلوم الحاسوب وممثلين عن صناعات خاصة ينتسبون إلى موفري تكنولوجيا معلومات واتصالات رئيسيين (أي موفرو بنية تحتية ومطورو برمجيات وما إلى ذلك).

وفي بعض البلدان، تتقاسم بالفعل مجموعات الاهتمام معلومات بشأن التهديدات ومواطن الضعف والآثار في المجال الأمني. كما يصدر عن هذه المجموعات في كثيرٍ من الأحيان تنبيهات وإنذارات إلى الأعضاء في توقيتات مناسبة تسهيلاً لجهود الحد من الحوادث الفعلية المؤثرة في البنى التحتية الحاسمة والاستجابة لها والتعافي منها. ومن أمثلة هذه المجموعات مراكز تقاسم المعلومات وتحليلها في الولايات المتحدة ونقاط الإنذار والتوجيه والإبلاغ في المملكة المتحدة.

وتستطيع أفرقة العمل المشتركة بين الحكومة والصناعة تسهيل تقاسم المعلومات بشكل كبير. فيمكن أن تستنير الحكومة بالصناعة من خلال التماس التعليقات من الصناعة على سياسات الأمن السيبراني ووضع استراتيجياته وتنسيق الجهود مع مؤسسات القطاع الخاص من خلال آليات تقاسم المعلومات. وينبغي للحكومة أن تكفل انخراط القطاع الخاص في المراحل المبدئية من تطوير المبادرات والسياسات وتنفيذها وتعهدها. كما تستطيع الصناعة الاستفادة من هذه المجموعات عن طريق اغتنام فرصة التأثير في صنع السياسات والتعرف على الموضع الملائم لقطاعها في الصورة الكلية للأمن القومي.

وأخيراً، يستطيع الفريق الوطني أداء دور مهم بتنظيم أفرقة عمل بين الصناعات التي تقوم بينها علاقات اعتماد. فمن شأن الحوادث التي تتعلق بأحد قطاعات البنية التحتية أن يكون لها آثار متعاقبة تسبب حوادث في قطاعات أخرى، مما ينشئ علاقات اعتماد بيني تكون في بعض الأحيان غير متوقعة. فعلى سبيل المثال، قد يؤدي انقطاع الخدمة في أحد المرافق العامة إلى زيادة كبيرة في اتصالات العملاء على نحوٍ يعطل شبكات الهاتف. ويستطيع الفريق الوطني، من خلال تكوين فهم لكيفية تأثير الأمن السيبراني في أنظمة متعددة، أداء دورٍ مهم في إعانة مالكي البنية التحتية ومؤسسات أخرى على استشعار علاقات الاعتماد البيني هذه. ومن شأن تقاسم المعلومات عبر شركات البنية التحتية أن يسهل الاستجابة للحوادث التي تؤثر على قطاعات متعددة.

هدف التمكين: مساعدة الحكومة الوطنية في الاستجابة للحوادث دعماً للعمليات الحكومية

يمكن للفريق الوطني، متى ما كان ذلك ملائماً وقائماً على اعتبارات سياسية وتنظيمية، تحسين دوره وفعاليته عن طريق معالجة الاستجابة للحوادث لجهات حكومية. ويعين قيامه بذلك على بناء علاقات قائمة على الثقة مع الإدارات الحكومية، كما يساعد الفريق الوطني في اكتساب دراية متواصلة بالأنظمة والتكنولوجيات المستخدمة حالياً. وفي حالات تولي فريق داخلي الاستجابة للحوادث في جهات معينة، كأن يخصص فريق استجابة للقوات المسلحة مثلاً، يستطيع الفريق الوطني تقديم الدعم عن طريق نشر المعلومات المتعلقة بالتهديدات والمعلومات المتحصل عليها من خلال التواصل مع مختلف أفرقة الاستجابة في البلاد.

8.4 الخلاصة

من شأن بناء قدرة وطنية لإدارة حوادث الأمن السيبراني أن يمثل خطوة مهمة نحو مساعدة البلاد على إدارة المخاطر وتأمين أنظمتها. وقد صمم هذا الكتيب بحيث يكون منهجاً دراسياً تعريفياً بتطوير قدرات الأمن السيبراني في البلدان. ومن بين المتلقين

المقصودين جهات الرعاية المحتملة للأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وصناع السياسات الحكومية والأفراد المسؤولون عن تكنولوجيات المعلومات والاتصالات الراغبون في معرفة المزيد عن عرض القيمة للأفرقة الوطنية وقدرة إدارة الحوادث بشكل عام. لكن من غير المقصود أن يكون دليلاً للعمليات اليومية للفريق الوطني، بل هو مصدر لمواد إعلامية بشأن سبل دعم قدرة إدارة لحوادث الأمن الحاسوبي للاستراتيجية الوطنية للأمن السيبراني.

والحقيقة ببساطة هي أن ثمة حاجة مشتركة إلى مقاومة التهديدات السيبرانية والحد منها ومكافحتها والاستجابة للهجمات. وتقدم الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وما شابهها من الكيانات استجابة تشغيلية مركزة محلياً وموسعة دولياً لتلك الحوادث السيبرانية التي من شأنها زعزعة استقرار البنية التحتية الحاسمة.

5 أفضل الممارسات المتعلقة بالأمن السيبراني – إدارة فريق وطني للاستجابة للحوادث الحاسوبية بعوامل النجاح الحاسمة

1.5 مقدمة

تمثل الأفرقة الوطنية للاستجابة للحوادث الحاسوبية أهمية حيوية بالنسبة إلى الأمن السيبراني الوطني، لكنها تفرض كذلك تحديات معتبرة في مجال الإدارة. ولذلك فمن المهم أن تحصل البلدان على معلومات استرشادية بشأن تكوين قدرة وطنية وتعهدها وفهم كيفية دعم تلك القدرة للأمن السيبراني الوطني وإدارة الحوادث على الصعيد الوطني، حتى تتعامل بفعالية مع التهديدات السيبرانية.

وعوامل النجاح الحاسمة عبارة عن أسلوب لتحديد السمات والأنشطة الضرورية التي تدعم نجاح أي كيان، وقد اتُبع هذا الأسلوب لتحديد متطلبات التنفيذيين من المعلومات وتحقيق الاتساق بين تكنولوجيا المعلومات ومحركات الأعمال في مؤسسات كبيرة. وتقدم الوثيقة "أفضل الممارسات للأمن السيبراني – إدارة فريق وطني للاستجابة للحوادث الحاسوبية بعوامل النجاح الحاسمة" لاستخدام عوامل النجاح الحاسمة في مجتمع الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وتصف عملية لتحديد تلك العوامل وتعرض ثلاثة أمثلة لكيفية استخدامها كجزء من إدارة الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية.

2.5 عوامل النجاح الحاسمة

عوامل النجاح الحاسمة بالنسبة إلى الفريق الوطني للاستجابة للحوادث الحاسوبية هي الأنشطة التي يجب تنفيذها أو الشروط التي يتعين الوفاء بها حتى يحقق الفريق الوطني رسالته ويخدم مستفيديه بفعالية. ومن المهم فهم العلاقة والاختلافات بين عوامل النجاح الحاسمة والأهداف الاستراتيجية، حيث إنها قد تبدو للوهلة الأولى مترادفة. فالأهداف الاستراتيجية غايات المستوى الأعلى التي تصف ما يتعين على الفريق الوطني إنجازه.

ومن أمثلة ذلك "حماية الشبكات الحكومية التي تخزن وتنقل من خلالها معلومات تتعلق بالعمليات العسكرية." وتزيد هذه البيانات، التي تتسم في العادة بالعمومية، رسالة المؤسسة وصفاً وتوضيحاً. وهي لا توفر لمديري الأفرقة الوطنية إرشادات بشأن كيفية تحقيق الهدف الاستراتيجي في سياق بيئاتهم التشغيلية الفريدة إلا قليلاً. وأما عوامل النجاح الحاسمة فهي تعين المدير أو التنفيذي على تبين وفهم ما يجب إنجازه في سبيل تحقيق الأهداف الاستراتيجية والرسالة. ويمكن تحويل هذه تشغيلياً إلى أنشطة قابلة للتنفيذ.

وتختلف عوامل النجاح الحاسمة كذلك عن أهداف الأداء، وإن كانت ترتبط بها ارتباطاً وثيقاً. فأهداف الأداء عبارة عن مستهدفات موضوعة للإسهام في نجاح المؤسسة أو نجاح وحدة عمل أو فردٍ ما على وجه التعيين. ويكون الغرض المعتاد من أهداف الأداء توفير مستهدفات للموظفين أو وحدات العمل حتى يمكن تنظيم الأعمال وتقدير الأداء. وكثيراً ما تكون أهداف الأداء محددة للغاية ومعبرة عن قياسات أداء كمية، كما أنها ترتبط في كثير من الأحيان بعملية إدارة أداء. وبينما يمثل هذا النوع من الأهداف ضرورة لتشغيل المؤسسات، فلا يقتضي ذلك كونها أفضل مؤشر للنجاح في جميع الحالات، حيث إن المديرين

في يضعون أهداف الأداء في كثير من الأحيان استناداً إلى افتراضات بشأن تحديد نوعيات النشاط القابلة للقياس، والأهم من ذلك أن أهداف الأداء غير موجهة على الحقيقة إلى إعانة المديرين على فهم الأنشطة الداخلية في مؤسستهم وتحديد أولوياتها، ولا هي موجهة إلى الإعانة على حل مشاكل الإدارة، بل توضع لاستخدام من يؤدون العمل في المؤسسة. وبالمقابل، تسد عوامل النجاح الحاسمة الفجوة بين الاعتبارات الاستراتيجية وأهداف المستويات الأدنى. ويمكن توظيف عوامل النجاح الحاسمة أيضاً لسد الفجوة بين هدف استراتيجي على مستوى أعلى وأهداف الأداء.

3.5 مزايا النهج القائم على عوامل النجاح الحاسمة

توجد مزايا عديدة لوضع عوامل النجاح الحاسمة على نهج نظامي في الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية، بل ولأي مؤسسة بشكل عام. ومن هذه المزايا ما يلي:

- الحد من الإبهام. من شأن عوامل النجاح الحاسمة أن تعين المديرين على تحقيق التوافق بين موظفيهم جميعاً بشأن غرض المؤسسة وأنشطتها. كما أن من شأن عملية تحديد عوامل النجاح الحاسمة وتنفيذها أن تعين على تعزيز التواصل في جميع الأفرقة عن طريق إشراكها في النقاش، مما يرفع من مستوى ثقة الفريق الوطني في القرارات التي تتخذها الإدارة.
- تحديد العوامل المقترحة للقياس ووضع الأهداف. يمثل قياس الأداء، كما سبقت الإشارة، أحد الأوجه الأساسية لإدارة أي مؤسسة. ومع ذلك، فإن قياس الأداء المؤسسي ينطوي على تكاليف ومسائل معقدة. فمن شأن جمع البيانات وتحليلها أن يستهلك ساعات عمل وأن يتطلب استثماراً في تجهيزات تكنولوجية. فما عساه يقاس؟ وعلى أي فترات؟ وتواجه مؤسسات كثيرة صعوبة في قياس الأشياء الملائمة – أو أنها لا تقيس إلا الأنشطة التي يسهل قياسها [هبرد – 2009]. وتفضي هذه الحالة من عدم التيقن أحياناً إلى انعدام قياس أنشطة المؤسسة أو قصوره عن الحد الأمثل. ومن الممكن توظيف عوامل النجاح الحاسمة في سبيل تحقيق الوضوح وحسن التوجيه بشأن هذه المسألة، مما يكفل الاستفادة من القياس والمقاييس في التوصل إلى أمثل النتائج.
- تحديد المتطلبات المعلوماتية. من شأن عوامل النجاح الحاسمة، إذا كانت متماشية مع وضع الأهداف بشكل وثيقة، أن تعين المديرين على تحديد أنواع المعلومات اللازمة بالفعل من أجل فهم عمليات الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية وسلامتها. ومن الممكن توظيف التقييم الوافي لعوامل النجاح الحاسمة لتبين ما خفي من المتطلبات المعلوماتية، مما يشكل أحياناً هدفاً في حد ذاته. فعلى سبيل المثال، كثيراً ما يعتمد نجاح الفريق الوطني على الكيفية المقرر أن يبلغ بها المستفيدون الأساسيون المتعاونون المؤسسة عن الحوادث وغير ذلك من المعلومات. ومن الممكن أن يؤدي الفحص النظامي لعوامل النجاح الحاسمة كهدف إلى بيان أن ما يلقى الفريق الوطني من قبول كجهة موثوق بها أو كرائد تكنولوجي يمثل عاملاً من عوامل النجاح الحاسمة. ومن شأن هذا أن يؤدي بمدير الفريق الوطني إلى طلب ومراقبة أنواع من المؤشرات والمعلومات لم يكن ليضعها في اعتباره لولا ذلك.
- تحديد شواغل إدارة المخاطر. يمكن الاستفادة من عوامل النجاح الحاسمة في سبيل تحديد الأصول والخدمات الحيوية التي تدعم المؤسسة في تأدية رسالتها. ومن شأن هذه الوظيفة أن تعين الفريق الوطني على تحديد الأنظمة والأصول التي ينبغي إخضاعها لعملية إدارة المخاطر. وقد أصبح هذا الاستخدام لعوامل النجاح الحاسمة شائعاً في صناعات كثيرة.

كما يمكن الاستفادة من عوامل النجاح الحاسمة بشكل خاص للمؤسسات الجديدة والمتطورة مثل الأفرقة الوطنية للاستجابة للحوادث الحاسوبية. ففي حالة المؤسسات التي تضم أعداداً كبيرة من الموظفين المتكافئين، كما هو الحال على سبيل المثال في صناعة السيارات التي تخدم سوقاً ناضجة لها تاريخ طويل أُرهق دراسةً، يحمل المعنيون فهماً، ولو كان حدسياً على الأقل، لما يتطلبه النجاح (أي عوامل النجاح الحاسمة) في صناعتهم. وقد يكون هذا الفهم مستنداً إلى تعليم مؤسسي أو التحاور مع نظراء في شركات أخرى أو إلى خبرات تاريخية في الصناعة. أما مديرو الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية فلا يتمتعون في العادة بنفس المزايا، مما يؤهلهم للاستفادة من مثل هذه العملية النظامية الرامية إلى تحديد ممارساتهم الأساسية.

4.5 مصادر عوامل النجاح الحاسمة

يركز الكثير من الأدبيات المتاحة عن عوامل النجاح الحاسمة على الشركات الصناعية الخاصة. وتلتمس هذه الشركات استخلاص عوامل النجاح الحاسمة من خلال كيانات ومصادر مختلفة [روكهارت 1979، كارالي 2004] من بينها الصناعة التي تنتمي إليها ونظراؤها ومناخ الأعمال العام والتنظيم الحكومي والمشاكل أو العوائق المحددة التي تواجه المؤسسة ومختلف التراتبات الداخلية في تنظيماتها. ولا تختلف مصادر عوامل النجاح الحاسمة بالنسبة إلى فريق وطني معني بالاستجابة للحوادث الحاسوبية اختلافاً كبيراً، ومن ذلك:

- المستفيدون. الراجح أن يكون هذا أهم مصدر لعوامل النجاح الحاسمة بالنسبة إلى الفريق الوطني، حيث تمثل حاجات المستفيدين وطلباتهم مدخلا أساسياً للخدمات المطلوب تقديمها. وتتباين الخدمات حسب قاعدة المستفيدين، فقد يتاح لفريق وطني يدعم جهات حكومية رصد شبكات الجهات الحكومية مباشرة إن كان مخولاً بالصلاحية اللازمة لذلك، بينما يتاح لفريق وطني يخدم مالكي البنية التحتية ومشغليها من القطاع الخاص جمع بيانات الحوادث من خلال البلاغات الطوعية. وقد يتعلق قسم كبير من دور الفريق بنشر أفضل الممارسات وأداء وظيفية إنذارية. وعدا مسألة تحديد الخدمات، من شأن قاعدة المستفيدين أن تزود الفريق الوطني بمدخلات بشأن مسائل تشغيلية، مثل السرعة التي يجب معالجة الحوادث أو تحليلها بها حتى تكون مفيدة.
- مؤسسات الإدارة أو الإشراف. تمثل المؤسسة التي ترعى الفريق الوطني وتشرف عليه مصدراً مهماً لعوامل النجاح الحاسمة. ويشار إلى هذا في كثيرٍ من الأحيان في رسالة المؤسسة الأم أو أهدافها.
- النظراء. من الممكن تحويل خبرات أفرقة وطنية أخرى معنية بالاستجابة للحوادث الحاسوبية إلى بنك معلومات قيِّم يستنار به في توجيه العمليات. فعلى سبيل المثال، ربما تكون مؤسسات نظيرة تخدم مجموعات مشابهة من المستفيدين أو واجهت تحديات مماثلة قد استفادت بالفعل دروساً من شأنها أن تكون نافعة لغيرها.
- البيئة القانونية أو السياسية. قد تواجه الأفرقة الوطنية متطلبات أو قيوداً دستورية أو تنظيمية تؤثر أيضاً في عوامل النجاح الحاسمة. فقد تحول قيود دستورية دون حصول الفريق الوطني على معلومات معينة أو تلزمه بواجبات لحماية معلومات محددة إلى مستوىً محدد. وربما تضمن ذلك لوائح تنظيمية تتعلق بخصوصية المعلومات الشخصية على سبيل المثال.

وتقع القضايا التنظيمية ضمن هذه الفئة كذلك. فعلى سبيل المثال، إذا كان الفريق الوطني جزءاً من مؤسسة تتولى أيضاً الإشراف على قاعدة المستفيدين أو تنظيمها، فقد تثير هذه العلاقة التنظيمية في حد ذاتها تحديات يجب أخذها في الاعتبار. وفي هذه الحالة تعييناً، يمكن وصف استعداد المستفيدين لتقديم معلومات بشأن الحوادث أو مواطن الضعف لديهم، بالرغم من الشاغل الواضح المتمثل في احتمال استخدام ذلك لأغراض تنظيمية، بأنه أحد عوامل النجاح الحاسمة.

- القيود على الموارد. تمثل القيود على الموارد التي قد تواجهها الأفرقة الوطنية مصدراً محتملاً لعوامل نجاح حاسمة. ومن القيود الأساسية في كثير من البيئات محدودية توافر الموظفين المهرة. ومن القيود المحتملة الأخرى عدم التيقن المحيط بالتمويل. وقد تقتضي القيود على الموارد عوامل نجاح حاسمة تحد من العمليات أو تقيدها، كما يمكن أن يعبر عامل النجاح الحاسم الناتج عن الحاجة إلى التخفيف من القيد وتنمية رأس المال البشري أو مصادر التمويل.

5.5 تحديد عوامل النجاح الحاسمة

المقصود من هذا القسم أن يؤدي وظيفة الدليل التمهيدي إلى هذا الموضوع ويصف عملية لتحديد عوامل النجاح الحاسمة في سياق الأفرقة الوطنية المعنية بالاستجابة للحوادث الحاسوبية. والمراد هنا تكوين فهم لدى مديري الأفرقة الوطنية بالعملية النظامية التي تحرك تطوير عوامل النجاح الحاسمة. ويمكن الاطلاع على مزيدٍ من التفاصيل بشأن عملية تحديد عوامل النجاح الحاسمة وتهذيبها في المصنفات المشار إليها في **الملحق باء** بهذا التقرير.

وكثيراً ما تُستخدم أنشطة مثل ورش العمل وحلقات العمل لاستخلاص عوامل النجاح الحاسمة أو تحديدها. وتختار الإدارة الأفراد القائمين على تسهيل هذه الأعمال استناداً إلى خصال مختلفة، مثل القدرة على التفكير بشكل موضوعي بشأن المؤسسة

والقدرات القيادية وفهم المؤسسة ومهارات التواصل. واستناداً إلى الأدبيات المتعلقة بهذا المجال، نقترح أربع مراحل لتحديد وتهذيب عوامل النجاح الحاسمة للأفرقة الوطنية. وهذه المراحل كما يلي:

- تعريف النطاق
- جمع بيانات؛ جمع وثائق وإجراء مقابلات
- تحليل البيانات
- استخلاص عوامل النجاح الحاسمة

6.5 تعريف النطاق

ينطوي تعريف النطاق في العادة على اتخاذ قرارٍ بشأن تركيز جمع عوامل النجاح الحاسمة على الأولويات المؤسسية للمؤسسة أو على أنشطة تشغيلية، حيث تركز عوامل النجاح الحاسمة المؤسسية على قرارات رئيسية طويلة الأمد، مثل أولويات التوظيف والخدمات التي ستقدم والتكنولوجيا المراد الاستثمار فيها والانتقال إلى مقر جديد من عدمه، بينما تركز عوامل النجاح الحاسمة التشغيلية بالمقابل على العمليات اليومية للمؤسسات. وفي حالة الفريق الوطني، قد تتعلق عوامل النجاح الحاسمة التشغيلية بسرعة معالجة الحوادث أو الأولويات المتبعة في معالجة مختلف أنواع الحوادث.

وتبدأ مؤسسات كثيرة، خاصة الشركات الكبيرة التي تضم شعباً وإدارات كثيرة، عملية عوامل النجاح الحاسمة على المستوى المؤسسي، وذلك طلباً للتبسيط. ومع ذلك، قد يكون الجمع بين عوامل النجاح الحاسمة المؤسسية والتشغيلية فعالاً في حالة المؤسسات الأصغر ذات الهيكل التنظيمي الأفقي (حيث يكون عدد الطبقات التنظيمية بين المديرين والعاملين قليل). ويشترك الكثير من الأفرقة الصغيرة التي تتألف منها الأفرقة الوطنية في هذه الخصائص بينها، مما يتيح استخلاص عوامل النجاح الحاسمة بسهولة من خلال عملية واحدة مجمعة.

7.5 جمع البيانات: جمع وثائق وإجراء مقابلات

تجمع البيانات اللازمة لوضع عوامل النجاح الحاسمة بأحد أسلوبين أساسيين هما جمع *الوثائق وإجراء مقابلات مع أفراد عاملين أساسيين*.

وينطوي جمع الوثائق في العادة على تجميع وثائق مهمة توفر معلومات عن العوامل الأساسية المؤثرة في أداء الفريق الوطني لمهمته. وتتضمن أنواع الوثائق التي تُجمع في العادة ما يلي:

- الاستراتيجية الوطنية للأمن السيبراني
- بيانات الرسالة للفريق الوطني والمؤسسة التي يتبعها
- بيانات الرسالة لأهم أصحاب المصلحة أو المستفيدين
- تقارير تدقيق سابقة تتعلق بالفريق الوطني
- تقارير سابقة عن الحوادث التي أثرت في المستفيدين
- التشريعات أو القوانين التي تؤسس الفريق الوطني وتحدد صلاحياته
- قوانين أو لوائح تنظيمية أخرى مهمة

ومن بين أسلوبي جمع البيانات، يكون إجراء المقابلات في العادة هو الأهم والأجدى، حيث يتيح إجراء مقابلات مع مديرين وموظفين ومستفيدين وأصحاب مصلحة آخرين الفرصة للتوصل إلى اتفاق وفهم ما هو مهم على الحقيقة بالنسبة إلى عمل المؤسسة. وعلاوة على ذلك، تسمح العملية التفاعلية المتمثلة في إجراء مقابلة للمشاركين الإسهام في توجيه العملية والكشف عن المجالات ذات البال وغير ذلك من الدقائق على نحو لا يتيحه جمع الوثائق في العادة.

ويتطلب تحقيق الفاعلية في مقابلات عوامل النجاح الحاسمة مشاركة الأشخاص الملائمين في هذه الفعالية، كما ينبغي التفكير سلفاً في أسئلة المقابلات. فعلى سبيل المثال، قد يُجنى شيء من المعلومات المفيدة بطرح السؤال البسيط "ما هي عوامل النجاح الحاسمة لديكم؟" على أحد المستفيدين، إلا أن من شأن أسئلة التحسس وأسئلة الإجابات المفتوحة أن تكون أنفع. على سبيل المثال:

- ما أهم شاغلين أو ثلاثة لديك فيما يتعلق بفقد المعلومات؟
- كيف يهدد أي خلل في نظام معلومات مؤسستك؟
- ما أهم أمرين أو ثلاثة تلزمك من أجل إدارة حوادث الأمن السيبراني مما تعجز عنه في الوقت الحالي؟
- ما عساه يجعلك تمتنع عن تقاسم معلومات بشأن مواطن الضعف أو الحوادث مع فريقنا الوطني؟
- كيف يمكن لنا اكتساب ثقة الناس في مؤسستك؟

8.5 تحليل البيانات

يجب بعد جمع البيانات إخضاعها للتحليل. وتُفحص خلال مرحلة التحليل الوثائق وإجابات المقابلات التماساً للمحاور المتشابهة. والمحاور هي أفكار أو أنشطة تبدو متكررة في جميع الوثائق أو الإجابات.

ومن شأن تحليل الوثائق لتبين المحاور أن يكون أمراً بسيطاً نسبياً. فعلى سبيل المثال، يبين الشكل 8 الأهداف من 1.3 إلى 3.3 من *الخطة الاستراتيجية لوزارة الأمن الداخلي بالولايات المتحدة للفترة 2008-2013*. وتظهر بعض أجزاء تلك الأهداف تحتها خط، ويبين الجدول 1 تلك البيانات والمحاور المتعلقة بها.

الشكل 8: مثال: ثلاثة أهداف من الخطة الاستراتيجية لوزارة الأمن الداخلي للفترة 2008 إلى 2013

الهدف 1.3

حماية وتعزيز مرونة البنية التحتية الحاسمة والموارد الأساسية في البلاد.

سنقود جهود الحد من مواطن الضعف المحتملة في البنية التحتية الحاسمة والموارد الأساسية في بلادنا ضماناً لحمايتها ومرونتها. وسننمي شراكات ذات منفعة متبادلة مع المالكين والمشغلين من القطاعين العام والخاص بغية وقاية البنية التحتية الحاسمة والموارد الأساسية لدينا من أخطر التهديدات والمخاطر الحاسمة. وسنعزز مرونة البنية التحتية الحاسمة والموارد الأساسية.

الهدف 2.3

ضمان استمرارية اتصالات الحكومة وعملياتها.

سننفذ تخطيط استمرارية العمليات على المستويات الحكومية الأساسية. وسنحسن قدرتنا على مواصلة أداء الوظائف/عمليات الأعمال والحكومة الضرورية، بما في ذلك حماية موظفي الحكومة ومرافقها وقادتها الوطنيين والبنية التحتية للاتصالات في البلاد عبر نطاق عريض من حالات الطوارئ المحتملة.

الهدف 3.3

تحسين الأمن السيبراني.

سنعمل على تقليل مواطن الضعف أمام تهديدات الأنظمة السيبرانية لدينا قبل أن يمكن استغلالها للإضرار بالبنى التحتية الحاسمة للبلاد وسنتكفل بالحد من تكرار حالات التعطل في الفضاء السيبراني هذه وبتقصير مددها إلى الحد الأدنى وبقابليتها للإدارة وبتسببها في أقل ضرر ممكن.

الجدول 1: استخلاص محاور من استعراض الوثائق

البيان	المحور
"الحد من مواطن الضعف المحتملة."	الحد من مواطن الضعف
"تقليل مواطن الضعف أمام تهديدات الأنظمة السيبرانية."	الحد من مواطن الضعف
"إنماء شراكات ذات منفعة متبادلة."	تكوين شراكات مع الصناعة الخاصة
"تعزيز مرونة البنية التحتية الحاسمة."	مرونة البنية التحتية
"حماية البنية التحتية للاتصالات."	مرونة البنية التحتية
"...تكفل بالحد من تكرار حالات التعطل في الفضاء السيبراني هذه وبتقصير مددها إلى الحد الأدنى وبقابليتها للإدارة وبتسببها في أقل ضرر ممكن."	مرونة البنية التحتية

وتُشتق المحاور من ملاحظات المقابلات على نحو مشابه، لكن من شأن ذلك أن يكون أصعب لوجوب تعمد الفريق الذي يسهل النشاط منع أي تأثير مضلل في نتائج العمل يتسبب عن انحيازاتهم الشخصية أو منصب الشخص الذي تجرى معه المقابلة أو غير ذلك من العوامل. وتجرى في العادة عملية تقييس على البيانات من أجل استبعاد أي انحيازات وإعطاء درجات للإجابات بشكل متكافئ. ومعنى تقييس البيانات هنا إعادة كتابة الإجابات وعرضها بشكل يحد من آثار الانحياز أو غيره من الأخطاء.

9.5 استخلاص عوامل النجاح الحاسمة

ينطوي استخلاص عوامل النجاح الحاسمة على تهذيب المحاور التي يسفر عنها التحليل بغية تطوير عوامل نجاح حاسمة مختصرة وفريدة تصف المجالات الحاسمة التي يجب أن يعمل فيها الفريق الوطني لأداء برسالته. ويشمل تهذيب المحاور تجميعها حسب الخصائص المتشابهة ثم التعبير، بأقصى درجات الاختصار الممكنة، عن مدلول المحور بالنسبة إلى المؤسسة. وتؤدى هذه العملية مراراً وتكراراً لاستبعاد عوامل النجاح الحاسمة المقترحة التي يشوبها شيء من عدم الوضوح أو الازدواجية. وفيما يلي قائمة نموذجية لعوامل النجاح الحاسمة التشغيلية والمؤسسية للفريق الوطني الخيالي الذي نعمل عليه.

- يجب اكتشاف أي حركة غير مصرح بها في الشبكات الحكومية.
- يجب السيطرة على أي دعاية سلبية بسبب الحوادث الأمنية.
- يجب أن ينسق الموظفون مع الموردين.
- يجب الحد من مواطن الضعف بشكل سريع.
- يجب تكوين شراكات قوية مع الصناعة الخاصة.
- يجب تقديم الخدمات بالمتاح حالياً من الموظفين الداخليين.[25]

ويجب عقب تحديد عوامل النجاح الحاسمة تطبيقها حتى تكون مفيدة. ويقدم القسم التالي ثلاثة أمثلة لاستخدام عوامل النجاح الحاسمة لدعم إدارة الفريق الوطني.

[25] ويشبه الفريق الوطني الخيالي المستخدم في هذا المثال كثيراً من الأفرقة الوطنية من حيث مواجهته لقيود على الموارد.

10.5 استخدام عوامل النجاح الحاسمة للأفرقة الوطنية

يتمثل الغرض من تحديد عوامل النجاح الحاسمة في مساعدة مديري الأفرقة الوطنية على فهم عملياتها واتخاذ قرارات أفضل. وللأفرقة الوطنية أن تستخدم عوامل النجاح الحاسمة كما يستخدمها الكثير من المؤسسات التي تتمحور أعمالها حول تكنولوجيا المعلومات. فعلى سبيل المثال، يمكن الاستعانة بعوامل النجاح الحاسمة على إدارة الأمن والمرونة عن طريق مساعدة المديرين في تمييز الخدمات والأصول التي لها أهمية حقيقية ويلزم تأمينها. ومن شأنها كذلك أن تعين المديرين على تحديد الأولوية النسبية لتأمين مختلف الأصول. وفيما يرتبط بهذه المسألة ارتباطاً وثيقاً، يمكن الاستعانة بعوامل النجاح الحاسمة على تحديد نطاق تقييمات المخاطر. ومن شأن تقييم المخاطر أن يتطلب جهداً ووقتاً بشكل مكثف، مما يجعل من وجود عملية نظامية لتحديد الخدمات المهمة وما يتعلق بها من الأصول ضرورة في سبيل تحقيق ثمرة من تقييم المخاطر. وأخيراً، يمكن استخدام عوامل النجاح الحاسمة لإعانة المديرين على تبين متطلبات المرونة (السرية والنزاهة والإتاحة) التي تدعم الأصول المعلوماتية.

وسيتناول هذا القسم السبل التي يمكن للقادة الراغبين في تكوين أو بدء فريق وطني بها الاستفادة من عوامل النجاح الحاسمة. ثم يركز القسم بشكل أضيق على مثالين يتعلقان بالإدارة التشغيلية لفريقنا الوطني الخيالي: تحديد خدمات تقدم للمستفيدين وتحديد أولويات القياس.

11.5 بناء قدرة وطنية لإدارة حوادث الأمن الحاسوبي

حددنا في تقرير سابق ضمن هذه السلسلة [هولر 2010] أربعة أهداف استراتيجية ومجموعة من أهداف التمكين لتطوير قدرة وطنية للاستجابة للحوادث الحاسوبية. وهذه الأهداف هي:

- تخطيط وبناء قدرة مركزية لإدارة حوادث الأمن الحاسوبي.
  - تحديد الجهات الراعية والمستضيفة.
  - تحديد القيود.
  - تحديد هيكلية الفريق الوطني المعني بالاستجابة الحوادث الحاسوبية.
  - تحديد صلاحيات الفريق الوطني المعني بالاستجابة الحوادث الحاسوبية.
  - تحديد خدمات الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية.
  - تحديد أصحاب مصلحة إضافيين.
- تهيئة الوعي الظرفي المشترك.
  - تكوين علاقات قائمة على الثقة والحفاظ عليها.
  - تنسيق تقاسم المعلومات بين المستفيدين المحليين.
  - دمج معلومات المخاطر الواردة من المجتمع.
  - جمع معلومات حول حوادث الأمن الحاسوبي.
- إدارة الحوادث السيبرانية.
  - تحديد الحوادث والتهديدات محل الاهتمام على الصعيد الوطني.
  - تحليل حوادث الأمن السيبراني.
  - تطوير عملية تدفق عمل فعالة.
  - إنذار المجتمع.
  - تعميم أفضل ممارسات الأمن السيبراني.

- دعم الاستراتيجية الوطنية للأمن السيبراني.
  - ترجمة الخبرات والمعلومات بغية تحسين إدارة الحوادث السيبرانية ووضع السياسات السيبرانية على الصعيد الوطني.
  - بناء قدرة الأمن السيبراني على الصعيد الوطني.
  - استثمار شراكات القطاعين العام والخاص في سبيل تحسين الوعي والفعالية.
  - المشاركة في تطوير مجموعات ومجتمعات تقاسم المعلومات والتشجيع على ذلك.
  - مساعدة الحكومة الوطنية في الاستجابة للحوادث دعماً للعمليات الحكومية.

وبينما تستعرض الأهداف الاستراتيجية وأهداف التمكين هذه أنشطة بناء فريق وطني، لا يصف التقرير السابق بشكل بات كيفية تحقيقها. ومن شأن تحديد عوامل النجاح الحاسمة أن يمثل خطوة مهمة، حيث يمكن لها تحقيق الوضوح وتقديم إجابات عن أسئلة أساسية عن كيفية تحقيق تلك الأهداف. ويعرض **الجدول 2** بعض أمثلة الأسئلة التقليدية التي قد تنشأ عند إنشاء فريق وطنية. وأهداف التمكين مقتبسة من الوثيقة السابقة.

الجدول 2: الأسئلة المطلوب معالجتها عند إنشاء فريق وطني

هدف التمكين	الأسئلة
تحديد خدمات الفريق الوطني المعني بالاستجابة للحوادث الحاسوبية	• ما هي الخدمات التي ينبغي تقديمها؟ • كيف يمكن لمديرِ ما أن يتيقن من ملاءمة هذه الخدمات؟ • بأي أولويات ينبغي تقديمها؟ • ولمن تقدم من المستفيدين؟
تكوين علاقات قائمة على الثقة والحفاظ عليها	• تكوين ثقة والحفاظ عليها مع من؟ • ما هي أنواع معلومات المخاطر التي ينبغي دمجها؟
دمج معلومات المخاطر الواردة من المجتمع	• من أي أعضاء المجتمع؟ • بأي أولويات؟
تحديد الحوادث والتهديدات محل الاهتمام على الصعيد الوطني	• الحوادث التي تؤثر في أي أنظمة ذات أهمية على الصعيد الوطني؟ • بأي أولويات ينبغي معالجتها؟
إنذار المجتمع	• أي أعضاء المجتمع؟ • بأي أولويات ينبغي إنذارهم؟ • بأي المعلومات ينذَرون؟
بناء قدرة الأمن السيبراني على الصعيد الوطني	• ما هي نوعية القدرة التي ينبغي بناؤها؟ • في أي مؤسسات؟ • بأي أولويات؟

ويتجاوز أي وصف كامل لكيفية استخدام عوامل النجاح الحاسمة لكل هدف نطاق هذه الوثيقة، إلا أن تحديد عوامل النجاح الحاسمة – وهو الأمر المهم فعلاً من أجل تحقيق النجاح – يمثل نشاطاً مستقلاً يجرى مرة واحدة ومن شأنه أن يوجه الكثير من أنواع القرارات التنظيمية ويعززها.

12.5 تحديد خدمات الفريق الوطني

تحدد رسالة الفريق الوطني وقاعدة مستفيديه ما ينبغي له تقديمه من خدمات.

وقد تتطلب بعض الخدمات نفقات كبيرة من حيث التمويل والتوظيف،[26] بينما لا يتجاوز البعض الآخر منها تكرار خدمات يمكن للمستفيدين أداؤها بأنفسهم أو ينبغي لهم ذلك. وينبغي من أجل تجنب إهدار الوقت والموارد أن ترتبط الخدمات ارتباطاً وثيقاً بالبيئة التشغيلية للفريق الوطني والاعتبارات السياسية وغيرها من الاعتبارات واحتياجات المستفيدين والأنشطة المهمة بحق بالنسبة إلى نجاح الفريق الوطني. وينبغي، اختصاراً، أن تربط بعوامل النجاح الحاسمة.

ويصف هذا القسم استعمال تحليل التواؤم لتحديد الخدمات التي ينبغي لفريقنا الوطني الخيالي تقديمها. وتحليل التواؤم أسلوب شائع لاستعمال عوامل النجاح الحاسمة ويوصف على النحو التالي

> *... التواؤم هو التشابه المتأصل أو المتصور بين شيئين. وتحليل التواؤم هو أسلوب لدراسة هذا التشابه بغية فهم العلاقات واستخلاص نتائج بشأن أثر أحدهما في الآخر [كارالي 2004].*

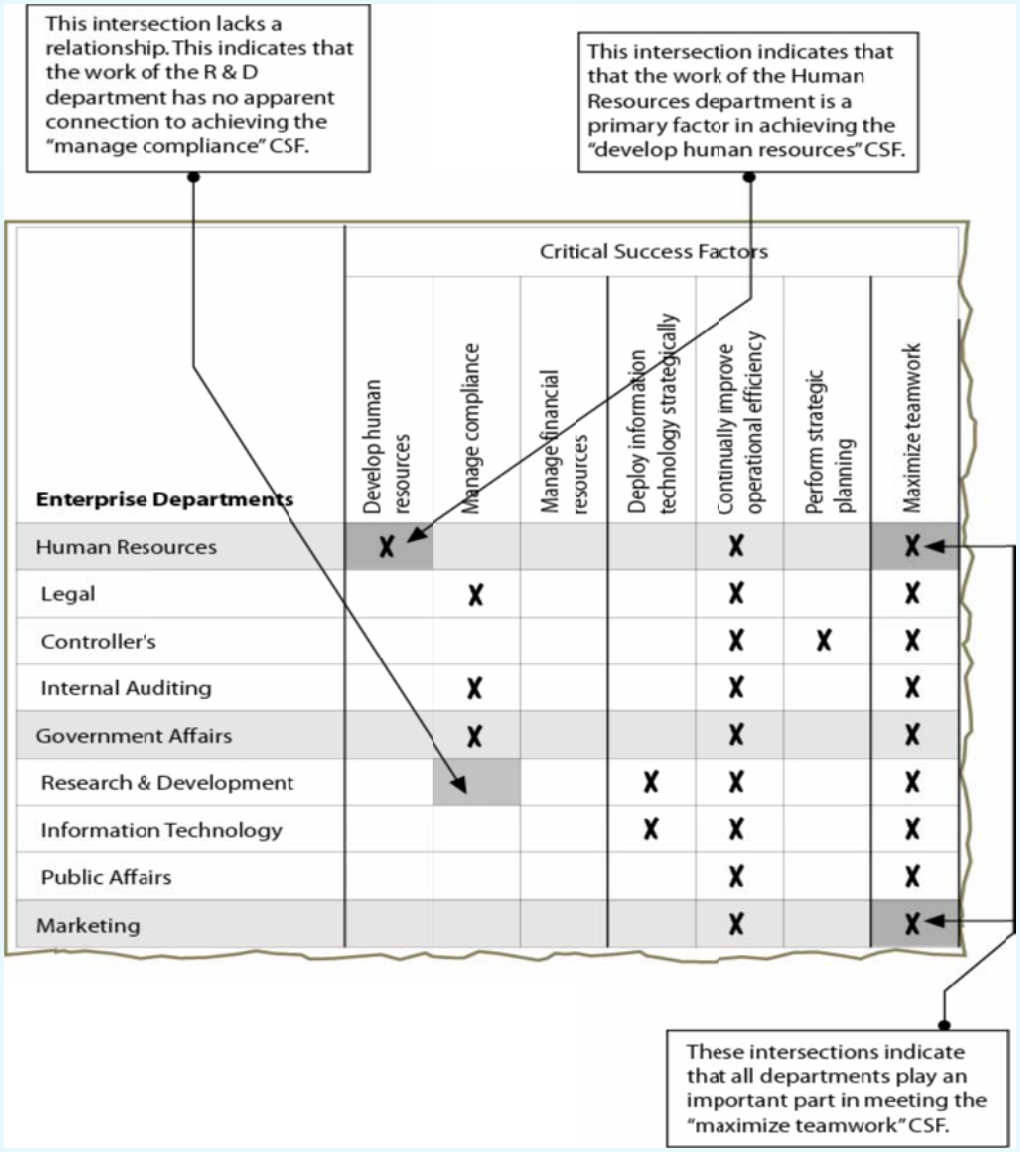
ويجرى تحليل التواؤم في العادة عن طريق تكوين مصفوفة مقارنات تتيح مقارنة عوامل النجاح الحاسمة وربطها بعلاقات بينية بمعايير متنوعة. وقد تكون معايير المقارنة أوجه مختلفة للنشاط التنظيمي، حسب نوع التحليل المطلوب إجراؤه. فقد تكون معايير المقارنة ما يلي على سبيل المثال:

- العمليات التنظيمية
- الأصول المعلوماتية
- الأصول المادية
- المتطلبات الأمنية
- مقاييس الأداء
- أهداف الوحدات التشغيلية أو غاياتها.

والغرض من تكوين مصفوفة مقارنات هو تبين العلاقة بين بعض المعايير وعوامل النجاح الحاسمة. فعلى سبيل المثال، تقارَن عوامل النجاح الحاسمة في المثال التالي البسيط للغاية بإدارات في مؤسسة مفترضة لتبين الإدارات التي تدعم عوامل نجاح حاسمة معينة.

[26] يمثل تحديد مجموعات الاقتحام، على سبيل المثال، نوعاً من تحليل العلاقات البينية لتزويد جهاز إنفاذ القانون وغيره من السلطات الحكومية بمعلومات تعزى بها الأنشطة الضارة إلى الأشخاص أو الكيانات المدبرة لها. ومن شأن هذا النوع من التحليل المتعمق عبر مجموعات كبيرة من الحوادث أن يتطلب جهوداً بشرية هائلة.

الشكل 9: تقارَن عوامل النجاح الحاسمة بإدارات في مؤسسة مفترضة لتبين الإدارات التي تدعم عوامل نجاح حاسمة معينة



ويتعلق المثال التالي بتحليل للخدمات التي ينبغي لفريقنا الوطني الخيالي تقديمها للحكومة ومستفيدي البنية التحتية الحاسمة. وقد أسفرت عملية نظامية – وفقاً لما تناوله القسم الثاني من هذا التقرير بشكل عام – ستة عوامل نجاح حاسمة، وهذه المراحل كما يلي:

- يجب اكتشاف أي حركة غير مصرح بها في الشبكات الحكومية.
- يجب السيطرة على أي دعاية سلبية بسبب الحوادث الأمنية.
- يجب أن ينسق الموظفون مع الموردين.
- يجب الحد من مواطن الضعف بشكل سريع.
- يجب تكوين شراكات قوية مع الصناعة الخاصة.
- يجب تقديم الخدمات بالمتاح حالياً من الموظفين الداخليين.

وتظهر مصفوفة تحليل التواؤم المستكملة في صفحة 51. وقد استكملت المصفوفة عن طريق مقارنة كل عامل من عوامل النجاح الحاسمة بكل خدمة مقترحة لمعرفة إذا كانت الخدمة تدعم عامل النجاح الحاسم (أو تتوافق معه). وفي هذه الحالة، يسفر استكمال مصفوفة مقارنات عن دروس ومعلومات تفيد مدير هذا الفريق الوطني.

ومن المشاهدات الأولية أن عامل النجاح الحاسم "يجب اكتشاف أي حركة غير مصرح بها في الشبكات الحكومية" غير مستوفٍ إلى حد بعيد وأنه سيكون صعب التحقيق للغاية. وبينما توجد خدمات من شأنها إعانة الفريق الوطني على اكتشاف الحركة غير المصرح بها، فلا يمكن الجمع بين تقديمها واستيفاء عامل النجاح الحاسم المقيِد "يجب تقديم الخدمات بالمتاح حالياً من الموظفين الداخليين". وفي هذه الحالة، ينبغي لمديري الفريق الوطني عقد المزيد من المناقشات حول عامل النجاح الحاسم هذا مع الجهة الحكومية الراعية للفريق، على أن يكون الغرض من ذلك تهذيب الشرط أو استبعاده أو تقديم مبررات زيادة التمويل حتى يتمكن الفريق الوطني من التعاقد مع موظفين أكثر عدداً وأعلى تدريباً.

ومن المشاهدات الأولية الأخرى من المصفوفة أن أفيد خدمة يستطيع الفريق الوطني تقديمها بشكل عام هي ببساطة أن يكون نقطة اتصال ومنسقاً موثوقاً،[27] وذلك لأن أداء دور المنسق يدعم عدداً كبيراً من عوامل النجاح الحاسمة.

وأخيراً، تكشف المصفوفة عن ضعف في القوام التوظيفي الحالي للفريق الوطني. فبينما يدعم "التنبيه والإنذار على الصعيد الوطني" عاملي نجاح حاسمين ويدعم "بناء قدرات أفرقة الاستجابة للحوادث الحاسوبية في المؤسسات" ثلاثة عوامل نجاح حاسمة فإن الفريق الوطني غير قادر في الوقت الراهن على تقديم هاتين الخدمتين لقصور قوامه التوظيفي عن القدرة على ذلك. فهو لا يستطيع تقديم هاتين الخدمتين بالمتاح حالياً من الموظفين الداخليين، وهو عامل النجاح الحاسم الأخير، مما يشير إلى الحاجة إلى استعمال المزيد من الموظفين لتقديم هاتين الخدمتين الحيويتين.[28]

[27] يتولى الفريق الوطني من خلال أدائه لهذا الدور التنسيق للمؤسسات المحلية التي تحاول حل حوادث متعلقة بالأمن السيبراني. وهو يؤدي هذا الدور أيضاً للكيانات الأجنبية التي تستفسر عن حوادث أمنية قد يكون لها صلة أو رابط بمستفيدي الفريق الوطني. وفي العادة لا يتولى الفريق الوطني في إطار هذا الدور تحليل الحوادث ولا حلها بنفسه، بل يساعد في توجيه المؤسسات إلى معلومات أو خدمات أو كيانات أخرى تستطيع مساعدتها.

[28] بالمقابل، يتيح القوام التوظيفي الحالي للفريق الوطني تقديم خدمتي معالجة الأشياء المصطنعة والرصد التكنولوجي، مما لا يسهم على أي نحو معتبر في عوامل النجاح الحاسمة الخمسة الأولى.

الجدول 3: مصفوفة تحليل التواؤم لاختيار خدمات الفريق الوطني الخيالي

		عوامل النجاح الحيوية				
	الخدمات المقترحة	يجب اكتشاف أي حركة غير مشروعة في الشبكات الحكومية.	يجب السيطرة على أي دعاية سلبية بسبب الحوادث الأمنية.	يجب أن ينسق الموظفون مع الموردين	يجب الحد من مواطن الضعف في البنية التحتية الحاسمة.	يجب تكوين شراكات قوية مع الصناعة الخاصة.	يجب تقديم الخدمات بالمتاح حالياً من الموظفين الداخليين
خدمات تقليدية لأفرقة الوطنية	اكتشاف مجموعات الاقتحام						
	تقديم استشارات للحكومة الوطنية بشأن أمور الأمن السيبراني		x				X
	تقييم التأهب وقدرة إدارة الأزمات على الصعيد الوطني						
	التنبيه والإنذار على الصعيد الوطني				X	x	
	بناء قدرات أفرقة الاستجابة للحوادث الحاسوبية في المؤسسات	x			X	x	
	نقطة اتصال وتنسيق موثوقة		x	x	X	x	X
	تكوين ثقافة الأمن السيبراني						
خدمات أفرقة الاستجابة للحوادث الحاسوبية المؤسسية التقليدية	التعامل مع الحوادث				X		X
	الاستجابة في الموقع	x					
	تنسيق الاستجابة للحوادث			x	X		x
	معالجة مواطن الضعف				X	x	x
	تحليل مواطن الضعف						
	الاستجابة لمواطن الضعف						
	معالجة الأشياء المصطنعة						X
	الرصد التكنولوجي				X		x
	خدمات اكتشاف الاقتحام	x			X		
	تقييمات المخاطر (مقدمة للبنية التحتية)				X		
	التثقيف والتدريب				X	x	x

وكما هو الشأن في كثيرٍ من الأحيان مع أي تحليل تستخدم فيه عوامل النجاح الحاسمة، لا تولد العملية النظامية نتائج تكون غير متوقعة تماماً. فعلى سبيل المثال، استناداً إلى معلومات تاريخية وأخرى مروية، يكون أداء دور المنسق الموثوق في كثير من الأحيان خدمة أساسية تدعم بشكل واسع مجموعة متنوعة من الوظائف، غير أن العمليات التحليلية النظامية تعين على إنماء التوافق بين المديرين وأصحاب المصلحة والمستفيدين الأساسيين. وفي حالة الفريق الوطني الخيالي محل الدراسة هنا، تدعم مصفوفة المقارنات بوضوح التوجه إلى إيلاء خدمة تنسيق أساسية أعلى درجات الدعم المبدئي، فهي خدمة عالية القيمة في سياق *هذا* الفريق الوطني. كما أن من شأن العملية النظامية أن تعين المديرين على التوصل إلى نتائج أخرى غير بارزة الوضوح، مثل ما يتسم به التوظيف في هذا الفريق الوطني تعييناً من عدم الاتساق مع الخدمات التي توجد إليها حاجة حقيقية.

13.5 تحديد أولويات القياس والمقاييس

من المجالات الأخرى التي يمكن الاستفادة من عوامل النجاح الحاسمة فيها تحديد أولويات القياس لمديري الأفرقة الوطنية، حيث يواجه التنفيذيون في أي مؤسسة في كثير من الأحيان مجموعة متنوعة من المعلومات على هيئة تقارير عن الأنشطة في مؤسساتهم، غير أن هذه المعلومات تكون في حالات كثيرة غير وجيهة أو غير مفيدة بالنسبة إلى المديرين الذين يحاولون تبين مدى سلامة مؤسساتهم ومدى تحقيقها لرسالتها.

فقد تكون التقارير في كثيرٍ من الأحيان موجهة أساساً إلى أجزاء أخرى من المؤسسة أو إلى تسهيل وظائف الأعمال العامة. وقد يتخذ ذلك في إطار مؤسسة ربحية شكل تقارير الحسابات المدينة أو تقارير مبيعات صنف معين. وفي بعض المؤسسات، لا يوجه إلا قدر قليل من الجهد صوب تزويد القيادات بمعلومات مخصصة بشأن سلامة المؤسسة في توقيت مناسب. ويكون من المفترض أحياناً أن بيئة التشغيل والعمل تتغير بسرعة تجعل من إعداد تقارير نظامية بشأن سلامة المؤسسة أمراً غير عملي، أو أنه من المفضل أن يتبين المديرون سلامة مؤسساتهم بمجرد التحدث مع موظفيهم وعملائهم.

وتهتم القيادات في العادة بالوقوف على مدى سلامة مؤسساتهم، إلا أن لقياس الجوانب غير الملموسة من الأداء المؤسسي كلفة تتخذ في العادة شكل ساعات عمالة وتكلفة الفرص. وعلى ذلك ينبغي تحديد متطلبات قادة المؤسسات من المعلومات بعناية. وتهيئ عوامل النجاح الحاسمة سبيلاً نافعاً لتبين هذه المتطلبات. وفي المثال التالي، تُعرض عوامل النجاح الحاسمة من فريقنا الوطني الخيالي جنباً إلى جنب مع بعض القياسات النموذجية التي تتعلق بكلٍ منها.

الجدول 4: قياسات نموذجية تدعم رسالة الفريق الوطني

عوامل النجاح الحيوية	المتطلبات المعلوماتية المقترحة
يجب اكتشاف أي حركة غير مصرح بها في الشبكات الحكومية	• عدد الحوادث من أول السنة حتى تاريخه المتعلقة بالإشارة إلى مضيف منتهَك أو ضار • معدل إيجابي زائف لقواعد اكتشاف الأحداث • النسبة المئوية لنقاط النفاذ الحكومية الخاضعة للرصد • تكرر تحديث معايير اكتشاف الأحداث
يجب السيطرة على أي دعاية سلبية بسبب الحوادث الأمنية	• عدد الاستفسارات الواردة إلى مسؤول اتصال الشؤون العامة المعين • النسبة المئوية للموضوعات الإخبارية المتعلقة بحوادث أمنية في قاعدة المستفيدين حيث لم يعلم الفريق الوطني بالحادثة إلا من وسائل الإعلام ذاتها • عدد الموضوعات الإخبارية المتعلقة بحوادث أمن حاسوبي بين قاعدة مستفيدي الفريق الوطني • عدد الاستفسارات الإعلامية التي أجاب عنها أفراد من الفريق الوطني غير مسؤول الاتصال الإعلامي المعين
يجب أن ينسق الموظفون مع الموردين	• عدد موردي تكنولوجيا المعلومات الذين يتعامل المستفيدون معهم مقابل عدد الموردين المقيدين في سجل الفريق الوطني

عوامل النجاح الحيوية	المتطلبات المعلوماتية المقترحة
يجب تكوين شراكات قوية مع الصناعة الخاصة	• عدد الحوادث التي أبلغ عنها مستفيدو القطاع الخاص طوعاً • عدد وتوجهات الاستفسارات الواردة من الصناعة الخاصة إلى الفريق الوطني حول التهديدات الأمنية الناشئة • عدد الدورات التدريبية المنفذة سنوياً لدى كبار أصحاب المصلحة المنتمين إلى الصناعة الخاصة
يجب الحد من مواطن الضعف بشكل سريع	• النسبة المئوية للحوادث المتكررة ذات التكلفة التي تزيد على حد معين وتنتج عن أسباب جذرية معروفة • زمن الدورة بين الإبلاغ عن موطن ضعف اليوم صفر وتنفيذ الإصلاح عبر قاعدة المستفيدين • النسبة المئوية للحوادث المبلغ بها التي تتعلق بمواطن ضعف معروفة ولا تقل مدتها عن 45 يوماً

ويمكن بدلاً من ذلك أن يكون لدى مديري الأفرقة الوطنية حصراً بالبلاغات *القائمة* حول أنشطة مؤسستهم ليختاروا منها، أو قد يجدوا أنفسهم أمام مهمة تحديد برمجيات لإدارة الحوادث قد توفر أنواعاً مختلفة من وظائف الإبلاغ. وفي هذه الحالة يمكن الاستعانة بتحليل التواؤم باستخدام عوامل النجاح الحاسمة – على نفس منوال المثال المقدم في القسم السابق – على تحديد أنواع البلاغات التي ينبغي الإبقاء عليها أو أنواع مرافق الإبلاغ التي من شأنها أن تكون الأنفع للمؤسسة.

14.5 الخلاصة

عوامل النجاح الحاسمة أدوات من شأنها إعانة المديرين في مؤسسات معقدة على اتخاذ قرارات في توقيتات مناسبة وتحديد أولويات خدماتهم وأصولهم. ومن المأمول أن تميئ المواد الواردة في هذا التقرير فهماً للكيفية التي يمكن بها لمديري الأفرقة الوطنية وغيرهم من أفرادها الاستفادة من تحديد عوامل النجاح الحاسمة واستعمالها بشكل نظامي في سبيل ربط أنشطتهم بنجاح مؤسستهم مباشرةً.

وتمثل إدارة فريق وطني للاستجابة للحوادث الحاسوبية تحدياً قيادياً فريداً ومعقداً، حيث تؤدي هذه المؤسسات دوراً حيوياً للغاية وتعين المستفيدين على الصعيد الوطني على فهم حوادث الأمن السيبراني والسيطرة عليها. ويجب أن تتطور إدارة الأفرقة الوطنية وتكتسب سمة نظامية حتى يكتمل دعمها للأمن السيبراني الوطني وتندمج بسلاسة في بيئات عملها الفريدة. والأفرقة الوطنية هذه مؤسسات متطورة من شأن أدوات مثل عوامل النجاح الحاسمة أن تعينها في مهام الإدارة المنوطة بها.

6 الفصل السادس: أفضل الممارسات المتعلقة بالأمن السيبراني – حماية شبكات مقدمي خدمات الإنترنت

1.6 مقدمة

تقع أشد مجالات مشكلة الشبكات الروبوتية وطأة في شبكات النطاق العريض السكنية المرتكزة على المستهلكين. وتمثل الشبكات الروبوتية مصدر قلق في الشبكات والخدمات المرتكزة على المؤسسات أيضاً، إلا أن الترتيبات المؤسسية في ذلك السياق أكثر تشعباً من سوق المستهلك السكني بكثير، كما يوجد بالفعل قدر أكبر من النشاط في السياق المؤسسي للاستجابة للشبكات الروبوتية. وعلى ذلك يركز هذا التقرير على تحديد أفضل الممارسات لمقدمي خدمات الإنترنت الذين يقدمون خدمات للمستهلكين على شبكات نطاق عريض سكنية.

وبالرغم من هذا التركيز فإن من شأن الكثير من أفضل الممارسات المبينة هنا أن يمثل ممارسات قيمة في حالة تطبيقها في سياقات الشبكات غير الاستهلاكية وغير السكنية. وفي ضوء التعقيد والتشعب الذي تتسم به الشبكات الفردية، والطبيعة سريعة التغير للتهديدات الأمنية من الشبكات الروبوتية، فينبغي تزويد الشبكات الفردية بالقدرة على الاستجابة للتهديدات الأمنية على أنسب نحو بالنسبة إلى الشبكة المعنية ذاتها.

ولا ينبغي اعتبار أفضل الممارسات هذه قائمة شاملة بجميع الخطوات التي يستطيع مقدمو خدمات الإنترنت اتخاذها في سبيل التعامل مع الشبكات الروبوتية والحواسيب المنتهَكة، بل إن الكثير من مقدمي الخدمات يتخذون بالفعل خطوات إضافية استجابةً لمشكلة الشبكات الروبوتية، ويعكف العديد منهم في كثير من الأحيان على تقييم التقنيات الجديدة أو الإضافية التي ينبغي النظر فيها، مما يتجاوز التدابير الأساسية المقترحة أدناه.

2.6 الهدف والنطاق والمنهجية

الهدف

يتفحص هذا التقرير الممارسات الحالية التي يوظفها مقدمو خدمات الإنترنت لحماية شبكاتهم من الأضرار المتسببة عن التوصيل المنطقي للمعدات الحاسوبية، علاوةً على الممارسات المستحسنة وما يقترن بذلك من معوقات في التنفيذ. وتعالج هذه الجهود تقنيات لتبين المعدات الحاسوبية المنخرطة في هجمات سيبرانية ضارة بشكل دينامي وإخطار المستخدم وعلاج المشكلة.

ويركز التقرير على العلاقة بين مقدمي خدمات الإنترنت والمستخدمين النهائيين في سياق النطاق العريض السكني (مشكلة أجهزة المستخدمين النهائيين المنتهَكة من قِبل الشبكات الروبوتية) ويبين أفضل الممارسات الفعالة لمقدمي خدمات الإنترنت في معالجة انتهاك أجهزة المستخدمين النهائيين.

النطاق

استشرى بسبب العلل الأمنية في المعدات و/أو البرمجيات التي يستخدمها المستهلكون، مقترنةً بتواضع ممارسات إدارة الأنظمة أو غيابها بالكلية لدى المستخدمين النهائيين، وباء من الحواسيب المنتهَكة على نحوٍ يتيح التحكم في كثير منها عن بُعد باعتبارها جزء مما يسمى في كثير من الأحيان "شبكات روبوتية". ويؤدي انتهاك هذه الحواسيب فوراً إلى تعريض مالكيها للخطر نظراً لإتاحتها رصد معلوماتهم الشخصية ومخاطباتهم.

يشمل مصطلح "المعدات الحاسوبية" على النحو المستخدم هنا مجموعة واسعة التنوع من المعدات الشخصية (مثل المخدمات والحواسيب الشخصية والهواتف الذكية والمسيّرات المترلية وما إلى ذلك) إضافةً إلى الأجهزة المترلية المزودة ضمنياً بتوصيل شبكي ببروتوكول الإنترنت. ويشير مصطلح "التوصيل المنطقي" إلى التشوير والنقل ببروتوكولات اتصالات بيانات المستخدمين النهائيين. وينتج الضرر عن إمكانية الحط من قدرات بنية الاتصالات التحتية من خلال تبادلات بروتوكولية ونقل معلومات ضارة مما قد يؤدي إلى تمكين من يتحكمون في الشبكة الروبوتية من استغلال القدرة الحاسوبية والنفاذ إلى الإنترنت. كما يمكن استعمال جيوش من هذه الحواسيب المنتَهكة بشكل مجمع لنشر رسائل اقتحامية وتخزين محتوى غير مشروع ونقله ولمهاجمة مخدمات تابعة لجهات حكومية وخاصة بهجمات مكثفة للحرمان من الخدمة الموزع.

ويتفحص هذا التقرير الممارسات الحالية التي يوظفها مقدمو خدمات الإنترنت لحماية شبكاتهم من الأضرار المتسببة عن التوصيل المنطقي للمعدات الحاسوبية، علاوةً على الممارسات المستحسنة وما يقترن بذلك من معوقات في التنفيذ. ويعالج هذا المصنف تقنيات لتبين المعدات الحاسوبية المنخرطة في هجمات سيبرانية ضارة بشكل دينامي وإخطار المستخدم وعلاج المشكلة. ويطرح التقرير توصيات لممارسات فضلى وإجراءات يمكن اتخاذها للإعانة على التغلب على معوقات التنفيذ.

وفيما يلي موجز لنتائج عروض واستشارات من خبراء:

- يمثل انتهاك الشبكات الروبوتية لأجهزة المستخدمين النهائيين مشكلة معتبرة تؤثر في جميع مقدمي خدمات الإنترنت أياً كان حجمهم.
- تنتشر برمجيات الشبكات الروبوتية الضارة بسرعة بين أجهزة المستخدمين النهائيين.
- يبدو أن المحرك للزيادة السريعة في إصابات الشبكات الروبوتية وتطورها التكنولوجي كان تمويلاً لتكنولوجيا الشبكات الروبوتية من عناصر إجرامية محنكة.
- تتحرك تكنولوجيا برمجيات الشبكات الروبوتية الضارة وإصاباتها وما ينتج عنها من آثار بسرعة تحول دون تمكن الطرائق والتكنولوجيات التي يوظفها قطاع مقدمي خدمات الإنترنت من التصدي لها.

- وتمثل الشبكات الروبوتية قضية معقدة تنطوي على مشاكل على صعيدي المستخدمين النهائيين والشبكات.
- ويجب أن تتضمن جهود مقدمي خدمات الإنترنت لمعالجة الشبكات الروبوتية تعاوناً وتقاسماً للمعلومات بينهم من أجل معالجة المشكلة بشكل تام.
- وتوجد بالفعل ممارسات فضلى (بما في ذلك بعض المعايير الصادرة عن فريق مهام هندسة الإنترنت) تعالج جوانب معينة في الشبكات الروبوتية (مثل ما يتعلق بالاستجابة للرسائل الاقتحامية) لكن لا يوجد حتى الآن نهج شامل محدد أو مطبق على نطاق واسع (في شبكات الولايات المتحدة على الأقل).
- وتثير طرائق اكتشاف الشبكات الروبوتية قضايا تتعلق بخصوصية المستخدمين النهائيين يلزم أخذها في الاعتبار في معرض تطوير نهج لمجابهة مشكلة الشبكات الروبوتية.
- ومن شأن تطبيق مقدمي خدمات الإنترنت الذين يخدمون مستهلكين على شبكات سكنية عريضة النطاق لأفضل الممارسات هذه، حسب الاقتضاء، أن يحد بشكل معتبر من مشكلة الشبكات الروبوتية في أجهزة المستخدمين النهائيين.

الخطوات التالية

يرسي هذا التقرير دعائم تقوم عليها معالجة مقدمي خدمات الإنترنت للبرمجيات الروبوتية في أجهزة المستخدمين النهائيين على شبكات النطاق العريض السكنية، مما يعين على الحد من أثر هجمات الشبكات الروبوتية على الشبكة. ومن الخطوات التالية المحتملة في التعامل مع البرمجيات الروبوتية والشبكات الروبوتية توسيع نطاق هذا العمل بحيث يتضمن وسائط الهجوم التي تستغل مواطن ضعف الشبكات لنشر البرمجيات الروبوتية والتهيئة للتعتيم على قنوات القيادة والسيطرة للشبكات الروبوتية. ويعرج هذا التقرير على هذا المجال استناداً إلى أعمال مبدئية في نظام أسماء الميادين والفضاء الدينامي والرسائل الاقتحامية، إلا أن هذا العمل يحتمل التوسع ليشمل تحسين الحماية من مواطن الضعف أمام الهندسة الاجتماعية وإصابة المواقع الإلكترونية العمومية ببرمجيات طروادية ذات علاقة بالبرمجيات الروبوتية وغيرها من البرمجيات الضارة، ومزيداً من العمل بشأن اكتشاف الشبكات وعزل حركة القيادة والسيطرة للبرمجيات الروبوتية.

وكما هو مذكور في قسم التوصيات، ينبغي إخضاع هذه الممارسات الفضلى للمراجعة والتحديث على فترات متلاحقة بحيث تعكس أحدث التكنولوجيات والطرائق في التعامل مع الشبكات الروبوتية. وعلاوةً على ذلك، من شأن أي أعمال إضافية للخروج بأفضل الممارسات في مجالات متركزة على شبكات غير شبكات النطاق العريض السكنية التي شكلت مرتكز هذا التقرير أن تمثل قيمة عالية.

إنشاء ممارسات فضلى جديدة

صُنفت أفضل الممارسات باعتبار الخطوات المنطقية اللازمة لمعالجة الشبكات الروبوتية إلى فئات منها المنع والاكتشاف وإخطار المستخدمين النهائيين والتخفيف من العواقب واعتبارات الخصوصية في اكتشاف البرمجيات الروبوتية وإخطار المستخدمين النهائيين. ويورد التذييل ألف أفضل الممارسات هذه.

أفضل ممارسات المنع

تستهدف أفضل ممارسات المنع الاثنتا عشرة منع إصابات الشبكات الروبوتية في أجهزة المستخدمين النهائيين والآثار الرئيسية التي تلحقها بشبكات مقدمي خدمات الإنترنت. وينصب التركيز الأساسي بالنسبة إلى المستخدمين النهائيين على سبل إعانة مقدمي خدمات الإنترنت للمستخدمين النهائيين لشبكات النطاق العريض السكنية على منع حدوث إصابات البرمجيات الروبوتية الضارة في أجهزتهم وشبكاتهم. ويتحقق ذلك بتحديد أفضل الممارسات لتوعية المستخدمين النهائيين وتثقيفهم بشأن أهمية تدابير الحفاظ على سلامة استخدام الإنترنت مثل التحديث المتواصل لأنظمة التشغيل والتطبيقات والوعي بحيل الهندسة الاجتماعية وما إلى ذلك والاستعانة ببرمجيات مكافحة الفيروسات على اكتشاف البرمجيات الضارة والروبوتية. ويجب على موظفي مقدمي خدمات الإنترنت مواكبة أحدث تكنولوجيات الشبكات الروبوتية والبرمجيات الضارة في سبيل معالجة مشاكل الشبكات الروبوتية بفعالية. وتعالج أفضل ممارسات المنع الشبكي سبل استغلال البرمجيات الروبوتية لنظام أسماء الميادين وفضاء

العناوين الدينامي ومنع الرسائل الاقتحامية النابعة عن برمجيات روبوتية (مما يعين على نشر البرمجيات الروبوتية والضارة وإحداث حالات ازدحام على الشبكات).

أفضل ممارسات الاكتشاف

تستهدف أفضل ممارسات الاكتشاف الخمس توفير إمكانيات فعالة لاكتشاف البرمجيات الروبوتية الموجهة إلى مقدمي خدمات الإنترنت وتقاسم المعلومات بين مقدمي خدمات الإنترنت. ونظراً للتطور المتزايد في الشبكات الروبوتية والتكنولوجيات سريعة التغير المستخدمة فيها، تمثل المداومة على تطبيق طرائق اكتشاف فعالة وتقاسم المعلومات أهمية حاسمة بالنسبة إلى معالجة حالات نشر الشبكات الروبوتية. كما تتناول الحاجة إلى توظيف طرائق اكتشاف غير متداخلة والتنفيذ في التوقيتات المناسبة.

أفضل ممارسات الإخطار

يلزم بمجرد اكتشاف الإصابة من شبكة روبوتية إخطار المستخدم النهائي حتى يمكن اتخاذ إجراء للتخفيف من العواقب. وتستهدف ممارستا الإخطار الفضليان المداومة على تطبيق طرائق إخطار فعالة وضمان توصيل معلومات خدمة حاسمة للمستخدمين النهائيين ممن يرجح إصابة أجهزتهم أو شبكاتهم ببرمجيات روبوتية. والمقترح تحقيق توازن حسن بين التيقن من الاكتشاف وسرعة الإخطار.

أفضل ممارسات التخفيف من العواقب

تستهدف ممارسات التخفيف من العواقب الفضلى الثلاث التخفيف من عواقب إصابات البرمجيات الروبوتية على أجهزة المستخدمين النهائيين وحماية المستخدمين النهائيين والشبكة من هجمات الشبكات الروبوتية. وتعالج أفضل ممارسات التخفيف من العواقب ضرورة إخطار مقدم خدمات الإنترنت المستخدمين النهائيين عن طريق تزويدهم بمعلومات عن كيفية معالجة أي إصابة محتملة من برمجيات روبوتية. كما توجد ممارسات فضلى محددة من أجل التعاون بين مقدمي خدمات الإنترنت في مواجهة الحوادث السيبرانية الحاسمة المحتمل تسببها عن هجمة شبكة روبوتية، علاوة على الحاجة المحتملة إلى العزل المؤقت للبرمجيات الروبوتية النشطة هجومياً للحد من احتمالات حدوث آثار سلبية على المستخدمين النهائيين أو الشبكة (مع ملاحظة أنه ينبغي الامتناع عن اتخاذ أي إجراء من هذا النوع إلا باعتباره "ملجأً أخيراً" أو غير ذلك من الظروف الحرجة، وأنه ينبغي في اتخاذ أي منها مراعاة حاجات المستخدمين المتأثرين).

أفضل ممارسات اعتبارات الخصوصية

يثير عدد من أفضل ممارسات المنع والاكتشاف والإخطار والتخفيف من العواقب القضية المتكررة المتمثلة في حماية معلومات المستخدم النهائي. ولمعالجة هذه الشواغل، يقدم التقرير ممارستين فضليين متركزتين على قضايا خصوصية المستخدمين النهائيين، حيث تتناول أولاهما احترام خصوصية المستهلكين فيما يتعلق بكشف معلومات العملاء في معرض معالجة إصابات البرمجيات الروبوتية وهجماتها، بينما تطرح الثانية استراتيجية متعددة الأوجه لتصميم تدابير تقنية لحماية خصوصية معلومات العملاء.

3.6 التحليل والنتائج والتوصيات

التحليل

يحدد التقرير أفضل الممارسات باعتبار الخطوات المنطقية اللازمة لمعالجة الشبكات الروبوتية. فأفضل ممارسات المنع هي التي تستهدف منع إصابات الشبكات الروبوتية وأثرها في شبكات مقدمي خدمات الإنترنت، بينما تستهدف أفضل ممارسات الاكتشاف اكتشاف مقدمي خدمات الإنترنت لإصابات الشبكات الروبوتية وهجماتها، وتستهدف أفضل ممارسات الإخطار إخطار المستخدمين النهائيين بإصابات الشبكات الروبوتية المحتملة، في حين تستهدف أفضل ممارسات التخفيف من العواقب التخفيف من عواقب إصابات الشبكات الروبوتية على أجهزة المستخدمين النهائيين الشبكة.

النتائج

تمثل الشبكات الروبوتية مشهداً سريع التحول من قدرات البرمجيات الضارة على الإصابة والقيادة والسيطرة والهجوم تغذيها أساساً رغبة في تحقيق مكاسب اقتصادية لدى من يطورون هذه الشبكات الروبوتية وينشرونها – وكثيراً ما يكونون مجرمين محنكين. ومن الممكن إلقاء قدر كبير من المسؤولية عن العدد الهائل من الإصابات التي تسببها وسائط الإصابة بالبرمجيات الضارة المتطورة على مواطن الضعف في أجهزة المستخدمين النهائيين، علاوةً على قصور في الفهم وما يستتبعه ذلك من قصور ردود الأفعال الوقائية من قِبل المستخدمين النهائيين أنفسهم.

وتنشأ الشبكات الروبوتية بمجرد إصابة جهاز ببرمجيات ضارة وتنشيطها عليه. حينئذٍ، تقيم البرمجيات الروبوتية اتصالاً مع نظام "القيادة والسيطرة" في الشبكة الروبوتية ثم تتحول في العادة إلى الخمول لتقليل احتمالات اكتشافها بينما ترتقب أوامر الهجوم من مالك الشبكة الروبوتية. وقد بلغ مستوى التطور مبلغاً يتيح تحديث البرمجيات الروبوتية بإصدارات جديدة من البرمجيات الروبوتية الضارة على فترات متلاحقة لإضافة قدرات هجومية وتقنيات تعتيم جديدة.

وتتألف الشبكة الروبوتية من جميع الروبوتات البرمجية المصابة الواقعة تحت قيادة وسيطرة مشتركة. وتكون البرمجيات الروبوتية الضارة ذاتها في بعض الأحيان متعددة الأشكال، مما يعوق الاكتشاف القائم على التوقيع على مستوى الجهاز. كما أن استخدام آليات القيادة والسيطرة المتطورة، مما يشمل استخدام تكنولوجيا الند-إلى-الند، يجعل من اكتشاف البرمجيات الروبوتية والشبكات الروبوتية أمراً صعباً. وتستغل آليات القيادة والسيطرة مواطن الضعف في البنية التحتية في الإنترنت ولدي مقدمي خدمات الإنترنت، مثل نظام أسماء الميادين، لتجنب اكتشاف حركة القيادة والسيطرة ولتهيئة وسائط إصابة لنشر البرمجيات الروبوتية الضارة بشكل ابتكاري.

وبمجرد انخراط جهاز المستخدم النهائي في شبكة روبوتية، تنشأ مخاطر على كلٍ من المستخدم النهائي وشبكة مقدم خدمات الإنترنت، حيث يتاح في هذه الحالة انتهاك سرية معلومات المستخدم النهائي الشخصية، مثل بيانات هويته حساباته المصرفية وبطاقات ائتمانه، كما يحتمل تعرض شبكة مقدم خدمات الإنترنت لهجمات الحرمان من الخدمة والرسائل الاقتحامية وغير ذلك من الهجمات ذات الصلة بالشبكات.

وتتطلب معالجة هذه المشاكل تعطيل دورة حياة الشبكة الروبوتية والعمل على التخفيف من عواقب البرمجيات الروبوتية الضارة التي أصابت الجهاز. ويلقي هذا التقرير الضوء على القضايا المتعلقة بالمستخدم النهائي وجهازه، علاوةً على بعض مواطن الضعف الرئيسية في الشبكات مما يعزز انتشار الشبكات الروبوتية ويزيد أثر الشبكات الروبوتية سوءاً.

ومن شأن تطبيق أفضل الممارسات المقترحة في سياق النطاق العريض السكني، حسب الاقتضاء، أن يؤدي إلى تخفيف عواقب مشكلة الشبكات الروبوتية بشكل معتبر. ويمكن من خلال النظر في الشبكات الروبوتية من منظور المنع والاكتشاف والإخطار والتخفيف من العواقب إنشاء برنامج متكامل يكون من شأنه أن يحدث أثراً معتبراً في الشبكات الروبوتية ووقعها على المستخدمين النهائيين وشبكات مقدمي خدمات الإنترنت. ويضم جل، لا كل، استراتيجيات السيطرة على الشبكات الروبوتية المدروسة عناصر من أفضل الممارسات.

وتؤيد هذه النتائج افتراض تحرك تكنولوجيا الشبكات الروبوتية ونشرها حتى الآن بخطىً أسرع من الطرائق المتبعة في قطاع مقدمي خدمات الإنترنت لمجابهتها. ومن القواسم المشتركة ضمن النتائج فكرة تمثيل التعاون مع المستخدم النهائي ومقدمي خدمات الإنترنت الآخرين أهمية حاسمة على مسار معالجة هذه القضية بفعالية. ولا توجد عصا سحرية تمحو هذه المشكلة بالكلية، بل تقتضي معالجة الشبكات الروبوتية بشكل شامل إقامة شراكة مع المستخدمين النهائيين ومقدمي خدمات الإنترنت الآخرين.

4.6 التوصيات

يبين التقرير أن النمو السريع في الشبكات الروبوتية في أجهزة المستخدمين النهائيين كان ومازال أسرع من القدرة على معالجة المشكلة بفعالية، ويشجع بقوة بناءً على ذلك بذل جهود معتبرة تتجاوز تطبيق أفضل الممارسات. وقد نتجت التوصيات التالية عن أبحاث الفريق وعمله على إعداد أفضل الممارسات:

- نظراً للنمو السريع للشبكات الروبوتية والتغير السريع في التكنولوجيا، ينبغي مراجعة أفضل الممارسات المتعلقة بالشبكات الروبوتية كل عامين على الأقل.
- ينبغي تحديد طرائق موحدة لتقاسم المعلومات مع المستخدمين النهائيين وفيما بين مقدمي خدمات الإنترنت على نحوٍ أفضل.
- تمثل حماية (واستبعاد) معلومات العملاء مما قد يجمعه مقدمو خدمات الإنترنت خلال معالجة الشبكات الروبوتية قضية مهمة تستدعي انتباهاً متواصلاً.
- ينبغي إجراء قياسات مرجعية على تطبيق مقدمي خدمات الإنترنت لأفضل ممارسات الشبكات الروبوتية لتكوين فكرة أفضل عن كيفية تعامل مقدمي خدمات الإنترنت مع مشكلة الشبكات الروبوتية.

ومن الإجراءات الإضافية المحتملة على صعيد السياسات ما يلي:

- إنشاء موقع إلكتروني لمكافحة الشبكات الروبوتية، ربما بتمويل حكومي، يتاح للمستخدمين النهائيين لإعانتهم على إزالة البرمجيات الروبوتية الضارة من أجهزتهم، مما يشبه مراكز مكافحة الشبكات الروبوتية التي أقيمت في ألمانيا (انظر http://botfrei.de) واليابان (انظر https://www.ccc.go.jp/en_ccc/)؛
- إطلاق حملة إعلامية عامة عن الأمن السيبراني تتضمن توعية بالشبكات الروبوتية؛
- تكوين مركز معلومات وموارد لأفرقة التأهب لحالات الطوارئ الحاسوبية يتاح لمقدمي خدمات الإنترنت والمستخدمين النهائيين، بحيث يخصص لاكتشاف الشبكات الروبوتية والتخفيف من عواقبها وما إلى ذلك؛
- يمكن التشجيع على إدخال تحسينات على تكنولوجيا الاكتشاف الشبكي لقيادة وسيطرة الشبكات الروبوتية واستغلالها للحركة من خلال إجراء أبحاث في جهات حكومية أو غيرها.

5.6 الخلاصة

يحدد هذا التقرير 24 ممارسة فضلى لمعالجة أجهزة المستخدمين النهائيين المصابة ببرمجيات روبوتية ووقع الشبكات الروبوتية على المستخدمين النهائيين وشبكات مقدمي خدمات الإنترنت. وتشكل أفضل الممارسات هذه دعائم لمعالجة هذه المشكلة المتنامية، وهي موجهة إلى مقدمي خدمات الإنترنت الذين يقدمون خدمات للمستهلكين على شبكات نطاق عريض سكنية كي ينظروا فيها. ومن الأعمال المستقبلية المحتملة مراجعة أفضل الممارسات هذه بانتظام لتواكب المستجدات ومن أجل تحقيق توسيع محتمل في نطاق أعمال أفضل الممارسات في المستقبل الرامية إلى تحديد ممارسات فضلى تستهدف معالجة انتشار البرمجيات الروبوتية الضارة من خلال الشبكة واكتشاف حركة القيادة والسيطرة للشبكات الروبوتية وتعطيلها.

وقد رُتبت أفضل الممارسات الجديدة على مجالات المنع (12 ممارسة فضلى) والاكتشاف (5 ممارسات فضلى) والإخطار (ممارستان فضليان) والتخفيف من العواقب (3 ممارسات فضلى). كما حددت علاوة على ذلك ممارستان فضليان في مجال اعتبارات الخصوصية المتعلقة بمعلومات العملاء في سياق معالجة الشبكات الروبوتية.

ومن بالغ الأهمية ملاحظة أن أفضل الممارسات ليست قابلة للتطبيق على جميع الحالات نظراً لعوامل متعددة، ولذلك فالمقصود أن يكون تطبيق أفضل الممارسات هذه اختيارياً لمقدمي خدمات الإنترنت. ومن شأن فرض مجموعة محددة من أفضل الممارسات إلزاماً أن يسهم في إضعاف تشغيل الشبكات وموثوقيتها أو أن يؤدي إلى عواقب سلبية أخرى.[29]

[29] انظر **الملحق دال** للاطلاع على مزيدٍ من المراجع المتعلقة بأفضل ممارسات حماية شبكات مقدمي خدمات الإنترنت.

ومع أخذ هذه القيود في الاعتبار، يوصي هذا التقرير بتطبيق مقدمي خدمات الإنترنت للتوصيات الواردة في التذييل ألف، حسب الاقتضاء، في سبيل معالجة مشكلة الشبكات الروبوتية المتنامية في أجهزة المستخدمين النهائيين وشبكات مقدمي خدمات الإنترنت.

7 العمل المقبل

يظل الأمن السيبراني أحد الشواغل الرئيسية بالنسبة لجميع المجتمعات. وتناولت المسألة العديد من القضايا التي أثيرت في اختصاصات فترة الدراسة هذه. وما زالت المجالات التالية مفتوحة:

- على الرغم من إجراء دراسة استقصائية، يود الفريق المعني بالمسألة إعطاء وقت إضافي لجميع الأعضاء للرد، ولذلك يُقترح أن تتم الدراسة الاستقصائية خلال فترة الدراسة التالية.
- يستمر تطور أشكال الرسائل الاقتحامية عبر البريد الإلكتروني وتهديدات أخرى وكذلك التدابير المضادة لمكافحتها. ويُقترح مواصلة هذا العمل.
- استجابة لنشاط التنسيق المشترك بشأن حماية الأطفال على الخط (JCA-COP)، يُقترح مواصلة العمل بشأن حماية الأطفال على الخط مع التركيز على الخبرات والشواغل الوطنية.
- وفي نفس السياق، نظراً لأن الأعضاء كانوا نشطين جداً في الإعراب عن شواغلهم وخبراتهم الوطنية فيما يتعلق بالأمن السيبراني، ينبغي الاستمرار في الخلاصة الوافية التي أُنتجت.

ينبغي القيام بجميع هذه الأعمال بالتعاون الوثيق مع برنامج مكتب تنمية الاتصالات ذي الصلة والقطاعين الآخرين والمنظمات المختصة.

التذييل ألف: مقدمة إلى أفضل الممارسات

الممارسات الفضلى هذه عبارة عن توجيهات إرشادية لأفضل نهج لمعالجة شاغلٍ ما. وهي تنطوي على حصاد تعاون على مستوى الصناعة تفاعلت خلاله خبرات هائلة وموارد معتبرة. والمقصود أن يكونَ تطبيق أفضل الممارسات هذه اختيارياً وأن يترك اتخاذ قرارات بشأن تطبيق إحداها من عدمه للمؤسسة المسؤولة (مثل مقدم الخدمة أو مشغل الشبكة أو مورد المعدات). وعلاوة على ذلك، تعتمد قابلية كل ممارسة فضلى للتطبيق تحت ظرف معين على عوامل كثيرة يتعين تقييمها بمعرفة أفراد لديهم خبرات وتجارب ملائمة في نفس المجال الذي تعالجه الممارسة الفضلى موضع النظر.

ولا يتسق فرض تطبيق أفضل الممارسات هذه إلزاماً مع المقصود منها. ولا يمكن تطبيق أفضل الممارسات هذه بشكل ملائم إلا بمعرفة أفراد لديهم دراية كافية بمعمارية البنية التحتية لشبكة الشركة تحديداً لفهم مقتضياتها. وقد صيغت أفضل الممارسات هذه على نحوٍ يسهل فهمها، إلا أن ذلك لا يقتضي ظهور معناها لمن لا يستوفي ذلك الشرط المسبق المذكور من المعرفة والخبرة. ويتطلّب التطبيق السليم فهم أثر الممارسة الفضلى في الأنظمة والعمليات والمؤسسات والشبكات والمشتركين وعمليات الأعمال وقضايا التكلفة المعقدة وغير ذلك من الاعتبارات. ولهذه الأسباب، لا يوصي هذا التقرير هنا بفرض السلطات الحكومية أفضل الممارسات هذه على الصناعة، كأن يكون ذلك من خلال لوائح تنظيمية مثلاً.

أفضل ممارسات المنع

من الجدير بالملاحظة أن أفضل الممارسات الواردة في هذه المجموعة موجهة أساساً إلى مقدمي خدمات الإنترنت الذين يقدمون خدماتهم إلى مستخدمين نهائيين أفراد على شبكات نطاق عريض سكنية، إلا أنها قد تكون قابلة للتطبيق على مستخدمين آخرين وشبكات أخرى كذلك.

ألف.1 الممارسة الفضلى رقم: منع 1

مواكبة مستجدات تقنيات البرمجيات الروبوتية/الضارة:

ينبغي لمقدمي خدمات الإنترنت مواكبة آخر مستجدات تقنيات البرمجيات الروبوتية/الضارة تأهباً لاكتشافها ومنعها.[30]

ألف.2 الممارسة الفضلى رقم: منع 2

توفير مقدمي خدمات الإنترنت موارد تعليمية بشأن سلامة الحواسيب / الحوسبة الآمنة:

ينبغي لمقدمي خدمات الإنترنت تزويد عملائهم بموارد تعليمية وتثقيفية وذاتية التوجيه أو دعم ما يتيحه آخرون من ذلك بغية تثقيف العملاء بشأن أهمية الحوسبة الآمنة وإعانتهم على تطوير ممارسات آمنة للحوسبة الآمنة.[31] وينبغي لمقدمي خدمات الإنترنت الإلمام بكيفية حماية أجهزة المستخدمين النهائيين وشبكاتهم من النفاذ غير المصرح به من خلال طرائق متنوعة، تتضمن على سبيل المثال لا الحصر ما يلي:

- استخدام برمجيات أمنية مشروعة تحمي من الفيروسات وبرمجيات التجسس؛
- التأكد من ورود أي برمجيات تنزل أو تشترى من مصدر مشروع؛
- استخدام جدران حماية؛
- ضبط تشكيل الحاسوب بحيث ينزل التحديثات الحاسمة لكلٍ من نظام التشغيل والتطبيقات المثبتة تلقائياً؛
- فحص الحاسوب بانتظام بحثاً عن برمجيات تجسس وغير ذلك من البرمجيات غير المرغوبة؛
- المداومة على تحديث برمجيات جميع التطبيقات وإضافات التطبيقات ونظام التشغيل واستخدام مزاياها الأمنية؛
- توخي الحذر عند فتح مرفقات رسائل البريد الإلكتروني؛
- الاحتراس عند تنزيل برامج والاطلاع على الصفحات الإلكترونية؛
- استخدام التراسل الفوري بحصافة؛
- استخدام مواقع التواصل الاجتماعي بشكل آمن؛

---

[30] الممارسة الفضلى منع 1: مراجع/تعليقات: انظر الوثيقة التالية للاطلاع على مزيدٍ من المعلومات: www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf
كما يمكن الوصول إلى مزيدٍ من المعلومات في: isc.sans.edu/index.html، www.us-cert.gov/
www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

[31] الممارسة الفضلى منع 2: مراجع/تعليقات: يمكن الوصول إلى مزيدٍ من المعلومات في:
التحالف الوطني للأمن السيبراني – www.staysafeonline.org/
OnGuard Online -www.onguardonline.gov/default.aspx
وزارة الأمن الداخلي – StopBadware – www.stopbadware.org/home/badware_prevent
Comcast.net Security - security.comcast.net/
Verizon Safety & Security – www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_safety
موقع Qwest Incredible Internet Security: www.incredibleinternet.com/
Microsoft – www.microsoft.com/security/pypc.aspx

- استخدام كلمات مرور قوية؛
- الامتناع تماماً عن الإفصاح عن كلمات المرور لآخرين.

ألف.3 الممارسة الفضلى رقم: منع 3

توفير مقدمي خدمات الإنترنت برمجيات لمكافحة الفيروسات/التأمين:

ينبغي لمقدمي خدمات الإنترنت إتاحة برمجيات و/أو خدمات لمكافحة الفيروسات/التأمين لمستخدميهم النهائيين.[32] وينبغي إذا لم يوفر مقدم خدمة الإنترنت البرمجيات/الخدمة مباشرة أن يتيح روابط إلى برمجيات/خدمات أخرى من خلال موارده التعليمية المتعلقة بالحوسبة الآمنة.

ألف.4 الممارسة الفضلى رقم: منع 4

حماية مخدمات نظام أسماء الميادين:

ينبغي لمقدمي خدمات الإنترنت حماية ما عندهم من مخدمات نظام أسماء الميادين من هجمات انتحال نظام أسماء الميادين واتخاذ خطوات لضمان منع أنظمة العملاء المنتهَكة من بث حركة انتحالية (وبالتالي المشاركة في هجمات تضخيم نظام أسماء الميادين).[33] ومن بين التدابير الدفاعية ما يلي:

- إدارة حركة نظام أسماء الميادين بما يتسق مع الإجراءات المقبولة في أوساط الصناعة؛
- حصر النفاذ إلى محللات نظام أسماء الميادين التكرارية على المستخدمين المصرح لهم متى ما أمكن ذلك؛
- حجب حركة الاستعلام الانتحالي لنظام أسماء الميادين عند حدود شبكاتهم؛
- التحقق من التشكيل التقني لمخدمات نظام أسماء الميادين بانتظام وذلك، على المثال،
- استخدام أدوات الاختبار المتاحة التي تتحقق من سلامة التشكيل التقني لمخدمات نظام أسماء الميادين.

ألف.5 الممارسة الفضلى رقم: منع 5

استخدام تمديدات أمن نظام أسماء الميادين (DNSSEC)

ينبغي لمقدمي خدمات الإنترنت استعمال تمديدات أمن نظام أسماء الميادين (DNSSEC) لحماية نظام أسماء الميادين.[34] وينبغي لمقدمي خدمات الإنترنت النظر، كحد أدنى، فيما يلي:

- التوقيع على ما عندهم من مناطق نظام أسماء الميادين واختبار صلاحيتها بانتظام؛

---

[32] الممارسة الفضلى منع 3: مراجع/تعليقات: لا يوجد

[33] الممارسة الفضلى منع 4: مراجع/تعليقات: تتناول الوثيقة التالية إجراءات إدارة حركة نظام أسماء الميادين المقبولة على نطاق واسع: www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_201006.pdf
وتتناول الممارسة الفضلى الحالية 140/المعيار 5358 من فريق مهام هندسة الإنترنت قضايا الأمن المتعلقة بالمحللات التكرارية. وتتناول الممارسة الفضلى الحالية 38/المعيار 2827 من فريق مهام هندسة الإنترنت الاستجابات للحركة الانتحالية، بما في ذلك الحركة الانتحالية ضمن نظام أسماء الميادين. ومن الأدوات التي تفحص مختلف جوانب تأمين مخدمات نظام أسماء الميادين ما يلي:
dnscheck.iis.se/
recursive.iana.org/
www.dnsoarc.net/oarc/services/dnsentropy
www.iana.org/reports/2008/cross-pollination-faq.html

[34] الممارسة الفضلى منع 5: مراجع/تعليقات: يمكن الوصول إلى مزيدٍ من المعلومات في:
www.dnssec.net
www.dnssec-deployment.org

- التحقق بانتظام من صلاحية توقيعات تمديدات أمن نظام أسماء الميادين للمناطق الأخرى؛
- توظيف طرائق مؤتمتة لاختبار المناطق الموقع عليها بتمديدات أمن نظام أسماء الميادين بانتظام للتحقق من صلاحية توقيعات تمديدات أمن نظام أسماء الميادين.

ألف.6 الممارسة الفضلى رقم: منع 6

التشجيع على استخدام بروتوكول نقل البريد البسيط المستيقن منه/حصر توصيلات الصادر على المنفذ 25.

ينبغي لمقدمي خدمات الإنترنت تشجيع المستخدمين على إرسال رسائل البريد الإلكتروني عبر بروتوكول نقل البريد البسيط المستيقن منه على المنفذ 587، مع اشتراط أمن طبقة النقل أو غير ذلك من الطرائق الملائمة لحماية اسم المستخدم وكلمة المرور.[35] كما ينبغي لمقدمي خدمات الإنترنت علاوة على ذلك حصر توصيلات الوارد والصادر من الشبكة، أو التحكم فيها بأي شكل آخر، على المنفذ 25 (بروتوكول نقل البريد البسيط) لأي شبكة أخرى، على أن يكون ذلك بشكل منتظم أو لكل حالة على حدة، كأن ينفذ ذلك لمخدمات البريد الإلكتروني المصرح بها على سبيل المثال.

ألف.7 الممارسة الفضلى رقم: منع 7

الاستيقان من البريد –الإلكتروني:

ينبغي لمقدمي خدمات الإنترنت الاستيقان من جميع رسائل البريد الإلكتروني الصادرة باستخدام البريد مثبت الهوية بمفاتيح الميدان (DKIM) وإطار سياسات المرسل (SPF).[36] وينبغي فحص الاستيقان على رسائل البريد الإلكتروني الواردة، كما ينبغي التحقق من توقيعات البريد مثبت الهوية بمفاتيح الميدان وسياسات إطار سياسات المرسل.

ألف.8 الممارسة الفضلى رقم: منع 8

الرفض الفوري– للبريد الإلكتروني غير القابل للتسليم

ينبغي لمقدمي خدمات الإنترنت تشكيل مخدمات معابر البريد بحيث ترفض فوراً رسائل البريد الإلكتروني غير القابلة للتسليم، لا أن تقبلها ثم تصدر إخطارات بعدم التسليم لاحقاً، وذلك لتجنب إرسال هذه الإخطارات لعناوين مزيفة.[37]

ألف.9 الممارسة الفضلى رقم: منع 9

حجب رس–ائل البريد الإلكتروني من الفضاء الدينامي:

ينبغي لمقدمي خدمات الإنترنت الامتناع عن قبول رسائل البريد الإلكتروني النابعة من مخدمات بريد في مجموعات عناوين بروتوكول الإنترنت مخصصة دينامياً، كما ينبغي لهم النظر في استخدام إحدى الخدمات المتاحة التي تتبين هذا النوع من المجموعات.[38]

---

[35] الممارسة الفضلى منع 6: مراجع/تعليقات: انظر الوثيقة التالية للحصول على مزيدٍ من المعلومات:
www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

[36] الممارسة الفضلى منع 7: مراجع/تعليقات: انظر الوثيقة التالية للحصول على مزيدٍ من المعلومات:
www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_200807.pdf
يمكن الوصول إلى مزيدٍ من المعلومات في:
www.dkim.org/
www.openspf.org

[37] الممارسة الفضلى منع 8: مراجع/تعليقات: يؤدي رفض معبر البريد الرسائل غير القابلة للتسليم إلى إبلاغ مخدم البريد المرسل بذلك، ويستطيع هذا الأخير تطبيق السياسة المحلية بشأن إخطار مرسل الرسالة بتعذر تسليم الرسالة الأصلية. انظر الوثيقة التالية للحصول على مزيدٍ من المعلومات: www.maawg.org/sites/maawg/files/news/MAAWG-BIAC_Expansion0707.pdf

[38] الممارسة الفضلى منع 9: مراجع/تعليقات: لا يوجد

ألف.10 الممارسة الفضلى رقم: منع 10

تقاسم معلومات فضاء العناوين الدينامي:

ينبغي لمقدمي خدمات الإنترنت تقاسم قوائم ما عندهم من عناوين بروتوكول الإنترنت الدينامية مع القائمين على قوائم حجب نظام أسماء الميادين وغيرها من الأدوات المشابهة. كما ينبغي إتاحة هذه القوائم بشكل عام، كأن يكون ذلك عبر موقع إلكتروني عمومي.[39]

ألف.11 الممارسة الفضلى رقم: منع 11

تسهيل تحديد هوية فضاء عناوين IPv4 الدينامي عن طريق نمط نظام أسماء الميادين العكسي:

ينبغي لمقدمي خدمات الإنترنت تسهيل تحديد هوية ما يقومون على إدارته من فضاء عناوين دينامي بالإصدار الرابع من بروتوكول الإنترنت، ويفضل أن يكون ذلك من خلال سلسلة ارتكاز أيمن بنمط لاحق مختار حتى يمكن القول، على سبيل المثال، بأن جميع سجلات نظام أسماء الميادين التي تنتهي بالسلسلة <some.text.example.com.*> هي التي تحدد هوية الفضاء الدينامي.[40]

ألف.12 الممارسة الفضلى رقم: منع 12

تسهيل تحديد هوية فضاء العناوين الدينامي عن طريق WHOIS:

ينبغي لمقدمي خدمات الإنترنت تسهيل تحديد هوية كل ما يقومون على إدارته من فضاء عناوين دينامي عن طريق استطلاع WHOIS أو RWHOIS.[41]

---

[39] الممارسة الفضلى منع 10: مراجع/تعليقات: يمكن الوصول إلى مزيدٍ من المعلومات في:
www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf
www.spamhaus.org/pbl/
www.mail-abuse.com/nominats_dul.html

[40] الممارسة الفضلى منع 11: مراجع/تعليقات: راجع الممارسة الفضلى منع 5 ذات الصلة.

[41] الممارسة الفضلى منع 12: مراجع/تعليقات: انظر الوثيقة التالية للحصول على مزيدٍ من المعلومات:
www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf
راجع الممارسة الفضلى منع 4 ذات الصلة.

أفضل ممارسات الاكتشاف

من الجدير بالملاحظة أن أفضل الممارسات الواردة في هذه المجموعة موجهة أساساً إلى مقدمي خدمات الإنترنت الذين يقدمون خدماتهم إلى مستخدمين نهائيين أفراد على شبكات نطاق عريض سكنية، إلا أنه قد تكون قابلة للتطبيق على مستخدمين آخرين وشبكات أخرى كذلك.

ألف.13 الممارسة الفضلى رقم: اكتشاف 1

إبلاغ مقدمي خدمات الإنترنت الآخرين بتنفيذ الوعي الظرفي وتدابير حماية:

ينبغي لمقدمي خدمات الإنترنت بذل جهود معقولة في سبيل التواصل مع غيرهم من المشغلين ومقدمي البرمجيات الأمنية، وذلك عن طريق إرسال و/أو استقبال بلاغات سوء الاستخدام عبر طرائق يدوية أو مؤتمتة.[42] وقد تتضمن هذه الجهود معلومات مثل تنفيذ "تدابير حماية" ومنها على سبيل المثال الإبلاغ عن سوء الاستخدام (الرسائل الاقتحامية مثلاً) عبر عروات تغذية راجعة باستخدام أنساق رسائل موحدة مثل نسق الإبلاغ عن سوء الاستخدام ARF. كما ينبغي لمقدمي خدمات الإنترنت، متى ما أمكن، الانخراط في جهود مع مشاركين آخرين من أوساط الصناعة وأعضاء آخرين في منظومة الإنترنت ترمي إلى تحقيق هدف تنفيذ تقاسم المعلومات بشكل أقوى وموحد في مجال اكتشاف الشبكات الروبوتية بين موردي القطاع الخاص.

ألف.14 الممارسة الفضلى رقم: اكتشاف 2

المداومة على اتباع طرائق لاكتشاف إصابات البرمجيات الروبوتية/الضارة:

ينبغي لمقدمي خدمات الإنترنت المداومة على استخدام طرائق لاكتشاف الإصابة المحتملة ببرمجيات ضارة في معدات العملاء. وتتنوع طرائق الاكتشاف تنوعاً واسعاً يعزى إلى مجموعة عوامل مختلفة.[43] وقد تشمل طرائق الاكتشاف وأدواته وعملياته على سبيل المثال لا الحصر: التغذية الراجعة الخارجية وملاحظة أحوال الشبكة وحركتها، مثل عرض النطاق و/أو تحليل أنماط الحركة، والتوقيعات وتقنيات السلوك والرصد الجنائي للعملاء على مستوى أكثر تفصيلاً.

---

[42] الممارسة الفضلى اكتشاف 1: مراجع/تعليقات: انظر الوثيقة التالية للحصول على مزيدٍ من المعلومات: www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf. ويمكن الإبلاغ عن مواطن الضعف على نحو موحد باستخدام المعلومات الواردة في nvd.nist.gov/
انظر أيضاً
puck.nether.net/mailman/listinfo/nsp-security
ops-trust.net/
www2.icsalabs.com/veris/

[43] الممارسة الفضلى اكتشاف 2: مراجع/تعليقات: انظر
www.team-cymru.org
www.shadowserver.org
www.abuse.ch
cbl.abuseat.org

ألف.15 الممارسة الفضلى رقم: اكتشاف 3

استخدام نهج طبقي لاكتشاف البرمجيات الروبوتية

ينبغي لمقدمي خدمات الإنترنت اتباع نهج طبقي لاكتشاف الشبكات الروبوتية، بحيث تطبق أولاً خصائص سلوكية لحركة المستخدمين (البحث الموسع) ثم تطبق تقنيات أكثر دقة (مثل اكتشاف التوقيعات) على الحركة التي يتبين احتمال تمثيلها مشكلة.[44]

ألف.16 الممارسة الفضلى رقم: اكتشاف 4

الامتناع عن حجب الحركة المشروعة:

ينبغي لمقدمي خدمات الإنترنت التأكد من عدم إفضاء طرائق الاكتشاف إلى حجب حركة مشروعة في معرض إجراء عمليات اكتشاف الشبكات الروبوتية، وينبغي لهم ببساطة بدلاً من ذلك توظيف طرائق اكتشاف تتسم بالشفافية وتجنب التعطيل لعملائهم وتطبيقات عملائهم.[45]

ألف.17 الممارسة الفضلى رقم: اكتشاف 5

ينبغي اتسام اكتشاف البرمجيات الروبوتية وما يناظره من إخطار بالسرعة:

ينبغي لمقدمي خدمات الإنترنت التأكد من اتسام اكتشاف البرمجيات الروبوتية وما يناظره من إخطار للمستخدمين النهائيين بالسرعة، حيث إن هذه المشاكل الأمنية حساسة من حيث الزمن.[46] أما في حالة اللجوء إلى إجراء تحليلات معقدة والتأكد عدة مرات من وجود برمجيات روبوتية بالفعل، فيمكن حينئذٍ أن تتسبب البرمجيات الضارة في إلحاق الأذى بالمضيف المصاب أو النظام المستهدف عن بُعد (مما يتجاوز ضرر الإصابة المبدئية) قبل أن يمكن إيقافها. وعلى ذلك، يتعين على مقدم خدمات الإنترنت تحقيق التوازن بين الرغبة في التيقن دون شك من الإصابة ببرمجيات ضارة، مما من شأنه أن يستغرق فترة زمنية مطولة، والقدرة على التنبؤ بالاحتمال القوي للإصابة ببرمجيات ضارة في فترة زمنية بالغة القصر. وما تحدي "التيقن مقابل الاحتمال" هذا باليسير، وينبغي لمقدم خدمات الإنترنت إذا وقع في الشك أن يجنح إلى الحذر عن طريق الإبلاغ بإصابة محتملة ببرمجيات ضارة مع اتخاذ خطوات معقولة لتجنب أي بلاغات كاذبة في نفس الوقت.

[44] الممارسة الفضلى اكتشاف 3: مراجع/تعليقات: ينبغي أن تساعد هذه التقنية على التقليل من كشف معلومات العملاء إلى الحد الأدنى في معرض اكتشاف البرمجيات الروبوتية وذلك عن طريق الامتناع عن جمع معلومات تفصيلية إلى أن يوجد مبرر معقول للاعتقاد بأن العميل مصاب. وقد يتضمن نهج البحث الموسع في حركة المستخدمين تلقي تغذية رجعية خارجية علاوة على نُهُج داخلية أخرى.

[45] الممارسة الفضلى اكتشاف 4: مراجع/تعليقات: لا يوجد

[46] الممارسة الفضلى اكتشاف 5: مراجع/تعليقات: لا يوجد

أفضل ممارسات الإخطار

من الجدير بالملاحظة أن أفضل الممارسات الواردة في هذه المجموعة موجهة أساساً إلى مقدمي خدمات الإنترنت الذين يقدمون خدماتهم إلى مستخدمين نهائيين أفراد على شبكات نطاق عريض سكنية، إلا أنه قد تكون قابلة للتطبيق على مستخدمين آخرين وشبكات أخرى كذلك.

ألف.18 الممارسة الفضلى رقم: إخطار 1

إخطار المستخدمين النهائيين:

ينبغي لمقدمي خدمات الإنترنت أن يداوموا على استخدام طرائق إخطار حاسمة لإبلاغ عملائهم باحتمال إصابة حاسوبهم و/أو شبكتهم ببرمجيات ضارة.[47] وينبغي أن يتضمن هذا خيارات متعددة لاستيعاب مجموعة متنوعة من العملاء وتكنولوجيات الشبكات. وينبغي بمجرد اكتشاف مقدم خدمات الإنترنت مشكلة أمنية محتملة عند مستخدم نهائي اتخاذ خطوات لإبلاغ مستخدم الإنترنت باحتمال مواجهته مشكلة أمنية. كما ينبغي لمقدم خدمات الإنترنت اتخاذ قرار بشأن أنسب طريقة أو طرائق لإخطار عملائه أو مستخدمي الإنترنت التابعين له، كما ينبغي له استخدام طرائق أخرى إن ثبتت للطريقة المختارة عدم الفعالية. وقد تختلف خيارات الإبلاغ حسب ما تنطوي عليه المشكلة من حدة/حرج. ومن طرائق الإخطار المتنوعة، على سبيل المثال لا الحصر: البريد الإلكتروني والاتصال الهاتفي والبريد العادي والتراسل الفوري وخدمة الرسائل القصيرة والإخطار عن طريق برنامج تصفح الويب.

ألف.19 الممارسة الفضلى رقم: إخطار 2

معلومات الإخطار للمستخدمين النهائيين:

ينبغي لمقدمي خدمات الإنترنت التأكد من احتواء الإخطارات بالشبكات الروبوتية الموجهة إلى المشتركين على معلومات خدمة حاسمة لا الإعلان عن خدمات جديدة أو غير ذلك من العروض.[48]

---

[47] الممارسة الفضلى إخطار 1: مراجع/تعليقات: يعتمد قرار مقدم خدمات الإنترنت بشأن أنسب طريقة أو طرائق إخطار عميل واحد أو أكثر من عملائه أو مستخدمي الإنترنت التابعين له على عدة عوامل بدءاً بقدرات مقدم خدمات الإنترنت التقنية إلى السمات التقنية لشبكته واعتبارات التكلفة وموارد المخدمات المتاحة والموارد المؤسسية المتاحة وعدد الأجهزة المضيفة التي يحتمل تعرضها للإصابة المكتشفة في أي وقت بعينه وشدة أي تهديدات محتملة، وعوامل أخرى كثيرة. ويسهل إلى حد معقول على مقدم خدمات إنترنت استخدام طرائق إخطار متعددة متزامنة، لكن ذلك قد يصعب على مورد برمجيات مكافحة فيروسات زائفة.

وتحتوي الممارسة الفضلى تخفيف 3 على معلومات بشأن كيفية معالجة الإصابة ببرمجيات ضارة.

[48] الممارسة الفضلى إخطار 2: مراجع/تعليقات: المقصد من هذه الممارسة الفضلى الإعانة على ضمان عدم حدوث التباس بين رسالة الإخطار وغير ذلك من المخاطبات مما قد يتلقاه العميل من مقدم الخدمات والإعانة كذلك على إبراز خطورة الموقف.

أفضل ممارسات التخفيف من العواقب

من الجدير بالملاحظة أن أفضل الممارسات الواردة في هذه المجموعة موجهة أساساً إلى مقدمي خدمات الإنترنت الذين يقدمون خدماتهم إلى مستخدمين نهائيين أفراد على شبكات نطاق عريض سكنية، إلا أنه قد تكون قابلة للتطبيق على مستخدمين آخرين وشبكات أخرى كذلك.

ألف.20 الممارسة الفضلى رقم: تخفيف 1

التعاون في أوساط الصناعة في أوقات الحوادث السيبرانية ذات البال:

ينبغي لمقدمي خدمات الإنترنت أن يكونوا على وعي دائم بمستويات التهديدات السيبرانية وأن يتعاونوا، كلما أمكن ذلك، مع مؤسسات أخرى في أوقات الحوادث السيبرانية ذات البال، مادين يد العون في سبيل جمع معلومات وتحليلها للوقوف على خصائص الهجمة وتوفير تقنيات للتخفيف من العواقب والتحرك من أجل ردع الهجمات السيبرانية أو الحماية منها على النحو الذي تكفله القوانين والسياسات السارية.[49]

ألف.21 الممارسة الفضلى رقم: تخفيف 2

عزل الأجهزة المصابة ببرمجيات ضارة مؤقتاً:

ينبغي لمقدمي خدمات الإنترنت أن يعزلوا بشكل مؤقت حساب المشترك أو جهازه في حالة اكتشاف جهاز منتهَك على شبكة المشترك وكان الجهاز الموصول شبكياً يبث حركة ضارة بنشاط.[50] وينبغي ألا يطبق مثل هذا العزل في الأحوال الطبيعية إلا إذا لم تسفر محاولات متعددة لإخطار العميل بالمشكلة (باستخدام طرائق متنوعة) عن الوصول إلى حل. وفي حالة وقوع هجمة حادة أو تمثيل المضيف المصاب خطراً قائماً ومعتبراً على سلامة تشغيل الشبكة، فربما يكون العزل الفوري مناسباً. وينبغي لمقدم خدمات الإنترنت في أي حالة يطبق فيها العزل وحسب حد الهجمة أو الخطر أن يجتهد في الاستجابة لاحتياجات العميل من أجل استعادة النفاذ إلى الشبكة. ولمقدم خدمات الإنترنت، متى ما أمكن ذلك، عزل الهجمة أو الحركة الضارة وترك ما دون ذلك دون تأثير.

ألف.22 الممارسة الفضلى رقم: تخفيف 3

إتاحة موقع إلكتروني للمساعدة في العلاج من البرمجيات الضارة:

ينبغي لمقدمي خدمات الإنترنت، بشكل مباشر أو غير مباشر، إتاحة موقع إلكتروني للمساعدة العملاء في العلاج من البرمجيات الضارة.[51]

---

[49] الممارسة الفضلى تخفيف 1: مراجع/تعليقات: في الولايات المتحدة، على سبيل المثال، وُضعت الخطة الوطنية للاستجابة للحوادث السيبرانية الحالية – المعروفة باسم المستوى الوطني للإنذار بالمخاطر السيبرانية (NCRAL) – كنظام رباعي المستويات لتسهيل المزامنة مع أنظمة مستويات إنذار أخرى، مثل IT-ISAC وSANS وتلك التابعة لمقدمي الخدمات الأمنية. وبهذا تصنف الحوادث السيبرانية ذات البال تحت مسمى حادة (المستوى 1) أو جسيمة (المستوى 2).

[50] الممارسة الفضلى تخفيف 2: مراجع/تعليقات:
لا يمثل التأخير المؤقت لصفحات إلكترونية بغرض تقديم إخطار عن طريق برنامج صفح الويب على النحو المقترح في أفضل ممارسات الإخطار (انظر لقسم 18.1.6) "عزلاً" بالمفهوم المستخدم في هذه الممارسة الفضلى.
ويمكن الوصول إلى معلومات تتعلق بتكنولوجيا العزل في:
www.trustedcomputinggroup.org/developers/trusted_network_connect

[51] الممارسة الفضلى تخفيف 3: مراجع/تعليقات: لا يوجد

ومعنى العلاج من البرمجيات الضارة على مضيف هو إزالة برمجيات روبوتية ضارة أو تعطيلها أو تحييد ضررها على أي نحو آخر. وقد يتضمن ذلك على سبيل المثال لا الحصر إتاحة موقع إلكتروني خاص يضم محتوى موجهاً إلى الاعتبارات الأمنية يخصص لهذا الغرض أو اقتراح موقع إلكتروني وجيه وموثوق تابع لطرف ثالث. وينبغي أن يكون ذلك موقعاً إلكترونياً موجهاً إلى الاعتبارات الأمنية يمكن إحالة مستخدم مصاب ببرمجيات روبوتية إليه لاتخاذ خطوات علاجية. كما ينبغي أن يوضح الموقع الإلكتروني الأمني هذا بجلاء ما هي البرمجيات الضارة والتهديدات التي قد تحدثها. وينبغي متى ما أمكن أن يوجد شرح واضح للخطوات التي ينبغي للمستخدم اتخاذها من أجل محاولة تطهير جهازه المضيف، كما ينبغي أن توجد معلومات توجه المستخدمين إلى أساليب لوقاية أجهزتهم من أي إصابات في المستقبل. وقد يضم الموقع الأمني كذلك عملية موجهة تصحب المستخدمين غير المتخصصين تقنياً خلال العملية العلاجية من خلال خطوات سهلة الفهم. ومن الممكن أيضاً أن يقدم الموقع توصيات بشأن خدمات العلاج المجانية وغير المجانية حتى يدرك المستخدم أن بين يديه خيارات متعددة، وأن منها ما يمكن اتباعه دون تكلفة.

أفضل ممارسات الخصوصية

من الجدير بالملاحظة أن أفضل الممارسات الواردة في هذه المجموعة موجهة أساساً إلى مقدمي خدمات الإنترنت الذين يقدمون خدماتهم إلى مستخدمين نهائيين أفراد على شبكات نطاق عريض سكنية، إلا أنه قد تكون قابلة للتطبيق على مستخدمين آخرين وشبكات أخرى كذلك.

ألف.23 الممارسة الفضلى رقم: اعتبارات الخصوصية 1

اعتبارات الخصوصية في اكتشاف الشبكات الروبوتية والإخطار بها والعلاج منها:

من شأن التدابير التقنية التي تستهدف (أ) اكتشاف أجهزة المستخدمين النهائيين المنتهَكة و(ب) إخطار المستخدمين النهائيين بالمشكلة الأمنية و(ج) المساعدة في معالجة المشكلة الأمنية أن تؤدي إلى جمع معلومات من العميل (مما قد يشمل "معلومات تعرّف هوية أصحابها شخصياً" ومعلومات حساسة أخرى، علاوةً على مضمون مخاطبات العميل)، مما يوجب على مقدمي خدمات الإنترنت ضمان معالجة كل هذه التدابير التقنية لخصوصية العميل والامتثال لجميع القوانين وسياسات خصوصية الشركات السارية والاتساق معها.[52]

ألف.24 الممارسة الفضلى رقم: اعتبارات الخصوصية 2

تدابير لحماية الخصوصية في الاستجابة لشبكات روبوتية

ينبغي لمقدمي خدمات الإنترنت في معرض تصميم تدابير تقنية لتحديد الهوية والإخطار وغير ذلك من أوجه الاستجابة لأجهزة المستخدمين النهائيين المنتهَكة ("تدابير تقنية") اتباع استراتيجية متعددة الأوجه لحماية خصوصية معلومات العملاء، مما يتضمن على سبيل المثال لا الحصر ما يلي:[53]

- ينبغي لمقدمي خدمات الإنترنت تصميم تدابير تقنية على نحو يقلل من جمع معلومات العملاء إلى الحد الأدنى؛
- في حالة تبين عدم الاحتياج إلى معلومات العميل لغرض الاستجابة لمشكلة أمنية، يجب المبادرة إلى استبعاد المعلومات؛
- ينبغي في جميع الأوقات حصر أي نفاذ إلى معلومات العملاء التي جمعت نتيجة لتدابير تقنية على الأشخاص التي تقتضي الضرورة المعقولة اشتراكهم في تنفيذ برنامج الاستجابة الأمنية للشبكة الروبوتية لدى مقدم خدمات الإنترنت، كما ينبغي منع نفاذ هؤلاء الأشخاص إلى تلك المعلومات إلا بالقدر اللازم لتنفيذ البرنامج الأمني؛
- في حالة اقتضاء الضرورة الاحتفاظ مؤقتاً بمعلومات العميل لتحديد هوية مصدر الإصابة بالبرمجيات الضارة أو للبرهنة للمستخدم على أن الرزم الضارة نابعة من توصيله عريض النطاق أو لأي أغراض أخرى لها صلة مباشرة ببرنامج الاستجابة الأمنية للشبكة الروبوتية، ينبغي الامتناع عن الاحتفاظ بهذه المعلومات لمدة أطول مما تقتضيه الضرورة المعقولة لتنفيذ البرنامج الأمني (باستثناء ما يطالب جهاز إنفاذ القانون القائم على التحقيق في حالة أمنية أو ملاحقة مرتكبيها بالاحتفاظ به من المعلومات باستخدام إجراءات ملائمة)؛
- ينبغي لمسؤول امتثال الخصوصية لدى مقدم خدمات الإنترنت، أو أي شخص آخر غير مشارك في تنفيذ البرنامج الأمني، التحقق من امتثال البرنامج الأمني لممارسات الخصوصية الملائمة.

[52] الممارسة الفضلى اعتبارات الخصوصية 1: مراجع/تعليقات: لا يوجد

[53] الممارسة الفضلى اعتبارات الخصوصية 2: مراجع/تعليقات: لا يوجد

8 أفضل الممارسات المتعلقة بالأمن السيبراني – دورة تدريبية على تكوين فريق للاستجابة للحوادث الحاسوبية وإدارته

1.8 مقدمة

يمثل إنشاء استراتيجية وطنية للأمن السيبراني الخطوة الأولى نحو تأسيس برنامج وطني. ومع ذلك، فليس من المحتم على أي بلد أن يكون لديه استراتيجية وافية شافية للأمن السيبراني قبل تكوين فريق وطني للاستجابة للحوادث الحاسوبية، بل قد حدث في حالات كثيرة أن ساعد الفريق الوطني الحكومة الوطنية في وضع استراتيجيتها وتهذيبها بعد سنوات من مباشرة أعماله. وتعنى الأفرقة الوطنية بدعم المرونة السيبرانية لبلدانها أو اقتصاداتها. وكثيراً ما يطلق على المؤسسات الوطنية المعنية بالاستجابة للحوادث أسماء مختلفة. وقد استخدم مسمى "الفريق الوطني" في هذه الوثيقة لشيوع استخدامه. وبينما تتنوع الأسماء المحددة لمؤسسات إدارة الحوادث السيبرانية، فقد يكون لاختيار الاسم وجه بالنسبة إلى علاقة المؤسسة بأعضاء مجتمع الاستجابة. وليس من النادر أن يكون في بلدٍ ما أكثر من فريق وطني، فقد يكون هناك تفضيل طبيعي لخدمة مجموعات معينة من المستفيدين من خلال مؤسسات مختلفة حسب أسلوب حكم البلاد وغير ذلك من العوامل الهيكلية.

وتؤدي الأفرقة الوطنية دوراً حاسماً في إنفاذ الأمن السيبراني، ومن ذلك على سبيل المثال التنبيه والإنذار على الصعيد الوطني وتكوين قدرات الأمن السيبراني وتمثيل مورد تقني وسياساتي للحكومة الوطنية بشأن قضايا الأمن السيبراني. وعلى ذلك فمن الأهمية البالغة أن تُعرف أفضل الممارسات المتعلقة بتكوين فريق استجابة للحوادث الحاسوبية وإدارته وتُفهم في أي بلد.[54]

[54] انظر **الملحق واو** للاطلاع على مزيدٍ من المعلومات بشأن الدورة التدريبية على تكوين أفرقة وطنية للاستجابة للحوادث الحاسوبية وإدارتها.

Annexes

Annex A: Best Practices for Cybersecurity – Planning and Establishing a National CIRT

Annex B: Best Practices for Cybersecurity – Managing a National CIRT with Critical Success Factors

Annex C: Best Practices for Cybersecurity – Guide for the Establishment of a National Cybersecurity Management System

Annex D: Best Practices for Cybersecurity – Internet Service Provider (ISP) Network Protection Best Practices

Annex E: Best practices for Cybersecurity –Training Course on Building and Managing National Computer Incident Response Teams (CIRTs)

Annex F: Best Practices for Cybersecurity – Survey on Measures Taken to Raise Awareness on Cybersecurity

Annex G: Best Practices for Cybersecurity – Public-Private Partnerships in Support of Cybersecurity Goals and Objectives

Annex H: Compendium on Cybersecurity Country Case Studies

Annex A: Best practices for Cybersecurity – Planning and Establishing a National CIRT

Abstract

As nations recognize that their critical infrastructures have integrated sophisticated information and communications technologies (ICT) to provide greater efficiency and reliability, they quickly acknowledge the need to effectively manage risk arising from the use of these technologies. Establishing a national computer security incident management capability can be an important step in managing that risk. In this document, this capability is referred to as a National Computer Security Incident Response Team (National CIRT), although the specific organizational form may vary among nations. The challenge that nations face when working to strengthen incident management is the lack of information that provides guidance for establishing a national capability, understanding how that capability may support national cybersecurity and national incident management. This report provides insight that interested organizations and governments can use to begin to develop a national incident management capability. The document explains the need for national incident management and provides strategic goals, enabling goals, and additional resources pertaining to the establishment of National CIRTs and organizations like them.

Executive Summary

This draft report is relevant to Item 2 b) (iii) ("with respect to creating a national cyber incident management capability, to elaborate on the development of watch, warning and response and recovery mechanisms, and the establishment of national computer security incident response teams") (see Document WTDC-10/162 Rev.1)

Managing cybersecurity through a national strategy is a necessity common to all national governments in the 21st century. Critical infrastructure in most nations, from transportation and power generation to food supply and hospitals, depends on Information and Communications Technology (ICT). The reliance on complex and constantly evolving technology is across all sectors of critical infrastructure, making it very difficult for national governments to understand and mitigate risks related to this technology. In fact, these risks are a shared responsibility that extends outward to include international perspectives. The shared responsibility within the nation includes private industry (which owns and operates much critical infrastructures), academia, and citizens.

Establishing and maintaining a computer security incident management capability can be a very valuable component to help manage this interdependence. This capability is referred to in this document as a National Computer Security Incident Response Team (National CIRT), but it can be implemented in a variety of different organizational forms. Beyond responding to discrete computer security incidents, a robust incident management capability enhances the ability of the national government to understand and respond to cyber threats. Operating a National CIRT – or an organization like it - is a core component of a nation's overall strategy to secure and maintain technologies vital to national security and economic vitality.

This handbook is designed to be an introductory curriculum for capacity development within nations. The intended audience includes leaders and managers in the nation who are seeking to learn more about the value proposition of National CIRTs and an incident management capability generally. It is not intended to be a guide on the daily operation of a National CIRT, but as informative materials on how National CIRTs support a national cybersecurity strategy and the first steps towards building this capacity.

This handbook provides principles and strategic goals to help nations develop a robust management capacity that is appropriate for the nation. It attempts to lessen the challenge many nations have in developing an incident management capability without much published guidance. Many nations attempting to develop National CIRTs have started by attempting to copy successful CIRT organizations that already exist. This approach can be problematic because not every nation has the same needs and resources. The operating principles and strategic goals discussed in this document enhance the ability of governments to manage cybersecurity risks and focus their efforts.

Strategic goals are essential design requirements and imperatives. They serve as fundamental elements of an incident management capability and are meant to provide clarity and direction. This document proposes four strategic goals as they relate to a national computer security incident management capability. They are:

1. Plan and establish a centralized computer security incident management capability (National CIRT)
2. Establish shared situational awareness
3. Manage cyber incidents
4. Support the national cybersecurity strategy

There is a common need to resist, reduce, and fight cyber threats and respond to attacks. National CIRTs provide a domestically-focused, internationally-amplified operational response to those cyber incidents that destabilize the interdependent nature of global telecommunications, data services, supply chains, and critical infrastructure. We hope sponsors of a National CIRT or similar capability will see these benefits and encourage the government and organizational leaders in their nation to participate in a global culture of security.

1 Introduction

Nations are increasingly dependent on complex systems and information technology. In many cases, Information and Communication Technologies (ICT) that are vital to national and economic security are subject to disruption from a number of causes, either originating from within the nation or outside its borders. The leaders of government and private industry organizations are increasingly confronted with uncertainty about cyber risk and vulnerabilities. This uncertainty stems from the complexity and interconnectivity of evolving technology used to support critical systems. Ensuring security and economic vitality increasingly means that nations must manage cybersecurity in accordance with their own economic, social, and political considerations.

Implicit in a strategy for cybersecurity is establishing a national computer security incident management capability. Often this capability may take the form of one or more National Computer Security Incident Response Teams (National CIRTs). National CIRTs are typically hosted by one or more sponsoring organizations, which build and manage cyber incident management assets. Organizations such as the National CIRT provide value in several ways. A National CIRT coordinates incident management and facilitates an understanding of cybersecurity issues for the national community. A National CIRT provides the specific technical competence to respond to cyber incidents that are of national interest. In this primary role the National CIRT fills a planned response function, providing solutions to urgent cyber problems. The ability of National CIRTs and similar organizations to identify cybersecurity problems and threats, and disseminate this information, also helps industry and government secure current and future systems.

Beyond the capacity to react to specific incidents and disseminate information, National CIRTs can enhance the ability of national government departments to fulfill their unique roles. Most government functional areas are touched by information technology in some way. Law enforcement and the judiciary are increasingly concerned by the global movement of criminals to the virtual world to commit crimes ranging from child exploitation to financial fraud. The world's defense services rely on advanced information technology-based systems for their capabilities. And other critical infrastructure, such as food, water, and electricity supply chains depend on reliable technology. A National CIRT can enhance the government's ability to meet core responsibilities while respecting their citizens' privacy and human rights, and upholding national values of openness and pluralism.

National CIRTs can also act as a focal point for a national discussion on cybersecurity. For a variety of reasons, cybersecurity poses new and unique social, legal, and organizational challenges. The global interconnectedness of computer networks, the anonymity of online actors, and the rapid exploitation of vulnerabilities mean that the actions of individuals – often located outside national borders – can have serious and magnified effects on vital national systems. Meanwhile governments are limited by the jurisdictional reach of their laws and the physical limits of their borders. The National CIRT can catalyze a thoughtful discussion on these issues, engaging authorities in the fields of education, law, and governance – among others – to help create solutions that are in keeping with national character and traditions.

Finally, building a national computer security incident management capability can help foster international cooperation on cybersecurity. National CIRTs provide a domestically-focused, operational response to those cyber incidents that destabilize modern telecommunications, data services, supply chains, critical infrastructure, banking, and financial services. Collaboration with peer organizations both regionally and globally can enhance this capability and help leaders better understand the current state of the global cyber threat. There is a common global interest in securing information and information systems, and in mitigating risk. To the extent that they cooperate on cybersecurity issues, national governments help make the world more secure and prosperous for their citizens.

The challenge for nations wanting to develop an incident management capability is that there is little published guidance available in this area. Typically nations model nascent capabilities on the National CIRTs or other CIRTs which have already been operating in other nations. The problem with this approach is that the organizations that already exist are in some measure products of the historical, political, or other circumstances in those countries. One nation's solution to cybersecurity management may not be appropriate for another nation. To date, the published guidance on how to systematically build a

cybersecurity and incident management capability has been in its infancy. This handbook begins to remedy this.

1.1 Intended Audience

The primary audience for this document consists of those sponsoring the development of a national computer security incident management capability – usually referred to as a National CIRT. This document will discuss the considerations and goals inherent in standing up a National CIRT. While this document focuses on a single National CIRT, there may be other organizational forms that are suitable for an incident management capability. Alternatively, some nations may find it advantageous to house this capability across several organizations. It is hoped that the principles and recommendations in this document are useful even to nations that do not choose the specific National CIRT organizational form.

1.2 How to Read This Handbook

This document is structured to serve as a strategic education on the building of a computer security incident management capability. Because of the breadth of this topic, the focus here is on the creation of a National CIRT. The material is intended to outline the stakeholders, constraints, and goals for National CIRTs, to raise awareness of the need for this type of capability, and to frame this capability in the national strategy. While the focus is on National CIRTs specifically, the guidelines herein are meant to help national leaders generally, regardless of the specific organizational form chosen to handle incident management.

The next section, *Setting the Context: National Cybersecurity*, includes information about National CIRTs as part of a larger national approach to cybersecurity. The section specifically discusses the importance of a national strategy, the context of a national cybersecurity policy framework, and an overview of key stakeholders in national cybersecurity as they relate to National CIRTs. The unique role of National CIRTs is also discussed.

The third section, *Strategic Goals and Enabling Goals for Incident Management Capability*, introduces a hierarchy of goals for ensuring alignment between the National CIRT and national cybersecurity strategy. *Strategic goals* outline the long term imperatives for a national computer security incident management capability, while the *Enabling Goals* highlight the necessary steps to building an operational National CIRT capacity.

2 Setting the Context: National Cybersecurity

Ensuring national security and economic vitality requires recognizing that not all risk is owned and mitigated by a nation's government. The national and local government and its various branches, critical infrastructure owners and operators, academia, and citizens all share this responsibility. New and emerging risks must be effectively identified, analyzed, and mitigated to ensure the safety and security of daily life for citizens. These risk management activities may involve ensuring continuity of government, safeguarding the generation of electricity, emergency response services, or ensuring a reliable supply chain, among others. Each of these relies heavily on information technology in a modern economy. National leaders increasingly realize that the security of information and information technology is a national security interest and should be codified in laws and national strategy. Chief among the strategies for enhancing this security are specific operational capabilities, such as the incident management activities typically performed by a National CIRT.

2.1 The Importance of a National Strategy for Cybersecurity

Building a national strategy for cybersecurity is ideally the first step in establishing a national cybersecurity program. A national policy framework should explain the importance of cybersecurity, help stakeholders understand their role, and set the goals and priorities. The national strategy should integrate

security fundamentals (such as raising awareness), and emphasize cooperative relationships among national stakeholders.The national strategy may also serve as a backdrop for the creation of laws that relate to cybersecurity; for instance in the areas of computer crime, the protection of intellectual property, and privacy. Finally the national strategy should reconcile the need for security with the need to honor citizens' rights and the nation's cultural values and norms.

The strategy should also articulate the need for specific operational capabilities, and the National CIRT should be deliberately aligned with those national cybersecurity strategic goals to ensure that its work contributes to achieving them. While establishing a national strategy is ideally the first step, in many cases this may not always be feasible. This might be the case because of the difficulty in getting a large number of stakeholders to agree on a strategy. Alternatively, national leaders may judge that establishing an incident management capability is a more pressing need than creating a fully integrated strategy. In such cases creating an effective strategy may occur concomitantly with building incident management capability. In any case, the sponsor or proponent of the National CIRT should work with the government to ensure that national needs and priorities are considered throughout the process of building and managing a National CIRT.

2.2 Key Stakeholders of National Cybersecurity

Cybersecurity involves many stakeholders. This section broadly describes the roles and responsibilities of typical national stakeholders, and how they might contribute to a national program for managing cybersecurity. These roles are not unique to National CIRT operations, but many of the stakeholders discussed here may directly interact with the National CIRT. Moreover, the National CIRT can enhance its role and help advance a culture of security by proactively interacting with these stakeholders.

The government has a multitude of roles and responsibilities to strengthen national cybersecurity. The primary role is to define the national strategy and provide the policy frameworkwhich describes the architecture by which the national efforts are built and operated. Following that, the government has a responsibility to participate with all stakeholders in efforts to identify, analyze, and mitigate risk. The government also has a key role to play in the arena of international relations and cybersecurity, particularly in the areas of treaties relating to cybersecurity and the harmonization of national laws relating to cybercrime.

2.2.1 Executive Branch of the Government

In most nations the executive branch of the government is typically responsible for enforcing laws and ensuring security. It may also include the military. The executive branch is often the sponsor of the national cybersecurity program. The executive area of government must ensure that the cybersecurity program remains viable and has appropriate resources (e.g., is authorized, staffed, funded, etc).

2.2.2 Legislative Branch of the Government

The legislative arm of government works to provide effective laws that promote a culture of cybersecurity. Whether through appropriations of resources or funding, legislation that mandates execution of the national strategy, privacy or tort laws, or laws that establish criminal behaviors, the legislature must ensure that the national cybersecurity program has the foundation it needs to be successful.

2.2.3 The Judiciary

The nation's judiciary and legal institutions have an important role to play in a national cybersecurity strategy. This role relates specifically to providing clarity and consistency in areas of law that may affect cybersecurity. Privacy law is an example. By working with their global counterparts, the legal community can also help to limit the ability of criminals and other malicious actors to take advantage of differences in legal jurisdictions.

2.2.4 Law Enforcement

Law enforcement ensures that legislation related to cybersecurity is enforced. Additionally, law enforcement can serve as an important source of intelligence about malicious activity, exploited vulnerabilities, and methods of attack. Sharing this information allows critical infrastructure owners and operators to learn from the experiences of others to improve cybersecurity practices and management. Finally, law enforcement can enhance cybersecurity by cooperating with their counterparts in other nations on the pursuit and apprehension of criminal actors who affect systems regardless of geographic borders.

2.2.5 Intelligence Community

The intelligence community plays an important watch and warning role for technical infrastructure. Intelligence organizations usually monitor various sources for information about threats and vulnerabilities to a nation's infrastructure. This information should be distilled and provided to the National CIRT and, where appropriate, to infrastructure owners. This helps to ensure that attacks are efficiently anticipated, recognized, and resolved.

2.2.6 Critical Infrastructure Owners and Operators

A general definition for critical infrastructure is:

> *Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

Critical infrastructure owners and operators are a very important stakeholder in the nation's overall cybersecurity strategy. Infrastructure operators typically have an understanding of how security threats and vulnerabilities affect their sector. Infrastructure operators also have the daily task of implementing the security recommendations or mandates created by the national government and other authorities. They must reconcile the need for security with the sometimes contradictory goals of efficiency and profitability.

Because of their unique position, infrastructure owners and operators frequently have very valuable information, ranging from the actual software problems and cyber attacks they may experience, to the efficacy of countermeasures or risk mitigation strategies. They are also a primary consumer of information about security vulnerabilities. Finally, because of their practical experience implementing security standards and complying with the law, owners and operators may have valuable input into the development of effective, realistic rulemaking and legislation.

2.2.7 Vendors

Vendors of information technologies and services contribute to national cybersecurity through development practices and ongoing vulnerability reduction efforts. Vendors can often be the source of vulnerability information; they ensure that users have up-to-date information and technical solutions to mitigate known vulnerabilities. Ideally, vendors will participate with National CIRTs and help extend the analytical and problem solving capabilities the National CIRT needs to conduct incident response. Information sharing among vendors, their major customers, and the National CIRT can create a partner relationship that continuously improves security for technologies and services.

2.2.8 Academia

Educational institutions play a key role in developing the human capital and technical skills needed to solve complex problems, such as aspects of cybersecurity. Academicians conduct research that enhances the technical, legal, and policy aspects of cybersecurity. Finally, in many countries educational institutions have championed and hosted National CIRTs.

2.2.9 Foreign Governments

Nation-states must take an interest in helping to prevent any cybersecurity attacks against their neighboring nations and allies. For a number of reasons, including economic, political, and infrastructure concerns, partnerships should be established to discuss global risk and interdependence. Allies and neighboring nations can also provide a valuable source of intelligence and promote regional cyber prevention and preparedness.

2.2.10 Citizens

Citizens rely on all stakeholders to create national security and critical infrastructure stability. The citizens of a nation have a stake in the reliable performance of a nation's strategy for cybersecurity, and are an inherent part of that strategy.

2.3 The Special Role of the National CIRT

National CIRTs and organizations like them ideally act as critical components of the national cybersecurity strategy. National CIRTs first provide the capability to react to computer security incidents that are deemed to be of national importance[1]. Because they collect and analyze information about computer security incidents on a daily basis, National CIRTs are an excellent source of lessons learned and other information that can help stakeholders mitigate risk. National CIRTs can also help catalyze a meaningful national discussion about cybersecurity and awareness by interacting with private and governmental stakeholders. The following is a discussion of the role of a National CIRT, though not every organization will perform these functions or do all of these tasks. However, these roles represent how a National CIRT typically supports national cybersecurity.

2.3.1 Analyzing Computer Security Incidents to Identify Intrusion Sets

An intrusion set is defined as groups of computer security incidents that share similar actors or methods. Determining that similar actors are involved may involve a variety of analytical techniques, and is closely tied to the question of method. Determining that different attacks use the same method may involve questions of attack vector (email, spoofed web pages, etc.), similarities across samples of malware, or the routing of stolen information (through specific proxy IP addresses, for instance).

Identifying intrusion sets is essentially a refined version of the correlation analysis that many computer security incident handlers are familiar with. Generally, incident activity is grouped into different categories, such as

– criminal activity

– activity conducted by other nations

– undetermined.

This information and analysis can then be submitted to other national authorities for action depending on the nation's security concerns and objectives.

2.3.2 Use of Sensitive Law Enforcement or Intelligence Information

Because of their national mission, their often close relationship with the national government, and their daily work safeguarding sensitive information, National CIRTs may be involved in using sensitive information from national intelligence or law enforcement organizations in their analysis. The use of this type of information can amplify the National CIRT's work, but requires strong trust relationships between the National CIRT and the government, as well as robust information security measures.

---

[1] The question of which incidents rise to the level of national importance is covered more fully in section 3.3.1.

2.3.3 Resource to the National Government on Cybersecurity Issues

A National CIRT can be a valuable resource to the national government on technical, policy, and legal issues relating to cybersecurity. It may be able to advise the government on the suitability or security of systems the government is planning to install or implement. In addition, the National CIRT can help government organizations with technical alerts and bulletins, best practices, and other advisories.

2.3.4 Assessing National Cyber Readiness and Crisis Management

The National CIRT can help national leaders and key stakeholders test and measure the nation's level of resilience to cyber attacks and crises. This assistance may take the form of providing the technical support and analytical methods to plan and stage exercises, or advising on the state of current cyber threats or the realism of exercises.

2.3.5 National Alert and Warning

Most of the existing National CIRTs fulfill a national alert and warning function. This function involves alerting key national communities about problems ranging from specific software and system vulnerabilities, to evolving criminal methods, to malware threats.

2.3.6 Organizational CIRT Capacity Building

National CIRTs have a key role to play in the building of cybersecurity capacity. Specifically, National CIRTs can help organizational CIRTs in the nation in a variety of ways including advice, training, best practices, or in some cases staffing.

2.3.7 Trusted Point of Contact and National Coordinator

National CIRTs frequently act as a trusted point of contact for the nation on cybersecurity issues. For example, national teams often handle requests from other nations or foreign organizations concerning malicious activity emanating from computers or systems within the nation. In a similar fashion, National CIRTs frequently act as coordinators for domestic organizations attempting to resolve cybersecurity incidents. In this role, the National CIRT does not typically analyze or resolve incidents itself, but rather it helps to direct organizations experiencing security incidents to information, services, or other entities that can help them.

2.3.8 Building a Cybersecurity Culture

The National CIRT can help to build a cybersecurity culture within the nation. Building a cybersecurity culture consists of many activities including awareness and education of private citizens on online risks, educating national stakeholders on the impact of virtual activities to their organizations, and the implications of their activities for cyber and information security.

3 Strategic Goals and Enabling Goals for Incident Management Capability

This section provides the strategic goals and enabling goals that should be considered when establishing a National CIRT. The information provides an overview of the considerations and goals that are needed to ensure support for the national cybersecurity strategy and to align the National CIRT with the national strategy. The enabling goals are specific steps to meeting strategic goals. Four strategic goals for a National CIRT are:

– Plan and establish a centralized computer security incident management capability (National CIRT)

– Establish shared situational awareness

– Manage cyber incidents

– Support the national cybersecurity strategy.

Each of these strategic goals explains the fundamental elements of the National CIRT and must be weighed carefully by the National CIRT sponsor. Strategic goals are essential, long term requirements that help build the capacity to react to cyber incidents and enhance information and cybersecurity on a national level. Following each strategic goal are Enabling Goals. Enabling Goals help the sponsor build the capacity. They explain the more detailed considerations and activities needed to implement the strategic goals. The guidance available for each goal varies based on the maturity of the topic. Some subjects, like incident handling, have a robust history. Others, such as implementing national cybersecurity strategy through National CIRTs, are still emerging disciplines.

This document is not meant to provide specific 'how-to' instructions. Instead, it highlights the unique requirements for building capacity in cyber incident management. Finally, each strategic goal section concludes with a listing of additional references and training resources. These sources are not exhaustive, but provide the reader with a 'next step' to both training and informational resources.

3.1. Strategic Goal: Plan and Establish a Centralized Computer Security Incident Management Capability (National CIRT)

Before the first cybersecurity incident can be managed, the capability must itself be established in an organizational form such as a National CIRT. Having a sole source or point of contact for computer security incidents and cybersecurity issues provides a number of benefits. A single organization provides stakeholders with a known source of information. A National CIRT can also provide the government with a conduit for coherent, consistent messaging on cybersecurity issues. With a single National CIRT, government departments have a source for technical information to support their individual functional areas. Finally, the National CIRT can encourage the discussion about cybersecurity and facilitate international cooperation on this issue. In some nations, unique considerations may dictate that there are multiple National CIRTs, or even an incident management capability that is spread across several organizations. This can be entirely appropriate. This document provides guidance regardless of the exact organizational form.

A National CIRT capability should be established and operated according to certain core principles. These principles help leaders make decisions in the face of limited resources and frequently complex problems. The core principles for the national management capability are:

– Technical excellence. The National CIRT's capability should be the best that it is possible to develop given the resources available. This is important because the National CIRT strives to be a trusted leader in the nation on computer security issues. While striving for excellence may seem an obvious point, it has certain implications for building a capacity subject to resource constraints. It implies, for instance, a preference for building one or two outstanding capabilities versus attempting to establish a range of capabilities without proper staffing or funding. The emphasis should be on technical competency.

– Trust. Almost by definition, a National CIRT will handle information that is sensitive or potentially embarrassing to stakeholders. Trust must be earned and maintained. Properly handling and protecting confidential information is an important component to building and managing this trust.

– Resource Efficiency. Resource efficiency means using the resources that are available effectively. This consideration will be covered in more detail below, but it implies an ongoing evaluation of which threats and incidents are truly of interest to the National CIRT's overall strategy as well as to the community it serves.

– Cooperation. The National CIRT should cooperate as fully as possible with both national stakeholders and other National CIRTs to exchange information and coordinate the solving of problems that are frequently very complex.

Chief to the National CIRT's success is adequate sponsorship and resourcing. The Enabling Goals listed here are intended to help the sponsor of a national incident management capability build this capability in

the most robust way possible. Consider the following enabling goals in planning and creating the national incident management capability.

3.1.1 Enabling Goal: Identify Sponsors and Hosts

The sponsor of the National CIRT should identify other sponsors and likely hosts for the National CIRT. Other sponsors may be able to bring additional funding and support to the National CIRT project. Of course, a physical location – or host – for the National CIRT must also be identified. In some countries the host has been an academic institution. Universities traditionally have been a venue for National CIRTs because aspects of their core mission – to serve the community and conduct research and analysis of difficult problems – aligns well with the mission of a National CIRT. However if it is hosted by a university, the National CIRT may not have adequate resources or the authority to enforce or take action; rather it achieves its success by influencing others through its good work.

There may be a variety of institutions and government departments interested in supporting or hosting a National CIRT. While any assistance is welcome, there may be pitfalls to receiving support from certain stakeholders. The National CIRT should be dedicated to serving its entire community in an unbiased fashion, without favor to a particular stakeholder. Receiving sponsorship from an entity that is closely tied to a particular stakeholder or industry may limit the National CIRT's perceived ability to service the entire community. This possibility should be examined, for example, if a specific for-profit enterprise operated a National CIRT. In other cases, the involvement of certain sponsoring organizations may impede the willingness of key constituents to share information. Certain constituents, for instance, might be reluctant to share information if a law enforcement organization was the National CIRT's primary sponsor. In addition, the National CIRT host should be sufficiently financed to ensure fiscal stability for continuity of operation.

3.1.2 Enabling Goal: Determine Constraints

The sponsor should determine what constraints may act to limit building and operating a National CIRT. Typical constraints are budget, the availability of skilled staff, and the physical infrastructure available to support National CIRT operations. The question of constraints bears heavily on the ability of a national government to build incident management capacity, and is usually a key driver behind decisions about which specific services to offer to the community. For instance, it may not be practical or desirable to build a malware analysis or deep packet inspection capacity in the National CIRT. Limited constraints may dictate that a more realistic approach is to build relationships with other domestic or overseas organizations that do have this capability.

Constraints relate strongly to three of the core operating principles identified above; technical excellence, trust, and resource efficiency. Technical excellence requires a clear understanding of the staffing and budget available to support certain CIRT activities. It may dictate an emphasis on a few core services performed well, rather than attempting to provide a broad array of services. Limited constraints can also make the ability to coordinate incident management very important, rather than attempting to complete every incident management task in-house. Earning the trust of key constituents requires operational and staffing stability, as well as the ability to safeguard sensitive information – all directly impacted by resource limitations. Finally, resource efficiency requires understanding what resources are available.

3.1.3 Enabling Goal: Determine the National CIRT Structure

Based on its function in national cybersecurity, a National CIRT can operate under a range of modes including: an independent agency with limited operating partnerships, a joint operation with national telecommunications providers, or an integral part of the national military defense strategy. A number of factors must be considered to ensure detection and incident coordination and response are appropriately structured. The following list of structural considerations is meant to be exploratory and not comprehensive:

– What level of government directs the National CIRT?

– Who funds the National CIRT and who approves the budget?

– Is there an independent body that oversees the National CIRT?

– What set of roles and responsibilities have been identified for National CIRT operating partners?

There are several considerations that may be helpful in resolving the question of organizational form, in addition to the core principles:

– What structure would best allow the National CIRT to alleviate potential stakeholder concerns with regard to sharing information? Are there any possible organizational structures that may limit the National CIRT's perceived ability to serve its community in an unbiased fashion?

– Are the nation's systems and infrastructure already structured in ways that would make multiple National CIRTs beneficial in terms of information sharing or reporting relationships?

– If multiple National CIRTs are instituted, how should they share information? Is there a risk that multiple National CIRTs may not be able to effectively share information across infrastructure sectors? What are the transaction costs associated with having multiple organizations? How to they compare to the benefits of scale of a single National CIRT?[2]

– Do the various possible organizational forms have any implications for staffing and managing human capital?

3.1.4 Enabling Goal: Determine the Authority of the National CIRT

The National CIRT proponent or sponsor should determine if the National CIRT will have the authority to proscribe or mandate certain actions or security measures. The authority of a National CIRT could involve mandating the reporting of security incidents, or the adoption of certain security measures, or both. In addition, the authority of a National CIRT may differ based on whether it is addressing private citizens and industry, or government departments. It may be entirely appropriate for the National CIRT or the sponsoring organization to maintain authority over various government departments, but to have no authority over private citizens.

These decisions will be made consistently with the nation's law and culture. However, it is frequently the case that National CIRTs are more effective when they act in an advisory role only. Major national stakeholders are often more willing and – depending on the legal environment – more able to fully share information and discuss security vulnerabilities in a collaborative venue where the National CIRT is not a regulatory or proscriptive body.

3.1.5 Enabling Goal: Determine the Services of the National CIRT

The minimal essential function of a National CIRT is the ability to respond to cybersecurity threats and incidents that are important to national stakeholders. The various National CIRTs currently in existence execute a variety of functions including:

---

[2] A Note about Regional Collaboration: The sponsor of a National CIRT may consider sharing resources and costs with neighboring nations to form a regional computer security incident management capability, essentially a "Regional CIRT." This may be an effective way to address the inherent problem of fulfilling many requirements with limited resources. A full examination of such an arrangement is beyond the scope of this report; however there are compromises inherent in this solution.

Because one of the functions of a National CIRT is to reconcile the need to respond to global challenges with the nation's embedded law, culture, and national structure, the ability of a regionally-based CIRT to provide value to multiple nations may become diluted. Secondly, because cybersecurity is part of a nation's overall security strategy, regional CIRTs may often possess information that has important national security implications. A regional CIRT may be limited in its ability to solicit this information from certain national stakeholders because of concerns about sharing this information in a multi-national venue. In any event, it would require a high degree of comfort and familiarity between nations - or an effective multi-national governance structure - for a regional CIRT to be successful.

Incident Handling Services	Vulnerability Assessments
Incident Analysis	Research Services
Forensic Services	Training/Education/Awareness
Network Monitoring Services	Coordinating Response
Malicious Code Analysis	

At the individual nation level these functions are limited by the constraints identified in Enabling Goal 3.1.2 (e.g., funding, staffing, physical resources). The National CIRT sponsor organization must determine which of these activities are realistic given the constraints involved. Typically the most significant constraint is human capital (i.e., staffing). Since the National CIRT serves as the national leader in cybersecurity incident management and analysis, the guiding principle for choosing particular functions should be excellence. It may be that the best way for a particular National CIRT to fulfill its role is through close coordination with other National CIRTs that have a greater technical capability, or who may already have trusted communication channels.

3.1.6 Enabling Goal: Identify Additional Stakeholders

The sponsor of the national incident management capability should evaluate which other institutions may have input or interest in the establishment of a National CIRT. A detailed list of the typical stakeholders in national cybersecurity policy appears in section two of this document. Additionally, some stakeholders may be interested in taking a more active role in the formation and operation of a National CIRT. Typically these include;

– law enforcement

– technology vendors

– government users (government agencies and ministries, etc)

– research communities

– governance bodies.

The National CIRT should understand how the identified stakeholders complement and integrate into National CIRT operations, and develop a plan to ensure that bi-directional communication is designed into its operations.

3.1.7 Additional Resources: For Planning and Establishing a National CIRT

The following is a list of publicly available resources for sponsors and champions considering the establishment of a National CIRT.

Reference materials

– CERT's Resource for National CIRTs: http://www.cert.org/CIRTs/national/

– CERT listing of National CIRTs: http://www.cert.org/CIRTs/national/contact.html

– Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?: http://www.cert.org/CIRTs/CIRT-staffing.html

– Resources for Computer Security Incident Response Teams (CIRTs): http://www.cert.org/CIRTs/resources.html

– Forum of International Response and Security Teams: http://www.first.org

– Forums of Incident Response and Security Teams (FIRST) Best Practice Guide: http://www.first.org/resources/guides/#bp21

– ENISA: Support for CERTs / CIRTs: http://www.enisa.europa.eu/act/cert/support

– ENISA: Baseline capabilities for National CIRTs: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

Training resources

– CERT Overview of Creating and Managing CIRTs: http://www.sei.cmu.edu/training/p68.cfm

– CERT Creating a Computer Security Incident Response Team (CIRT): http://www.sei.cmu.edu/training/p25.cfm

3.2 Strategic Goal: Establish Shared Situational Awareness

The essential function of a National CIRT is the ability to manage cybersecurity threats and incidents that are of importance to national stakeholders. Excellence in incident management helps the National CIRT to build relationships with stakeholders and achieve other strategic objectives, such as supporting the national cybersecurity strategy. The first step in managing incidents is establishing an understanding or awareness of who the National CIRT's major constituents are, what types of systems they employ (Information and Communications Technology), and what types of incidents they are experiencing. This general understanding of the environment is typically referred to as shared situational awareness.

The most able staff and the best technical infrastructure are wasted if the community is unwilling to inform the National CIRT about incidents. Therefore, the first enabling goal focuses on this issue.

3.2.1 Enabling Goal: Establish and Maintain Trust Relationships

National CIRTs collect sensitive information about national constituents' problems, concerns, and vulnerabilities. They frequently use this information to derive lessons learned and publish informational reports, a process which carries the risk of revealing too much information if performed carelessly. National CIRTs also disseminate general information to stakeholders about threats, vulnerabilities, and best practices. Building trusted relationships with stakeholders is essential to facilitating this two-way information exchange. Without the confidence of knowing that sensitive information will be adequately protected and compartmentalized, stakeholders will be unwilling to share their sensitive information, crucial to the National CIRT. Stated plainly, it is difficult to manage security incidents when the victims are unwilling to tell the National CIRT about them.

By establishing relationships and partnerships with owners and operators of national critical infrastructure and other key constituents, the National CIRT gains access to information crucial to its operations. These relationships and partnerships are directly with the National CIRT and among constituents. The National CIRT may act as a trusted communications channel between key constituents.

Ensuring the confidentiality of stakeholder information is an information security problem. It requires information security risk assessments at the National CIRT level and implementation of the resulting recommendations. Policies to strengthen information security range from properly vetting employees to employee Non-Disclosure Agreements (NDAs) and similar legal devices, which make maintaining confidentiality a condition of employment. Classification levels for information are another basic way to ensure that access to information is limited to persons who need it to perform their job. Regardless of the specific security measures and policies, the National CIRT should proactively address stakeholder concerns in this area and be as transparent as possible about the security steps taken. A fuller discussion of policies to facilitate information sharing and security in a National CIRT environment will appear later in this series.

3.2.2 Enabling Goal: Coordinate Information Sharing between Domestic Constituents

One of the most important factors in establishing a national capability is to facilitate reliable and effective information sharing. A key role for a National CIRT is to obtain incident information from the community

and to disseminate timely and relevant response information back to the community. This type of information generally includes the following:

– incoming information about security incidents, collected through a variety of means
– security bulletins, awareness information on cyber threats and vulnerabilities
– general, specific, and urgent cyber warnings and alerts (technical and non-technical)
– best practices to prevent cybersecurity problems, events, and incidents
– general National CIRT information (e.g., organizational chart, sponsorship, services provided by the National CIRT, contact number/email address, etc.)
– resources and reference materials (e.g., security tools, partner organizations)

The information that the National CIRT collects can be used to reduce risk by providing support to organizations that have been attacked. This support may take the form of direct technical support or it may involve working with third parties to find remedies and workarounds, or raising awareness of the general and private industry. A key part of information sharing is that sensitive information from constituents may be shared with other constituents only after being anonymized during the analysis process and in accordance with the National CIRT's policies.

Anonymization requires sensitivity to specific circumstances, either involving computer security incidents themselves or the major constituents. For instance, a publicized incident report may redact the names of the victims or the constituent company involved. However, if it involves a notable incident discussed in the press, it may fail at actually protecting confidences. A basic principle of protecting information is receiving the approval of the parties involved before releasing information or publicizing reports.

A key component of information sharing is maintaining tools, techniques, and methods that enable the National CIRT to communicate with its community. Examples of these can include the following:

– a website for communicating and disseminating information – both general (publicly accessible) and sensitive (secure portal requiring authentication) between the CIRT and its community
– mailing lists, newsletters, trends and analysis reports
– implementation of secure information networks for CIRT operations

3.2.3 Enabling Goal: Integrate Risk Information from the Community

National CIRTs benefit from open, shared information from private industry, academia, and government. When organizations conduct thorough risk assessments and share the results with the National CIRT, situational awareness increases. Risk information from the community can help the National CIRT understand the effect that security vulnerabilities and system problems might have on important assets and infrastructure, helping the National CIRT to focus and refine its incident management process.

In its operational role of responding to incidents, a National CIRT is a key contributor to situational awareness. By analyzing trends in the incidents being managed, the National CIRT learns about the status of cybersecurity within the community it serves. The National CIRT uses this knowledge and its own perspective on problems to produce a credible, realistic picture of national situational awareness. This helps the National CIRT to identify proactive defense strategies, as well as needed improvements in practices and behaviors within the community.

3.2.4 Enabling Goal: Collect Information about Computer Security Incidents

A National CIRT must be able to collect information about computer security incidents and events, receiving reports about suspected or confirmed incidents that require coordination or response. National CIRTs collect information about incidents through two primary means; the trusted relationships they build and the technical infrastructure required to process incoming reports. While incident reporting is frequently voluntary and facilitated by trust, in some cases it may be mandated.

A National CIRT receives reports of computer security incidents through a variety of technical means, such as a 24/7 hotline or web portal. Web portals may be accessible from any computer for the general public or may be a secure web portal for the exchange of sensitive information. Capturing reports about computer security incidents requires the community to detect, identify, and track anomalous activity, employing both technical and non-technical methods. Anomalous activity is defined as activity that deviates from some establish norm of system operation. In many cases, collecting computer security incident information may first require educating communities about detecting this activity.

3.3 Strategic Goal: Manage Incidents

A National CIRT, acting as a trusted, national cybersecurity focal point, is uniquely situated to manage incidents of national concern. To accomplish this, many National CIRTs establish certain active capabilities, such as incident response and containment, and service reconstitution. It is important to remember that in many cases the National CIRT will not handle all of the incident handling and analysis itself. A National CIRT may act to facilitate and coordinate analysis and response, either because of limited resources or because knowledge about the specific problem may reside elsewhere, for instance at another National CIRT or at a technology vendor.

3.3.1 Enabling Goal: Define Incidents and Threats of National Interest

Resources are scarce. Defining the incidents and threats that are of interest to a National CIRT is perhaps the most challenging task facing the National CIRT. Determining where the National CIRT should focus its attention is an iterative, evolving process. After the initial formation of an incident management capability, the National CIRT typically becomes inundated with questions and requests for assistance. This places the National CIRT in the position of having to balance the scarcity of time and resources with a desire to serve the community and build its relationships with stakeholders.

During the process of building the National CIRT capability there are several resources that will help the sponsor define the initial focus areas for the National CIRT. These include the following:

– Information systems and incidents that affect those critical infrastructure sectors identified in the National Cybersecurity Policy, if there is one. This should be the primary initial driver behind the National CIRT focus areas. Providing guidance to the National CIRT is one of the principle reasons for having a coordinated national policy.

– Incidents and threats that may affect systems in one or more sectors of critical infrastructure.

– Types of incidents or activity that may be of unique concern to national authorities because they may directly affect national security, result in revealing sensitive information, cause embarrassment to the nation, or because of other unique factors.

– Incidents that substantially affect a majority of computer users in the general public.

– The knowledge and experience of the National CIRT's staff.

– Types of threats that are judged by the National CIRT's incident analysts and the incident response community as part of greater or evolving threats.

– The knowledge and shared wisdom from other National CIRTs.

Having an awareness of the systems currently in use by the National CIRT's key constituents can also help the National CIRT focus its analysis of incidents. This awareness is built over time through handling incidents and interacting with the community.

3.3.2 Enabling Goal: Analyze Computer Security Incidents

All National CIRTs must possess the capability to respond to cyber incidents and provide the community with analysis and support. Not all National CIRTs will have identical specific capabilities to do this work. For instance, National CIRTs will not all have the same level of external partnership with information technology experts, software development communities, and security researchers. Nor will all National

CIRTs have internal teams to perform code-level analysis of malware and software and to replicate attacks and exploits. However, at a minimum National CIRTs should analyze reports of problems for shared characteristics, to determine their importance and accurately gauge the level of threat represented by the problem. Shared characteristics may include such things as attack vector and attack targets. In some cases, these shared characteristics may involve identifying or attribution information that can be useful to the nation's security services.

3.3.3 Enabling Goal: Develop an Efficient Workflow Process

A National CIRT will inevitably receive information from multiple sources about computer security incidents. These notifications will come via email, web form, telephone, fax, or automated process (i.e., event notification from automated information systems and sensors). Personal reports (i.e., those from individuals rather than information systems) should be expected from both known and unknown sources. Known sources include operating partners, information sharing networks, trusted members of private industry, government stakeholders, and significant domain subject matter experts (research scientists, etc). Unknown sources may include reports from citizens and other organizations where a relationship does not exist. One example is the "hotline," which is a posted phone number or instant messaging service which allows all parties to report incidents to the National CIRT 24 hours a day and 365 days a year. These incidents will vary in their severity and importance.

In order for the National CIRT to efficiently and fairly handle reports it should establish a clear, consistent workflow process. Typical steps would include

– Detect incidents.

– Collect and document incident evidence.

– Analyze and triage events.

– Respond to and recover from incidents.

– Learn from incidents.

3.3.4 Enabling Goal: Warn the Community

The National CIRT warns the community it serves for a number of reasons. Timely notification of a threat enables proactive protection of systems as well as recovery from an incident. Warnings and alerts increase the ability of the affected constituents to prepare against and detect threats and vulnerabilities, reducing the potential impact of risk. Warning the community about relevant problems will foster healthy relationships, and promote practices for situational awareness. It also can provide evidence for the "value-added" benefit of a National CIRT.

A National CIRT uses its relationships with stakeholders and with other National CIRTs, as well as its collected incident reports and analysis of those reports, to learn about threats and vulnerabilities and identify information that needs to be distributed to the community. A National CIRT must design warnings to inform the community and encourage them to act to defend themselves. However the National CIRT must balance the need to disseminate the information quickly with the sensitivity of the information and the format of the warning. Such warnings must be sent to the community in a manner that provides for its authenticity, integrity, and privacy where required. In addition, some warnings require confidentiality regarding the source of the information, particularly in cases where an intelligence source supplies threat information. Care needs to be exercised to ensure that while relevant threat information is effectively shared, it is not shared to those without a need to know. Many National CIRTs remove information that may indicate the source of threat and vulnerability data, limiting communications to the vulnerability discovered or obscuring specific threat data.

Warnings from the National CIRT to stakeholders and the national community in general are typically more effective when transmitted through trusted, confidential communications channels that have already been established. These "channels" may take the form of specific individuals or offices in key organizations. Working through pre-established confidential communication mechanisms has proven to

be a very successful strategy for building trusted relationships. As a basis of the trusted relationships, National CIRTs and their stakeholders and major constituents agree upon the communications method, the terms of information handling, and other protections. This enabling goal is closely tied with establishing trusted communications.

3.3.5 Enabling Goal: Publicize Cybersecurity Best Practices

A National CIRT collects information about security problems through various means and its collective historical knowledge is an excellent source of "Lessons Learned." The lessons extracted from incidents can form the basis for targeted skills development and general security awareness. Moreover, these lessons learned often improve situational awareness and contribute to overall cyber risk management. A National CIRT may communicate best practices it has codified through the publication of general cybersecurity best practice documents, guidance for incident response and prevention, training, recommended organizational procedures, and published case studies of practice adoptions. For example, a National CIRT may produce best practices about:

– How to secure specific technologies against known attacks and cybersecurity threats.

– How to develop, test, and exercise emergency response plans, procedures, and protocols.

– How to coordinate with the National CIRT on security research (e.g., vulnerability identification, root cause analysis, and threat and attack community research).

3.3.6 Additional Resources: For Establishing Situational Awareness and Managing Incidents

The following is a list of publicly available resources for establishing cybersecurity awareness and managing incidents:

Reference materials

– Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): http://www.cert.org/octave/

– CERT Resiliency Management Model (RMM): http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

– FIRST Papers & Presentations related to Computer Security: http://www.first.org/resources/papers/index.html

– FIRST Best Practices Guides: http://www.first.org/resources/guides/index.html

– ENISA Quarterly Review: http://www.enisa.europa.eu/publications/eqr

Training resources

– CERT Assessing Information Security Risk Using the OCTAVE Approach: http://www.sei.cmu.edu/training/p10b.cfm

– CERT OCTAVE Approach Instructor Training: http://www.sei.cmu.edu/training/p42b.cfm

– CERT Computer Security Incident Handling Certification: http://www.sei.cmu.edu/certification/security/csih/

– FIRST Network Monitoring SIG meetings: http://www.first.org/meetings/nm-sig/

– Computer Security Incident Handling: http://www.first.org/conference/

– CERT Virtual Training Environment: https://www.vte.cert.org/vteweb/default.aspx

– FIRST Technical Colloquia & Symposia: http://www.first.org/events/colloquia/

– SANS courses: http://www.sans.org/security-training/courses.phP

Materials on Warning the Community

- United States Department of Homeland Securty Stay Safe Online Website: http://www.staysafeonline.org/ncsam
- The United States' US-CERT maintains a repository of cybersecurity situational awareness information: http://www.uscert.gov/
- US-CERT Vulnerability Notes Database: https://www.kb.cert.org/vuls/
- National Institute of Standards and Technology: National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search
- Australia's Stay Smart Online Alert Service: https://www.ssoalertservice.net.au/
- United Kingdom's Warning, Advice, and Reporting Point's newsletters: http://www.warp.gov.uk/Index/WARPNews/indexnewsletter.htm
- International Telecommunications Union's collection of Security Alert Providers: http://www.itu.int/osg/spu/ni/security/links/alert.html

3.4 Strategic Goal: Support the National Cybersecurity Strategy

A National CIRT is a significant operational component of a national approach to executing cybersecurity strategy. A National CIRT participates within a broader context for national incident management against a host of diverse threats (i.e., man-made and natural; physical and cyber). A National CIRT can be used to help

- determine additional national strategic requirements for cybersecurity
- identify needed technical practices, educational improvements, skills development of cybersecurity practitioners, and research and development
- identify opportunities to improve cybersecurity policy, laws and regulations
- distribute lessons learned from cybersecurity experiences affecting the national approach to cybersecurity itself
- improve the measurement of damages and costs associated with cyber incidents.

Perhaps most importantly for the national cybersecurity strategy, the National CIRT can help promote a national culture of cybersecurity. By bringing together diverse stakeholders, the National CIRT can help stakeholders better understand cybersecurity issues and the importance of this area to their various communities.

3.4.1 Enabling Goal: Translate Experiences and Information to Improve National Cyber Incident Management and Cyber Policy Development

While organizations of all sizes will continue to perform internal cyber incident management, a National CIRT alone has the primary responsibility of addressing national level concerns. Translating National CIRT experiences in a way that is useful to policymakers, stakeholders, and the community of security practitioners generally enhances national cybersecurity. Translating experiences implies considering ways in which the National CIRT's work and the experiences of the community may have broader implications for national laws and policies. This translation can produce lessons-learned and improve problem avoidance and risk mitigation nationally, as well as influence national regulations, guidance, initiatives and directives.

One example of such an experience may include incidents involving vulnerabilities affecting a system the national government is considering deploying across its departments, agencies, and ministries. Understanding the inherent risks may determine whether it will choose a technology or not. Another example may involve some ambiguity or inconsistency in privacy law that impedes information sharing

among private stakeholders. The sources for these lessons learned include both the National CIRT's experiences and the experiences of stakeholders.

3.4.2 Enabling Goal: Build National Cybersecurity Capacity

A National CIRT is uniquely situated to serve as a trusted, national focal point. By taking advantage of this, a National CIRT can coordinate with all owners and operators of ICT (private and/or public) to gain a uniquely comprehensive perspective of the national cybersecurity landscape. This allows the National CIRT to support the national cybersecurity strategy, manage incidents of national concern, and support government operations most effectively. A National CIRT typically builds national cybersecurity capacity by publishing best practices and providing services, guidance, training, education, and awareness for the building of other organizational CIRTs.

A National CIRT may foster a national culture of cybersecurity. Publications and advisory services of the National CIRT should be designed to build collective national capability, rather than cater to specific niche needs. It is incumbent on a National CIRT not to act in the capacity of advocating the interests of a particular stakeholder. The National CIRT can act as a valuable bridge between stakeholders and national policymakers. The extent to which a National CIRT can fulfill this role may depend on legal and structural factors.

3.4.3 Enabling Goal: Leverage Public Private Partnerships to Enhance Awareness and Effectiveness

Protecting critical infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government and the private sector, which often owns and operates much of the infrastructure. Successful government-industry collaboration requires three important elements: (1) a clear value proposition; (2) clearly delineated roles and responsibilities; and (3) two-way information sharing. The success of the partnership depends on articulating the mutual benefits to government and industry partners. Benefits to all partners include:

– increased situational awareness through robust two-way information sharing

– access to actionable information regarding critical infrastructure threats

– increased sector stability that accompanies proactive risk management

National CIRT operational and strategic capabilities require active participation from all its partners. Governments and industry should collaboratively adopt a risk management approach that enables government and the private sector to identify the cyber infrastructure, analyze threats, assess vulnerabilities, evaluate consequences, and identify mitigations plans.

3.4.4 Enabling Goal: Participate In and Encourage the Development of Information Sharing Groups and Communities

The National CIRT's participation in information sharing groups and communities is an important way to enhance situational awareness and build trust relationships. Information sharing in this context should ideally be bi-directional between the National CIRT and its community. With regard to infrastructure operators specifically, incident and risk information should flow to the National CIRT from industry while the National CIRT in turn disseminates threat, vulnerability, and mitigation information. Government, the National CIRT, and industry can enhance this information flow by collaboratively developing a formal framework for incident handling, including issues surrounding information sharing. The framework should include policies and procedures for sharing information and reporting incidents, protecting and disseminating sensitive (government and industry) proprietary information, and mechanisms for communicating and disseminating information.

There are several different types of information sharing groups. Where the National CIRT identifies a need for a particular venue in which to share information, it should take the lead in establishing such an organization.

Industry groups are comprised of separate firms in the same industry, for instance the several electrical suppliers in a nation. These groups are often a valuable source of information about vulnerabilities and incidents in a particular industry and can be fruitful venues to catalyze discussion about cybersecurity. While industry groups are very beneficial, participants may sometimes be reluctant to share proprietary or sensitive information in a group of their competitors.

Communities of interest are generally groups with a narrow, technology focus. These groups are integral components of information sharing because they often have deep technical knowledge, skills, and experience to study a problem and create solutions. Participants in these groups are often individuals recognized for their technical skills, leading researchers in the fields of cybersecurity and computer science, and private industry representatives from key information and communications technology providers (i.e., infrastructure providers, software developers, etc.).

In some countries, communities of interest already share information on security threats, vulnerabilities, and impacts. Often, these groups also provide timely alerts and warning to members to facilitate efforts to mitigate, respond to, and recover from actual incidents impacting the critical infrastructures. Examples of these groups include Information Sharing and Analysis Centers (ISACs) in the United States, and Warning, Advice, and Reporting points (WARPs) in the U.K.

Government-Industry working groups can greatly facilitate information sharing. Government can be informed by industry, soliciting comments from industry for cybersecurity policy and strategy development, and coordinating efforts with private sector organizations through information sharing mechanisms. Government should ensure that the private sector is engaged in the initial stages of the development, implementation, and maintenance of initiatives and policies. Industry can benefit from these groups by gaining the opportunity to affect policy making and learning how their sector fits in the overall national security picture.

Finally, the National CIRT can play an important role organizing working groups among interdependent industries. Incidents involving one infrastructure sector can have cascading effects that result in incidents in others, creating interdependencies that are not always anticipated. For example, service disruptions in one public utility may create high volumes of customer calls, disrupting telephone networks. By developing an understanding of how cybersecurity affects multiple systems, the National CIRT can play an important role in helping infrastructure owners and other organizations be sensitive to these interdependencies. Sharing information across infrastructure firms can facilitate the response to incidents that cut across multiple sectors.

3.4.5 Enabling Goal: Assist the National Government in Responding to Incidents in Support of Government Operations

Where it is appropriate, based on political and organizational considerations, the National CIRT enhances its role and effectiveness by handling incident response for government entities. Doing so helps to build trust relationships with government departments and helps the National CIRT maintain an awareness of the systems and technology currently in use. In cases where incident response in specific departments is handled by an in-house CIRT, for instance a CIRT dedicated to the nation's armed forces, the National CIRT can provide support by disseminating threat information and information obtained through outreach with the nation's various organizational CIRTs.

3.4.6 Additional resources: Support the National Cybersecurity Strategy

The following is a list of publicly available resources for understanding how National CIRTs support a national cybersecurity strategy.

Reference materials

– DHS National Infrastructure Advisory Council: Reports and Recommendations: http://www.dhs.gov/niac

– US-CERT Government Collaboration Groups and Efforts to support government infrastructure: http://www.uscert.gov/federal/collaboration.html

– The National Council for Public-Private Partnerships (U.S.): http://www.ncppp.org/

– Partnership for Critical Infrastructure Security, Inc: http://www.pcis.org/

– DHS National Infrastructure Protection Plan and Sector-Specific Plans: http://www.dhs.gov/nipp

– OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

– CIRTs and WARPs: Improving Security Together: http://www.warp.gov.uk/Marketing/WARPCIRT%20handout.pdf

4 Conclusion

Instituting a national computer security incident management capability can be a valuable step towards helping nations manage risk and secure their systems. This handbook is designed to be introductory curricula for cybersecurity capacity development within nations. The intended audience includes potential sponsors of National CIRTs, government policymakers, and individuals responsible for information and communications technologies wanting to learn more about the value proposition of National CIRTs and incident management capability generally. It is not intended to be a guide on the daily operations of a National CIRT, but as informative materials on how a computer security incident management capability may support a national cybersecurity strategy.

The simple truth is that there is a common need to resist, reduce, and fight cyber threats and respond to attacks. National CIRTs and organizations like them provide a domestically-focused, internationally-amplified operational response to those cyber incidents that can destabilize critical infrastructure.

References

URLs are valid as of the publication date of this document.

[Brunner 2009]

Brunner, Elgin M. & Suter, Manuel. *International CIIP Handbook 2008/2009.* Zurich, Switzerland: Swiss Federal Institute of Technology Zurich. 2009. http://www.css.ethz.ch/publications/CIIP_HB_08.

[DHS 2003]

Department of Homeland Security. *The National Strategy to Secure Cyberspace.* Washington, D.C. 2003. http://www.dhs.gov/files/publications/publication_0016.shtm.

[DHS 2008]

Department of Homeland Security. *National Response Framework.*Washington, D.C. 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[DHS 2009]

Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*. Washington, D.C. 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[Killcrece 2004]

Killcrece, Georgia. *Steps for Creating National CIRTs.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. 2004. http://www.cert.org/CIRTs/national/ .

[West-Brown 2003]

West-Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CIRTs).* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. 2003. http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm.

This work was created in the performance of a Federal Government Contract by Carnegie Mellon University for the operation of the Software Engineering Institute; a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license. The ideas and findings in this report should not be construed as an official US Government position. It is published in the interest of scientific and technical information exchange.

Annex B: Best practices for Cybersecurity – Managing a National CIRT with Critical Success Factors

Abstract

This draft report is relevant to Item 2 b) (i) (a) ("with respect to developing a national strategy for cybersecurity, (a) to develop models for national cybersecurity management of the ITU-D Study Group 1 Q22/1 work program) (see Document WTDC-10/162 Rev.1)

National security, economic vitality, and critical infrastructure are increasingly dependent on secure, reliable information and communications technology (ICT). Government authorities are faced with having to secure information and information assets from complex vulnerabilities and poorly attributable threats. These problems are often beyond the reach of traditional governmental and legal processes. National CIRTs are an essential element to supporting national cybersecurity and ensuring the resilience of critical ICT.

While National CIRTs are vital to national cybersecurity, they pose significant management challenges. This paper proposes critical success factors (CSFs) as an aid to leaders and managers in National CIRTs. CSFs are a way to identify the essential attributes and activities that support an organization's success, and they have been used to identify information requirements for executives and align information technology (IT) with business drivers in large organizations. This paper introduces the use of CSFs in the National CIRT community, describes a process to identify them, and provides three examples of how they can be used as part of National CIRT management.

1 Introduction

National security and economic vitality are increasingly dependent on the storage, transmittal, and use of information over interconnected, complex networks. Government and industry leaders are faced with uncertainty and concerns over the confidentiality, availability, and integrity of data and systems that support critical services in their societies. These concerns stem from many causes, including the complexity of the systems themselves, complex supply chains where the end-user is many times removed from the manufacturer, and the rapid exploitation of new vulnerabilities. Online anonymity implies that individuals or groups can affect complex, important systems from behind their own political borders, while national governments are constrained by the limits of their jurisdiction and the speed of legal and organizational processes. As a result, government leaders face a dilemma, one in which they must protect complex, evolving critical information and communications technology (ICT) over which they have little control and which are subject to disruption from a number of poorly understood or non-attributable causes. This security challenge is unique.

A computer security incident response team with national responsibility (referred to in this document as a National CIRT) is an essential organization for helping national constituencies understand and manage cybersecurity incidents. A National CIRT is a nation's primary computer security incident response team, with responsibility to one or more constituencies considered important for national security, public health and safety, critical infrastructure, or economic vitality. National CIRTs are frequently, but not necessarily, a formal part of the government. While many nations have a single National CIRT, it is not unusual for there to be more than one National CIRT, each of which serves its own national constituency. A National CIRT coordinates incident management and facilitates an understanding of cybersecurity issues. It provides the specific technical capability to respond to cyber incidents of interest to its national constituency. In this primary role, the National CIRT provides incident management solutions for government authorities and national constituents.

Beyond the capacity to respond to discrete incidents, National CIRTs can enhance the ability of government departments to fulfill their unique roles. Most government functional areas are touched by IT or cybersecurity threats in some way. Law enforcement and the judiciary are increasingly concerned by the global movement of criminals to the virtual world to commit crimes ranging from the exploitation of vulnerable groups to financial fraud. National CIRTs can help authorities by tracking and analyzing incidents involving the malware and techniques used to commit these types of crimes. The world's defense services, as well as critical infrastructure sectors–such as food, water, and energy–depend on reliable ICT that may be degraded by cyber vulnerabilities of all kinds. The National CIRT can help national governments manage these vulnerabilities by identifying them and educating its constituency on best practices and mitigation.

Finally, National CIRTs can help foster international cooperation on cybersecurity by serving as a communication channel for information about incidents, threats, and vulnerabilities that cross borders. Regional and global collaboration with peer organizations, governments, and technology providers can enhance this capability and help leaders better understand the current state of the global cyber threat.

This paper addresses the unique management challenges facing National CIRTs. These organizations frequently operate under varying legal and political environments, are overseen by differing organizations, are staffed by people with unique skill sets, and are funded at different levels. They frequently have widely differing constituencies, ranging from the owners of government agency networks, to academic networks, to critical infrastructure providers. The services that National CIRTs provide depend strongly on the capabilities of their constituents. For instance, some National CIRTs may serve constituents that already have a robust internal response capability. Others may serve constituents with a limited in-house capability, requiring the National CIRT to provide direct technical assistance. National CIRTs are very rarely "one size fits all" organizations.

Fortunately, these challenges are not unprecedented. Corporations and other industrial organizations have long faced similar problems relating to the management of complex problems, uncertainty, and the demands of ever-changing markets and competitors. While corporations and firms serve different roles in

society, both types of organizations must manage operations in uncertain, complex environments to serve constituents and customers with changing, evolving needs.

Over the last two decades, these challenges have become more acute. As IT has become critical to the operations of most organizations, their leaders have struggled to align the use of technology with their business environment and requirements. One useful tool has been critical success factors (CSFs).

This paper will propose and explain the use of CSFs as an aid to helping National CIRT leaders manage their organizations more effectively. CSFs are an expression of the several activities and attributes that are truly important to the success of the organization. Specifically, the paper will explain CSFs, describe the general process an organization would use to derive its own set of CSFs, and provide three examples of how CSFs can be used to help manage a National CIRT:

– using CSFs as an aid in building a national computer security incident management capability

– using CSFs to select which constituent services to provide

– using CSFs to identify priorities for measurement and metrics

How to Read this Document

This document is intended for managers and leaders involved in operating National CIRTs. It is also intended for leaders in organizations interested in best practices for national cybersecurity. The discussion of CSFs presented in this document might also be of interest to managers in other organizations; for instance, those managing incidents across infrastructure sectors or extended supply chains.

This paper employs the example of a fictional National CIRT charged with the mission "Protect national security and critical infrastructure from cybersecurity threats and vulnerabilities." It is based in no particular country, and is not intended to resemble any actual National CIRT. However, it shares similarities with many incident management organizations. It has limited funding and staffing. Its constituency has evolving and changing needs and may not know what incident management services it really needs. Its parent organization does not really understand what it does or how to measure its performance. The CIRT is usually not noticed until something goes wrong. The goals and CSFs that apply to this fictional National CIRT are not intended to apply generally to actual incident management organizations, although they may to some degree.[3]

The use of CSFs relies on two primary assumptions. The first is that a mission and strategic objectives are in place for the National CIRT. The mission describes what the organization does, and why it does it. The National CIRT mission should ordinarily flow directly from a national cybersecurity strategy, since most of its activity centers on supporting national cybersecurity. Strategic objectives are a more specific articulation of the mission and are designed to provide guidance for the organization itself and also for outside observers seeking to understand the National CIRT's role.

For example, the mission for our fictional National CIRT is "Protect national security and critical infrastructure from cybersecurity threats and vulnerabilities." Strategic objectives may express these in more granular terms, such as

– Protect government networks that store and transport information relating to military operations. Protect systems in the water and power generation infrastructure sectors from software vulnerabilities and attack.

The second assumption, which follows closely from the first, is that the constituency for the National CIRT is defined. This might be an explicit, documented decision made by the sponsoring or governing organization through statutes, memoranda, or other documentation. It may also be implicit and follow

[3] The question of what community CSFs apply to *all* or *any* National CIRT—in other words what every National CIRT must do well—will be the subject of a future paper.

logically from the organizational placement of the National CIRT. For example, a National CIRT operated by national military authorities may primarily support military networks.

Both assumptions may be more or less true in some cases. Many National CIRTs provide services to their constituents despite the lack of a well-defined national cybersecurity strategy or mission. National CIRT constituencies may also be ambiguous. In some situations, National CIRTs may provide services to a variety of stakeholders on an ad hoc basis or as incidents unfold. Nevertheless, the National CIRT's managers must have some idea of what it hopes to accomplish and what constituency it intends to serve. CSFs help leaders manage their organizations to ensure alignment with the mission and strategic objectives. They provide an actionable roadmap with tangible outcomes for measuring success. They will not provide or inform the mission itself.

2 Critical Success Factors

The use of critical success factors started with work conducted by John Rockhart of the Massachusetts Institute for Technology (MIT) Sloan School of Management [Bullen 1981]. This work originally involved helping organizations identify information needs[4] for senior executives. It has also been applied to the question of helping senior IT managers (CIOs and CISOs, for example) plan the use of IT so that it supports business drivers across large organizations. Rockhart advocated using CSFs as a way for senior executives to better manage information systems.

Critical success factors themselves have been defined in different ways in the literature, including:

– key activities in which favorable results are necessary to reach goals

– key areas where things must go right for the business to flourish

– factors that are critical to the success of the organization

– a relatively small number of truly important areas.

These definitions share similarities. Critical success factors are the things that an organization must do, or attributes the organization must have, to achieve its mission. They have been described as things that "must be achieved *in addition to* the organization's goals and objectives" [Caralli 2004]. Indeed, CSFs can be attributes or conditions, such as "be a trusted partner," "passion," "shared ownership," or "clear authority and responsibility." In this sense, CSFs are not simply deconstructed or more granular versions of strategic goals. We will use the following definition:

> *National CIRT critical success factors are the activities that must be done or conditions that must be met in order for the National CIRT to achieve its mission and effectively serve its constituency.*

It is important to understand the relationship and differences between CSFs and strategic goals, as these might initially seem to be interchangeable. Strategic goals are the higher-level objectives that describe what the National CIRT must accomplish. An example might be: "Protect government networks that store and transport information relating to military operations." These typically general statements further describe and explain the mission of the organization. They provide little guidance to National CIRT managers about how to accomplish the strategic goal in the context of their unique operating environments. CSFs, on the other hand, help the manager or executive identify and understand what *must* be accomplished to achieve the strategic goals and mission. These can then be operationalized into actionable activities.

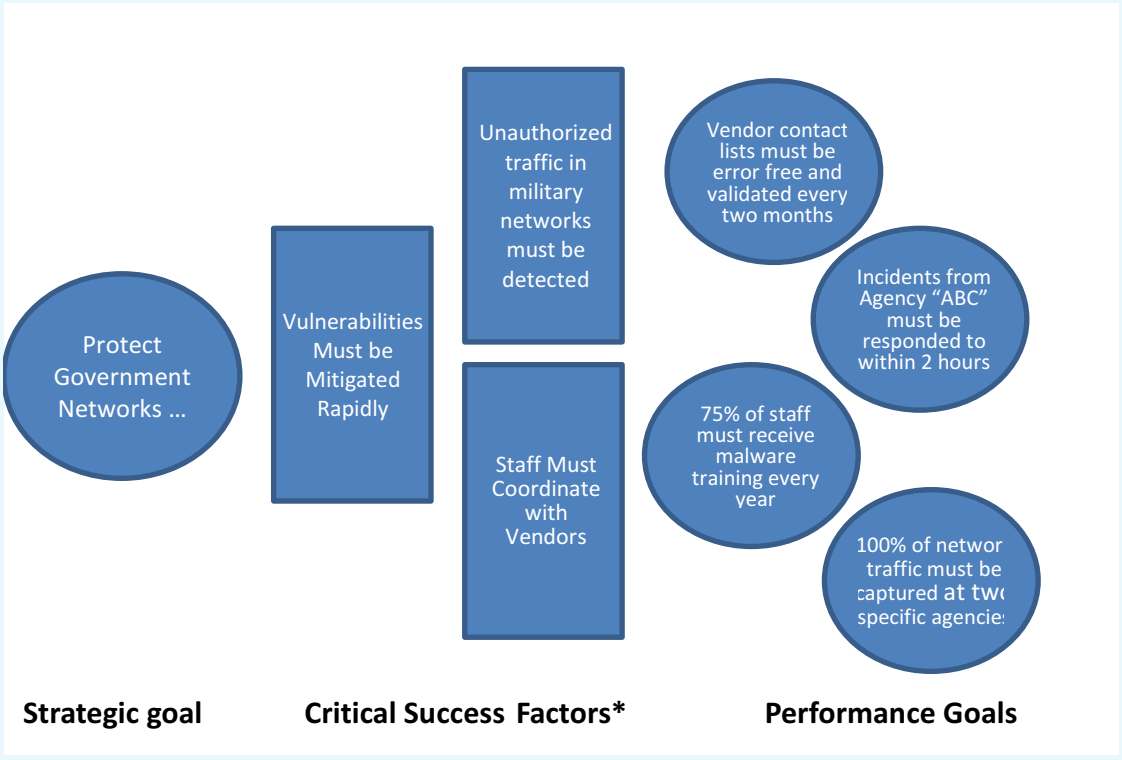
[4] Information needs consist of information executives need about the operations of their organizations. Identifying information needs for executives can be a difficult problem in large, complex organizations because many of the reports or other sources of information are generated, among other reasons, to facilitate routine business functions rather than monitor the health of the organization.

CSFs are also different than performance goals, although they are closely related to them. Performance goals are targets established to contribute to the organization's success or the success of a particular business unit or individual. For instance, the sales office of a manufacturing company may have a goal of "Achieve a 10 percent increase in sales over the next fiscal year." By comparison, a particular CIRT serving a private firm may have the goal "Respond to all incidents within 24 hours."

The usual purpose of performance goals is to provide targets to employees and business units so work can be organized and performance rated. Performance goals are frequently very specific, express quantitative measures of performance, and are often tied to a performance management process. While these types of goals are necessary to operate organizations, they may not always be the best indicator of success. Managers frequently set performance goals based on assumptions about what type of activity is measureable. In fact, they may show a preference for goals that are *easily* measureable, even if the activity does not always directly support the mission of the organization. Because performance goals usually involve the performance management of individuals and business sub-units, managers may also write goals that are generally attainable, for reasons relating to leadership and morale.

More fundamentally, performance goals are not really intended to help managers understand and prioritize their organization's internal activity. Nor are they intended to help solve management problems. Rather, they are for consumption by those performing the work in the organization. CSFs, by contrast, fill the void between strategic considerations and lower-level goals. The following example, derived from our fictional National CIRT, shows how CSFs can bridge the gap between a higher-level strategic goal and performance goals.[5]

Figure 1: Various roles of strategic goals, CSFs, and performance goals



[5] This example includes three of the six CSFs for the National CIRT. The full list appears on page 16.

Figure 1 illustrates a set of strategic goals, CSFs, performance goals, and the roles filled by each of these management tools. The strategic goal "Protect Government networks that store and transport information about military operations" provides guidance and indicates the leadership's intent to the entire organization. At the opposite end of the spectrum, performance goals help those in specific functions to understand how they should be contributing to the overall mission. In this case, the training coordinator knows that 75 percent of staff must receive refresher training on malware each year. Moreover, this performance goal has been explicitly linked to the strategic goal through a formal CSF process. Likewise, incident handlers understand they should respond to incidents from agency "ABC" within two hours.

The critical success factors identified in this case fill an important niche between extremes: they help the managers understand which activities *must* be accomplished to accomplish the mission. Together, strategic goals, CSFs, and performance goals can create a seamless web wherein performance measures and goals closely align with the mission and strategic goals. This understanding and prioritization helps the National CIRT prioritize its efforts to foster resilience across the array of constituent technology and information assets.

2.1 Advantages of a CSF Approach

There are several advantages to developing a formal approach to CSFs in National CIRTs, and organizations generally. These advantages include

– Reducing ambiguity. CSFs can help managers build agreement across their staff on the purpose and activities of the organization. The process of identifying and implementing CSFs can help to foster communication throughout teams by involving them in the discussion, improving the National CIRT's confidence in the decisions made by management.

– Identifying Candidates for Measurement and Goal Setting. As noted, a key aspect of managing any organization is measuring performance. However, measuring organizational performance involves costs and complicated questions. Gathering and analyzing data can consume man hours and require investment in technology. What is to be measured? How often? Many organizations find measuring the right things difficult—or they measure only those activities that are simple to measure [Hubbard 2009]. Sometimes this uncertainty results in no, or sub-optimal, measurement of the organization's activity. Evaluating CSFs can provide clarity and direction on this question, ensuring that measurement and metrics help to produce optimal results.

– Identifying Information Requirements. When closely aligned with goal setting, CSFs can help managers identify what types of information they really need to understand the operations and health of their National CIRTs. Sometimes an objective, thorough evaluation of CSFs can identify information requirements that are not obvious. For example, the success of a National CIRT often hinges on how willing major constituents are to communicate incident and other information to the organization. An objective, formal examination of CSFs may indicate that whether or not the National CIRT is perceived as trustworthy or as a technology leader in its community is a CSF. This can lead the National CIRT manager to request and watch types of indicators and information he or she may not have considered.

– Identifying Risk Management Concerns. CSFs can help identify the vital assets and services supporting the organization's mission. This function can help a National CIRT identify which systems and assets should be subject to a risk management process. This use of CSFs has become common in many industries.

CSFs can be especially helpful for new and evolving organizations like National CIRTs. People in organizations with many similarly-situated peers - the automobile industry for example, which serves a mature market with a long, well studied history - have at least some gut-level understanding of what it takes (i.e., the CSFs) to succeed in their industry. This understanding may be based on organizational learning, talking to peers in other firms, or on historical experiences in the industry. Managers of National

CIRTs do not typically have the same advantages, and can benefit from a formal process to identify their essential practices.

2.2 Sources of CSFs

Much of the existing literature about CSFs centers on private industrial firms. These firms look to various entities and sources to derive CSFs [Rockhart 1979, Caralli 2004]. These include their industry, their peers, the general business climate, government regulation, specific problems or barriers facing the organization, and the different hierarchies in their own organization. For a National CIRT, the sources of CSFs are not very different. They include the following:

– The constituency. This is probably the most important source of CSFs for a National CIRT. The needs and demands of the constituency form a primary input to the services to be provided. Services will vary depending on the constituency. A National CIRT that supports government agencies directly may monitor government agency networks if granted the authority to do so. Alternatively, a National CIRT serving private infrastructure owners and operators may collect incident information through voluntary reporting. Much of its role may relate to disseminating best practices and fulfilling a warning function. Beyond the question of selecting services, the constituency can provide input to operational questions for the National CIRT; for instance, how quickly incidents must be processed or analyzed to be of service.

– Governing or oversight organizations. The organization that sponsors and overseas the National CIRT is an important source of CSFs. This is often expressed in the parent organization's mission or objectives.

– Peers. The experiences of other National CIRTs can form a valuable bank of knowledge to inform operations. For instance, where peer organizations serve similar constituencies or face similar challenges, they may have already learned lessons that can be helpful.

– The legal or political environment. There may be constitutional or regulatory demands or limitations placed on National CIRTs that also affect CSFs. Constitutional limitations may prevent the National CIRT from obtaining certain information, or may place duties on the National CIRT to safeguard particular information to a certain standard. These may include regulations having to do with the privacy of personal information, for instance.

  Organizational issues fall into this category, as well. For example, if the National CIRT is part of an organization that also overseas or regulates the constituency, this organizational relationship itself may create challenges that must be considered. In this particular case, the willingness of constituents to provide information about incidents or their vulnerabilities, despite an obvious concern that it could be used for regulatory purposes, could be identified as a CSF.

– Resource constraints. The resource constraints National CIRTs may face are a potential source of CSFs. A basic constraint in many environments is the limited availability of skilled staff. Other constraints might include uncertainty surrounding funding. Resource constraints may imply CSFs that limit or constrain operations, or the resulting CSF may express the need to alleviate the constraint and develop human capital or funding sources.

2.3 Identifying CSFs

This section is intended to serve as a primer on this topic and to describe a process for identifying CSFs in the context of National CIRTs. The intent is to give National CIRT managers an understanding of the formal process that drives development of CSFs. Additional detail concerning the process of identifying and refining CSFs can be found in the works cited earlier in this report.

Activities such as workshops and working sessions are often used to derive or identify CSFs. The personnel facilitating this work are selected by management based on various traits, such as their ability to think objectively about the organization, their leadership ability, their understanding of the organization, and

their communication skills. Based on the literature in this area, we propose four phases for the identification and refinement of CSFs for National CIRTs. These are

– Defining Scope
– Collecting Data; Document Collection and Interviews
– Analyzing Data
– Deriving CSFs.

2.3.1 Defining Scope

Defining scope usually involves deciding whether the task of collecting CSFs is focused on enterprise priorities for the organization or on operational activities. Enterprise CSFs focus on long-term, major decisions, such as priorities for staffing, which services to offer, which technology to invest in, or whether or not to move into a new facility. By contrast, operational CSFs involve the daily operations of organizations. For a National CIRT, operational CSFs may involve the speed of incident handling or in what priority different types of incidents should be handled.

Many organizations, especially large firms with many subsidiary divisions and departments, start their CSF process at the enterprise level. They do so for the sake of simplicity. However, for smaller organizations or organizations with a flat organizational structure (where there are few organizational layers between managers and workers), collecting both enterprise and operational CSFs at the same time can be effective. Many of the small teams of which National CIRTs are composed share these characteristics and can feasibly derive CSFs in one exercise.

2.3.2 Collecting Data: Document Collection and Interviews

Collecting data to develop CSFs is done in two primary ways, *document collection* and *interviews of key personnel*.

Document collection normally involves gathering important documents that provide information about the essential factors affecting the National CIRT's mission. The types of documents to be gathered usually include

– the national cybersecurity strategy
– the mission statements for the National CIRT and the National CIRT's parent organization
– the mission statements of the most important stakeholders or constituents
– previous audit reports concerning the National CIRT
– previous reports about incidents that have affected the constituency
– the legislation or statutes that establish and give authority to the National CIRT
– important laws or other regulations.

Of the two data collection methods, interviewing is typically the more important and fruitful method. Interviewing managers, employees, constituents, and other stakeholders provides the opportunity to reach agreement and understand what is truly important for the operation of the organization. In addition, the interactive process of an interview allows for participants to help guide the process and expose areas of concern and other nuances in a way that document review usually does not.

For CSF interviews to be productive, the right people must participate in the event, and forethought should be put into the interview questions. For instance, while simply asking a constituent "What are your critical success factors?" can yield useful information, probing or open-ended questions can be more beneficial. For example

– What are your top two or three concerns about losing information?
– How could the failure of an information system jeopardize your organization?

– What are the top two or three things you need to manage cybersecurity incidents, which are currently beyond your capability?

– What would cause you not to share information about vulnerabilities or incidents with our National CIRT?

– How do we earn the trust of people in your organization?

2.3.3 Analyzing Data

After data is collected, it must be analyzed. During the analysis phase, documents and interview responses are examined to identify similar themes. Themes are ideas or activities that seem to recur throughout the documents or responses.

Analyzing documents to identify themes can be relatively straightforward. As an example, Figure 1 presents objectives 3.1 through 3.3 of the *United States Department of Homeland Security Strategic Plan for 2008 to 2013*. Certain sections of these objectives are underlined below. These statements and the themes that relate to them appear in Table 1.

Figure 2: Example: Three objectives from the DHS Strategic Plan for 2008 to 2013

Objective 3.1
Protect and Strengthen the Resilience of the Nation's Critical Infrastructure and Key Resources.

We will lead the effort to mitigate potential vulnerabilities of our Nation's critical infrastructure and key resources to ensure its protection and resilience. We will foster mutually beneficial partnerships with public and private sector owners and operators to safeguard our critical infrastructure and key resources against the most dangerous threats and critical risks. We will strengthen resilience of critical infrastructure and key resources.

Objective 3.2
Ensure Continuity of Government Communications and Operations.

We will implement continuity of operations planning at key levels of government. We will improve our ability to continue performance of essential functions/business and government operations, including the protection of government personnel, facilities, national leaders, and the Nation's communications infrastructure across a wide range of potential emergencies.

Objective 3.3
Improve Cyber Security.

We will reduce our vulnerabilities to cyber system threats before they can be exploited to damage the Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible.

Table 1: Deriving themes from document review

Statement	Theme
"Mitigate potential vulnerabilities."	Mitigate vulnerabilities
"Reduce our vulnerabilities to cyber system threats."	Mitigate vulnerabilities
"Foster mutually beneficial partnerships."	Build partnerships with private industry
"Strengthen resilience of critical infrastructure."	Infrastructure resilience
"Protection of communications infrastructure."	Infrastructure resilience
"…ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible."	Infrastructure resilience

Deriving themes from interview notes is done in a similar fashion, but can be more difficult because the team facilitating the activity must not let their personal biases, the position of the interviewee, or other factors skew the results of the work. A process of normalizing data is usually conducted in order to remove bias and grade interview responses equally. Normalizing data means rewriting and presenting the responses in such a way as to limit the effects of bias or other error.

2.3.4 Deriving CSFs

Deriving CSFs involves taking the themes identified during analysis and further refining them to develop concise, unique CSFs describing the critical areas in which the National CIRT must perform in order to satisfy its mission. Refinement of the themes involves grouping them together by their similar characteristics and, as concisely as possible, expressing what the theme means to the organization. This process is done over and over to eliminate candidate CSFs that are unclear or duplicative. The following is a sample list of operational and enterprise CSFs for our fictional National CIRT.

– Unauthorized traffic in government networks must be detected.
– Negative publicity from security incidents must be managed.
– Staff must coordinate with vendors.
– Vulnerabilities must be mitigated rapidly.
– Strong partnerships must be built with private industry.
– Services must be provided with current in-house staff.[6]

Once CSFs are identified, they must be implemented to be useful. The following section gives three examples of how CSFs can be used to support National CIRT management.

3 Using Critical Success Factors for National CIRTs

The purpose of identifying CSFs is to help National CIRT managers understand their operations and make better decisions. National CIRTs can use CSFs in ways similar to many IT-centric organizations. For instance, CSFs can be used to help manage security and resilience by helping managers understand what

[6] The fictional National CIRT used in this example is like many National CIRTs, in that it faces resource constraints.

services and assets are truly important and need to be secured. They can also help managers determine the relative priority of securing various assets. Closely related to this question, CSFs can be used to help determine the scope for risk assessments. Risk assessment can be a labor- and time-intensive process. Consequently, having a formal process to identify important services, and their related assets, is essential for making risk assessment fruitful. Finally, CSFs can be used to help managers identify the resilience requirements (confidentiality, integrity, and availability) that support information assets.

This section will discuss how CSFs can help leaders who want to build or start a National CIRT. It will then focus more narrowly on two examples involving operational management of our hypothetical National CIRT: selecting services to be offered to the constituency and identifying measurement priorities

3.1 Building a National Computer Security Incident Management Capability

In a previous report in this series [Haller 2010], we identified four strategic goals and a set of enabling goals for the development of a National CIRT capability. These goals are as follows:

1 Plan and establish a centralized computer security incident management capability.

- Identify sponsors and hosts.
- Determine constraints.
- Determine the National CIRT structure.
- Determine the authority of the National CIRT.
- Determine the services of the National CIRT.
- Identify additional stakeholders.

2 Establish shared situational awareness.

- Establish and maintain trust relationships.
- Coordinate information sharing between domestic constituents.
- Integrate risk information from the community.
- Collect information about computer security incidents.

3 Manage cyber incidents.

- Define incidents and threats of national interest.
- Analyze computer security incidents.
- Develop an efficient workflow process.
- Warn the community.
- Publicize cybersecurity best practices.

4 Support the national cybersecurity strategy.

- Translate experiences and information to improve national cyber incident management and cyber policy development.
- Build national cybersecurity capacity.
- Leverage public private partnerships to enhance awareness and effectiveness.
- Participate in and encourage the development of information sharing groups and communities.
- Assist the national government in responding to incidents in support of government operations.

While these strategic and enabling goals outline the activities for building a National CIRT, the previous report does not conclusively describe how to achieve them. Identifying CSFs can be an important step. CSFs can provide clarity and answer basic questions about how these goals can be achieved. Table 2 provides some examples of typical questions that might arise when starting a National CIRT. The enabling goals are taken from the previous paper:

Table 2: Questions to address when starting a National CIRT

Enabling Goal	Questions
Determine the Services of the National CIRT	• What services should be provided? • How can a manager be confident that they are the right services? • In what priority should they be provided? • Provided to which constituents?
Establish and Maintain Trust Relationships	• Establish and maintain trust with whom? • What types of risk information should be integrated?
Integrate Risk Information from the Community	• From which members of the community? • In what priority?
Define Incidents and Threats of National Interest	• Incidents affecting which nationally important systems? • In what priority should they be handled?
Warn the Community	• Which members of the community? • In what priority should they be warned? • Warned with what information?
Build National Cybersecurity Capacity	• What type of capacity should be built? • In what organizations? • In what priority?

A complete description of how CSFs could be used for each goal is beyond the scope of this paper. However, identifying CSFs—what is really important for success-is a discrete, one-time activity that can inform and strengthen many types of organizational decisions.

3.2 Selecting National CIRT Services

The mission and constituency of a National CIRT will determine the services that it provides.

Some services may require large expenditures in terms of funding and staffing.[7] Others may merely duplicate services that constituents can or should do themselves. To avoid wasted time and resources, services should be closely tied to the National CIRT's operating environment, political and other considerations, the needs of constituents, and the activities that are truly important to the success of the National CIRT. In short, they should be tied to CSFs.

[7] Identifying intrusion sets, for instance, is a type of correlation analysis intended to provide law enforcement and other government authorities with information to attribute malicious activity to the persons or entities behind it. This type of in-depth analysis across large sets of incidents can be very labor intensive.

This section will describe the use of affinity analysis to determine the services our fictional National CIRT should provide. Affinity analysis is a common technique for using CSFs and is described as

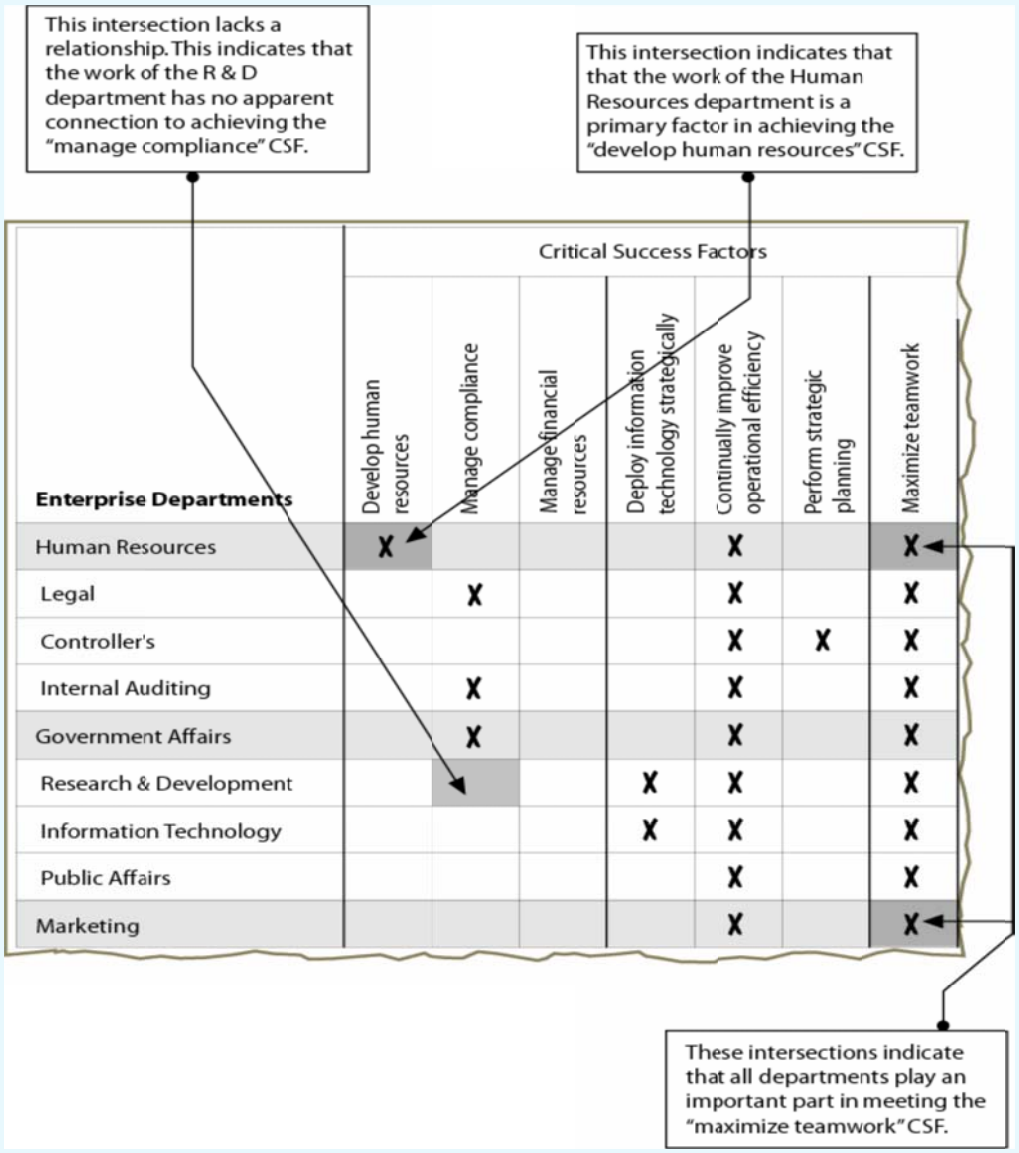
> *…affinity is the inherent or perceived similarity between two things. Affinity analysis is a way of studying this similarity to understand relationships and draw conclusions about the affect of one thing on another* [Caralli 2004].

Affinity analysis is usually performed by constructing a comparison matrix that allows CSFs to be compared and correlated with various criteria. The comparison criteria could be various facets of organizational activity, depending on which type of analysis is to be conducted. For instance, the comparison criteria could be the following:

– organizational processes
– information assets
– physical assets
– security requirements
– performance metrics
– operational unit goals or objectives

The purpose of constructing a comparison matrix is to identify the relationship between some criteria and the CSFs. For instance, in the very simple example below, CSFs are compared to departments in a hypothetical organization to determine which departments support which critical success factors.

Figure 3: CSFs are compared to departments to determine which departments support which critical success factors



The following example involves an analysis of which services our fictional National CIRT should offer its government and critical infrastructure constituency. After a formal process—along the lines described in section two of this report--six CSFs were identified. These are

- Unauthorized traffic in government networks must be detected.
- Negative publicity from security incidents must be managed.
- Staff must coordinate with vendors.
- Vulnerabilities must be mitigated rapidly.
- Strong partnerships must be built with private industry.
- Services must be provided with current in-house staff.

The completed affinity analysis matrix appears on page 18. The matrix was completed by comparing each CSF with each candidate service to determine if the service supported (or was compatible with) the CSF. In this case, the completion of a comparison matrix yields lessons and information helpful to the manager of this National CIRT.

An initial observation is that the CSF "Unauthorized traffic in government networks must be detected" is largely unfulfilled and will be very difficult to accomplish. While there are services that can help the National CIRT detect unauthorized traffic, they cannot be offered while satisfying the constraint CSF "Services must be provided with current in-house staff." In this case, the managers of the National CIRT should further discuss this success factor with their government sponsoring organization, either to further refine or eliminate the requirement or to make the case for more funding so that the National CIRT can hire more, and more highly trained staff.

Another initial observation from the matrix is that the most generally useful service the National CIRT can provide is simply to be a trusted point of contact and coordinator.[8] This is because acting as a coordinator supports a large number of CSFs.

Finally, the matrix indicates a weakness in how the National CIRT is currently staffed. "National Alert and Warning" and "Organizational CIRT Capacity Building" are both services that support two and three CSFs, respectively. However, the National CIRT is currently unable to offer these services because it is not adequately staffed to do so. It cannot provide these services with current in-house staff, which is the last CSF. This indicates a need to hire additional staff to offer these vital services.[9]

[8] In this role, the National CIRT acts as a coordinator for domestic organizations attempting to resolve cybersecurity incidents. It also performs this role for foreign entities inquiring about security incidents that may have some nexus or tie to the National CIRT's constituency. In this role, the National CIRT does not typically analyze or resolve incidents itself, but rather it helps to direct organizations to information, services, or other entities that can help them.

[9] Conversely, the National CIRT is staffed to provide two services, Artifact Handling and Technology Watch, that do not significantly contribute to the first five CSFs.

Table 3: Affinity analysis matrix for fictional National CIRT choosing services

	Candidate Services	Critical Success Factors					
		Illicit traffic in government networks must be detected.	Negative publicity from security incidents must be managed.	Staff must coordinate with vendors	Vulnerabilities must be mitigated in critical infrastructure.	Strong partnerships must be built with private industry.	Services must be provided with current in-house staff
Typical National CIRT Services	Detection of Intrusion Sets						
	Advise the National Government on Cybersecurity Matters		**x**				X
	Assess National Readiness and Crisis Management Capability						
	National Alert and Warning				**X**	**x**	
	Organizational CIRT Capacity Building	**x**			**X**	**x**	
	Trusted Point of Contact and Coordinator		**x**	**x**	**X**	**x**	**X**
	Build Cybersecurity Culture						
Traditional organizational CIRT Services	Incident Handling				**X**		X
	On-site Response	**x**					
	Incident Response Coordination			**x**	**X**		**x**
	Vulnerability Handling				**X**	**x**	**x**
	Vulnerability Analysis						
	Vulnerability Response						
	Artifact Handling						**X**
	Technology Watch				**X**		**x**
	Intrusion Detection Services	**x**			**X**		
	Risk Assessments (provided to infrastructure)				X		
	Education and Training				**X**	**x**	**x**

As is often the case with an analysis using CSFs, the formal process does not yield results that are entirely unexpected. For example, based on historic and anecdotal information, it is often the case that acting as a trusted coordinator is a basic service that broadly supports a variety of functions. However, a formal analytical process helps to foster agreement among managers, stakeholders, and major constituents. In the case of the fictional National CIRT studied here, the comparison matrix offers clear support for the proposition that a basic coordinating service should receive the highest degree of initial support. It is a high-value service in the context of *this* National CIRT. A formal process can also help managers draw other non-obvious conclusions, such as how the staffing in this particular National CIRT is somewhat mismatched with the services that are really needed.

3.3 Identifying Priorities for Measurement and Metrics

Another area in which CSFs can be helpful is identifying measurement priorities for National CIRT managers. Executives in any organization are often faced with a broad variety of information in the form of reports about activity in their organizations. However, in many cases this information is either irrelevant or not helpful to managers trying to determine the health of their organization and whether or not it is accomplishing its mission.

Reports may often be primarily intended for other parts of the organization or to facilitate general business functions. In a for-profit business, these may take the form of accounts receivable reports or sales reports about a particular item. In some organizations, there is little effort aimed at providing leadership with timely, tailored information about the health of the organization. Sometimes it is assumed the operational and working environment changes so rapidly that formalized reporting about the organization's health is not practical, or that it's preferable for managers to determine the state of their organization simply by talking to their staff and customers.

While leaders are usually very interested in knowing the health of their organization, there are costs to measuring intangible aspects of organizational performance. These usually take the form of labor hours and opportunity cost. Therefore, the information requirements for organizational leaders should be identified carefully. CSFs provide a useful way to identify these requirements. In the following example, the CSFs from our fictional National CIRT are presented along with some sample measures that relate to each of them.

Table 4: Sample measurements that support the mission of a National CIRT

Critical Success Factors	Candidate Information Requirement
Unauthorized traffic in government networks must be detected	• Number of incidents year to date involving beaconing to a compromised or malicious host • False positive rate for event detection rules • Percentage of government access points being monitored • Frequency of updating event detection criteria
Negative publicity from security incidents must be managed	• Number of inquiries to the designated public affairs contact person • Percentage of news stories involving security incidents in the constituency where the National CIRT first learned about the incident from the media itself • Number of news stories involving computer security incidents among the National CIRT's constituency. • Number of media inquiries answered by National CIRT personnel other than the designated media point of contact

Critical Success Factors	Candidate Information Requirement
Staff must coordinate with vendors	• Number of IT vendors used by the constituency vs. the number of vendors in the National CIRT's rolodex.
Strong partnerships must be built with private industry	• Number of incidents voluntarily reported by private industrial constituents • Number and trending of private industry inquiries to the National CIRT about emerging security threats • Number of training courses taught at major private industry stakeholders every year.
Vulnerabilities must be mitigated rapidly	• Percentage of recurring incidents with costs greater than X from known route causes • Cycle time between report of zero-day vulnerability and patching done across the constituency • Percentage of incidents reported that relate to known vulnerabilities that are at least 45 days old.

Alternatively, National CIRT managers may have a catalogue of *existing* reports about their organization's activity from which to choose. Or, they may be faced with the task of selecting incident management software that may offer different types of report functionality. In these cases affinity analysis using CSFs—similar to the example in the previous section - can be used to help determine what types of reports should be sustained or which types of reporting utilities would most benefit the organization.

4 Conclusion

CSFs are valuable tools that can help managers in complex organizations make timely decisions and prioritize their services and assets. It is hoped that the materials in this report provide an understanding of how the formal identification and use of CSFs can help the National CIRT manager and other personnel tie their activities directly to the success of the organization.

Managing National CIRTs is a unique, complex leadership challenge. These organizations fill an ever more vital role and help national constituencies understand and manage cybersecurity incidents. The management of National CIRTs must evolve and formalize so that they fully support national cybersecurity and integrate smoothly in their unique operating environments. National CIRTs are evolving organizations and tools such as CSFs may help in their management.

References/Bibliography

URLs are valid as of the publication date of this document.

[Bullen 1981]

Bullen, Christine V. & Rockhart, John F. *A Primer on Critical Success Factors* (Working Paper 1220-81, 69). Sloan School of Management, Center for Information Systems Research, 1981. http://dspace.mit.edu/handle/1721.1/1988

[Caralli 2004]

Caralli, Richard A. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/library/abstracts/reports/04tr010.cfm

[CERT 2002]

CERT Program. CIRT Services. http://www.cert.org/CIRTs/services.html (2002).

[DHS 2008]

Department of Homeland Security (DHS). U.S. Department of Homeland Security Strategic Plan: Fiscal Years 2008–2013. http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf (2008).

[Haller 2010]

Haller, John; Merrell, Samuel A.; Butkovic, Matthew J.; & Willke, Bradford J. *Best Practices for National Cybersecurity: Building a National Computer Security Incident Management Capability* (CMU/SEI-2010-SR-009). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10sr009.cfm

[Hubbard 2009]

Hubbard, Douglas & Samuelson, Douglas A. "Analysis Placebos: The Difference Between Perceived and Real Benefits of Risk Analysis and Decision Models." *Analytics Magazine* (Fall 2009): 14–17. http://viewer.zmags.com/publication/2d674a63#/2d674a63/1

[Rockhart 1979]

Rockhart, John. "Chief Executives Define Their Own Data Needs." *Harvard Business Review* (March/April 1979): 82–84.

This work was created in the performance of a U.S. Federal Government Contract by Carnegie Mellon University for the operation of the Software Engineering Institute; a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license. The ideas and findings in this report should not be construed as an official US Government position. It is published in the interest of scientific and technical information exchange.

Annex C: Best practices for Cybersecurity – Guide for the Establishment of a National Cybersecurity Management System

Abstract

This document contains the revised version of the contribution from Morocco contribution on a “National Cybersecurity Management System: Framework – Maturity Model – Responsibilities and Implementation Guide” as a National Roadmap for Global Cybersecurity for discussion in Question 22-1/1. The changes in this document are dated July 27, 2011 and include the following:

1 Proposed changes by the U.S. delegation, recorded in the May 2011 Rapporteur’s Group Document RGQ 22-1/1/008 and Document 1/102-E submitted to the September 2011 meeting;

2 Changes in the various models describing the proposed approach;

3 Additional paragraph defining the maturity model, taken from the COBIT (ISACA), and this in response to remarks by the representative of FIRST "That There Is a Difference between a" model "and a" maturity model ";

4 Explanation of the process "EM1" (NCSec observatory);

5 Introduction of a new table on "Information Criteria NCSec";

6 Improved descriptions of some of the processes of the maturity model.

Executive Summary

This report is responsive to Question 22-1/1, work item 2 b) ii) a), namely, “to develop models for national security management.The digital revolution has changed how business is transacted, how governments operate. Globalization and technology advancement have made critical infrastructure vulnerable and thus a potential terrorist target. Countries face real risks, and vulnerabilities in the critical information systems could be exploited by adversaries. They seek to incapacitate critical infrastructure and key resources to threaten national security, causing considerable mass casualties, weaken world economy, and damage public morale and confidence. Cyberspace is far from secure today. In the light of this changing environment, there is an urgent need to take action – at national as well as international levels – against all forms of cyberthreats.

It is the role of governments to face computer security challenges. These challenges are serious in a context where there is an absence of appropriate organizational and institutional structures to deal with incidents. But more important than the question of which agency or agencies should be given the responsibility for computer security is the point that some national leadership should be designated to ensure that computer security will receive government-wide attention. Therefore, sectors and lead agencies should assess the reliability, vulnerability, and threat environments of the infrastructures and employ appropriate protective measures and responses to safeguard them.

Countries suffer from a lack of international standards for a State or a region to measure its current security status. Existing standards, such as ISO 27000 family and Cobit, for example, are not adapted to information security implementation at both national and regional levels.

Governmental Cybersecurity Policies are not enough. It becomes necessary to create and endorse a "Generic Policy Model" of Cybersecurity, associated to "National Coordinated Strategies" against cyberthreats, answering also the needs of ITU through its "Global Cybersecurity Agenda". This process requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices, and consideration of the role of all stakeholders.

Appropriate national and regional organizational structures to deal with cyberthreats are needed more than any time.

The ITU has already proposed a whole process for developing and implementing a national Cybersecurity plan. But this process requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices, and consideration of the role of all stakeholders.

This contribution proposes global Governance answering the former needs expressed by the ITU. It is intended to present «NCSecMS», the "National Cybersecurity Management System", which is a guide for the development for effective National Cybersecurity. It ensures the implementation of a National Roadmap of Cybersecurity Governance, through the 4 following components:

1 "NCSec Framework" proposes five domains and 34 processes for covering main issues related to Cybersecurity at the National level, as the ISO 27002 for organizations;

2 "NCSec Maturity Model", classifies "NCSec Framework" processes depending on their level of maturity;

3 "NCSec RACI chart" helps to define roles and responsibilities for the main stakeholders concerned by Cybersecurity in a country or a region;

4 "NCSec Implementation Guide" is a generalization of ISO 27001 and 27003 standards at the national level. It underlines best practices that organizations can use to measure their readiness status.

This proposal defines a methodology to implement a Roadmap of National Cybersecurity Governance, including a framework of Best Practices and a Maturity Model, to assess for different aspects related to National Cybersecurity.

1 Introduction

1.1 Cyber Challenges and Threats

We are heading toward a future of "pervasive computing" in which information technology will be ubiquitously integrated into everyday objects. Information and Communication Technologies (ICT) is a critical component of innovation and is responsible for nearly 40% of productivity growth worldwide. In addition, this highly innovative sector is responsible for more than a quarter of the total industrial effort and plays a key role in the creation of economic growth and jobs throughout a number of economies. The availability, reliability and security of networks and information systems are increasingly central to economies and to the fabric of society.

The information technology infrastructure is critical, but its protection is more critical, by deploying sound security products and adopting good security practices. A number of analysts think that the Cybersecurity threat is real, imminent, and growing in severity. Though Cybersecurity is a problem of national importance, the risks are often underestimated. The relevance of information and communication technologies (ICT) for the economies is undeniable.

There have been significant changes in the level of sophistication of cyberthreats since 1986 when the first known case of a computer virus aimed at advertising a Computer Store in Lahore, Pakistan, was reported.

Spam has also evolved to become a vehicle for delivering more dangerous malware and payloads, such as the dissemination of viruses, worms and Trojans that are today a means for online financial fraud, identity or trade-secret theft as well as various other forms of cyber threats. One of the emerging and rather dangerous trends is the shift in strategy by hackers from the central command-and-control model for controlling botnets to a peer-to-peer model with a distributed command structure capable of spreading to computers located in different countries.

About 70% of global email volume is nothing else but spam. Spam is now used as a vehicle for spreading viruses and spyware. After security violations, damages were experienced by: 25.4% of business end-users; 36.2% of active Internet users. The increasing deployment of mobile devices (including 3G mobile phones, portable video game consoles, etc.) and mobile-based network services poses new threats to security. These threats could turn out to be more dangerous than attacks on PCs as the latter already have a significant level of security. Governments worldwide have faced the computer securities challenges. This challenge is serious where, there is an absence of appropriate organizational and institutional structures to deal with incidents (such as virus and network attacks resulting in fraud, the destruction of information and/or the dissemination of inappropriate content) is also a genuine problem in responding to cyber attacks.

But more important than the question of which agency or agencies should be given responsibility for computer security is the point that some national leadership should be designated to ensure that computer security will receive government-wide attention. Therefore, sectors and lead agencies should frequently assess the reliability, vulnerability, and threat environments of the infrastructures and employ appropriate protective measures and responses to safeguard them.

1.2 Strategic context

Cybersecurity has been considered as a priority since a long time: indeed, ITU Membership has been calling for a greater role to be played by ITU in matters relating to Cybersecurity through a number of resolutions, decisions, programmes and recommendations. Moreover, the ITU Secretary-General has set Cybersecurity as a top priority. ITU constitutes hence a unique global forum to discuss Cybersecurity.

Between 2003 and 2005, world leaders at the « World Summit on the Information Society » (WSIS) entrusted ITU as sole facilitator for WSIS Action Line C5 – « Building Confidence and Security in the use of ICTs ». WSIS has mandated ITU to promote a global culture of Cybersecurity.

In 2006, ITU Plenipotentiary Conference in Turkey put Cybersecurity as a priority for the Union, in terms of resolutions and strategic plan. The conference delegates also gave ITU a clear mandate to focus on infrastructure and Cybersecurity.

In 2008, during ITU « World Telecommunications and Standardization Assembly » (WTSA) in South Africa, one of the three evening side events corresponded to Cybersecurity topics. It was convened to address the global concern of security in information and communication technologies (ICT), as well as providing a high-level overview of the subject. This side event also provided insights on security challenges faced by ICT community, including network operators, enterprises, governments and individuals.

In 2010, ITU World Telecommunication Development Conference (WTDC), held in India, put Cybersecurity as a priority in ITU-D work programme.

1.3 ITU & WSIS

The outcomes of both phases of the « World Summit on the Information Society » (WSIS) emphasize that building confidence and security in the use of ICTs is a necessary pillar for building a global information society. Indeed, the « WSIS Declaration of Principles » states that « strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs ». It further states that a « … global culture of Cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies ».

In particular, the Agenda of the second phase of the WSIS describes the establishment of a mechanism for implementation and follow-up to WSIS, and requests ITU to play a facilitator/moderator role for the WSIS Action Line C5.

The WSIS Phase II Agenda, proposed in Tunis, seeks to « build confidence and security in the use of ICTs by strengthening the trust framework ». It also reaffirms « the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of Cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks ».

This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. Access and trade will be enhanced by continued development of the culture of Cybersecurity. It will have to take into account the level of social and economic development of each country and to respect the development-oriented aspects of the Information Society.

The crucial role that confidence and security play as one of the main pillars in building an inclusive, secure and global information society was one of the main conclusions of the World Summit on the Information Society (WSIS).

The global nature of the legal, technical and organizational challenges related to Cybersecurity can only be properly addressed through a strategy that takes account of the role to be played by all relevant stakeholders, existing initiatives in a framework of international cooperation.

Attempts to address these challenges at the national and regional levels are not sufficient due to the fact that the information society has no definite geographical borders.

1.3.1 Action Line C5

WSIS Action Line C5's goal is to help building confidence and security in use of ICTs. As mentioned above, the WSIS recognized the real and significant risks posed by cyberthreats and entrusted the ITU to facilitate the implementation of WSIS Action Line C5: « Building confidence and security in the use of ICTs ».

We will remind the different areas covered by the Action Line C5 along with extracts from the WSIS texts highlighting building confidence and trust in the use of ICTs:

– Critical Information Infrastructure Protection (CIIP) ;

– Promotion of a Global Culture of Cybersecurity;
– Harmonizing National Legal Approaches, International Legal Coordination and Enforcement;
– Countering Spam;
– Developing Watch, Warning and Incident Response Capabilities;
– Information Sharing of National Approaches, Good Practices and Guidelines;
– Privacy, Data and Consumer Protection.

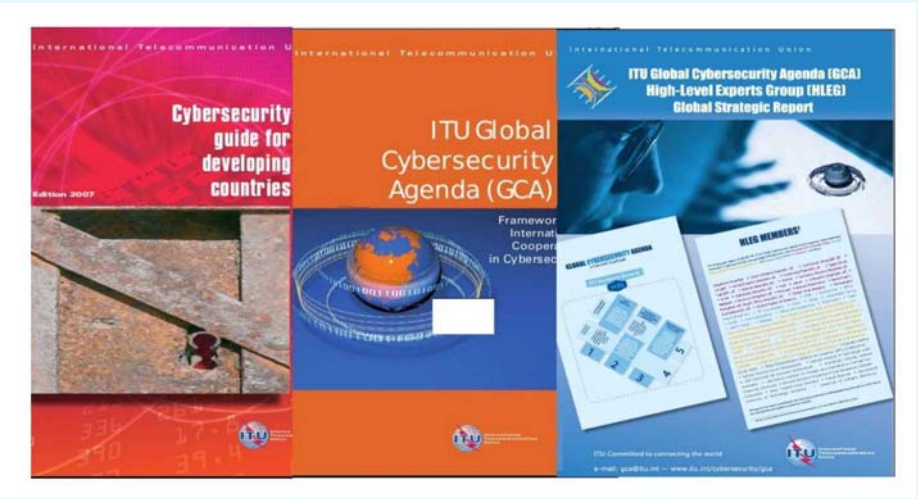
According to these statements, confidence and security in using ICTs are vital and fundamental in building an inclusive, secure and global information society as acknowledged by the WSIS.

In this context, and in response to its mandate as sole Facilitator of WSIS Action Line C5, the ITU launched, on 17 May 2007, the Global Cybersecurity Agenda as a framework for international cooperation aimed at enhancing confidence and security in the information society.

ITU has been entrusted by the WSIS community of stakeholders to facilitate the implementation of WSIS Action Line C5 (Building confidence and security in the use of ICTs). With its 191 Member States and more than 700 Sector Members, ITU is uniquely placed to propose a framework for international cooperation in Cybersecurity. Its membership includes the least developed, developing and emerging economies as well as developed countries. ITU therefore provides a forum where these diverse views of what Cybersecurity and cyberthreats mean to various countries can be discussed, with the goal of arriving at a common understanding amongst countries on how these challenges can be addressed.

1.3.2 ITU's Global Cybersecurity Agenda

Figure 1: Global Cybersecurity Agenda



The Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing solutions to enhance confidence and security in the information society. It will be built on the basis of existing national and regional initiatives in order to avoid duplication of work and encourage collaboration with all relevant partners.

The main goal of Global Cybersecurity Agenda (GCA) is to propose solutions to address some of the challenges faced today in Cybersecurity and cyberthreats. The ultimate objective of the Global Cybersecurity Agenda is to make significant progress on the agreed goals within the framework of fight against cybercrime. It will also increase the level of confidence and security in the information society. It

will be based on international cooperation, and will strive at getting the engagement of all relevant stakeholders in a concerted and coordinated effort to make a difference and to build security and confidence in the information society.

The GCA rests on five pillars or work areas:

1 Legal Measures: to develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner;

2 Technical and Procedural Measures: to focus on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards;

3 Organizational Structures: to consider generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyber attacks, including the protection of countries' critical information infrastructure systems;

4 Capacity Building: to elaborate strategies for capacity building mechanisms to raise awareness, transfer know-how and boost Cybersecurity on the national policy agenda;

5 International Cooperation: to develop a strategy for international cooperation, dialogue and coordination in dealing with cyberthreats.

Since its launch, GCA has attracted the support and recognition of leaders and Cybersecurity experts around the world: H.E. Blaise Compaoré, President of Burkina Faso and H.E. Dr Óscar Arias Sánchez, Former President of the Republic of Costa Rica and Nobel Peace Laureate, are both Patrons of the GCA.

An important new element of the GCA is the ITU's Child Online Protection initiative which is a unique and global initiative bringing together partners from all sectors of the community to identify key risks and vulnerabilities in cyberspace; create awareness; develop practical tools; and share knowledge and experience.

The GCA has benefited from the advice of an expert panel, the High-Level Experts Group, on the complex issues surrounding cybersecurity.

1.3.3 HLEG Report

The Report of the Chairman of the High Level Expert Group (HLEG) to the Global Cybersecurity Agenda (GCA) launched by the Secretary-General on 17 May 2007 summarizes the proposals of various experts with respect to the seven main strategy goals embedded within this initiative, with concentration on relevant Recommendations for the following five working areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structure; 4) Capacity building; and 5) International cooperation.

1.3.4 ITU Q22/1 Report on Best Practices

In the last study cycle (2006-2009), ITU-D Question 22/1 developed a report on "Best Practices for a National Approach to Cybersecurity: Building Blocks for Organizing National Cybersecurity Efforts." At WTDC-10, it was agreed that Question 22-1/1 should develop more in-depth reports on various topics in the Report on Best Practices, including reports on models for national security management.

1.4 National Issue: Lack of standards

Cybersecurity organizational and institutional structures may not always be systematically efficient at the national level; this situation makes it difficult, at times, to deal with cyber threats and incidents. National Cybersecurity challenges are serious in a context where there may be a lack of standards that can help countries identifying responsibilities for specific elements. There are numbers of different best practice documents at the organizational level, in order to affect responsibilities, but there is not always clear guidance for states and regions in this arena.

Cybersecurity standards enable organizational structures to practice safe security techniques in order to minimize the number of successful Cybersecurity attacks. Cybersecurity implementation becomes easier with these guides, through general outlines and specific technical specifications.

Many norms and models that deal with information security do exist: We can mention, for example, ISO/IEC 27000 family, COBIT, etc. Do these norms address Cybersecurity at the national level?

1.4.1 ISO 27000 family

The basis of the standard was originally a document published by the UK government, re-published first by BSI as BS7799, and by ISO, as ISO 17799, then 27001. The ISO 27002 standard is a code of practice for information security. These two documents are intended to be used together, with one complimenting the other. For the time being, the ISO 27000 series of standards have been specifically reserved by ISO for information security matters at the organizational level, not at the national level.

These control objectives can't be used at the national level. But the methodological approach suggested by ISO is interesting. If adapted to the National context of Cybersecurity, it would offer an appropriate framework of cyberconfidence. This is one of the objectives of the proposed « National Cybersecurity Framework », and more specifically the pedestal of the whole discussed process. So, as for ISO/IEC 27002, one should first define « control objectives » at the national level.

1.4.2 Cobit

Cobit is a framework developed for IT process management with a strong focus on control, and less on execution. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. Cobit's good practices represent the consensus of experts. The maturity model associated to Cobit measures the degree of achievement of processes, and identifies the associated responsibilities of business and IT process owners. Cobit can't be applied to the national level.

1.4.3 Community Cybersecurity Maturity Model (CCSMM)

The Community Cybersecurity Maturity Model provides a structure which communities and states can use to determine their level of preparedness and to create a plan to improve their security posture and enhance their chances of successfully preventing or detecting and responding to a cyber attack.

But this proposition suffers from the following lacks: The methodology is empiric, based on professional experience rather than systematic approach; The proposed maturity model is not based on a global framework that is already settled, which means that it will be too complex in order to be deployed; The number of stakeholders is limited to 3, which are: Government, Critical Infrastructure, and Citizens. Whereas in reality, one has to consider more, such as Private Sector, and Academia; The proposed level of maturity n°5 is called: "Full Security Operational Capability", whereas we all know that "Total Security" doesn't exist. It is recommended in this situation to replace it with "Optimized Security" that is under improvement.

1.4.4 Need for National Standards

This maturity model is dedicated to Critical Infrastructure, which makes it difficult to be applied under a more general e-Government vision.

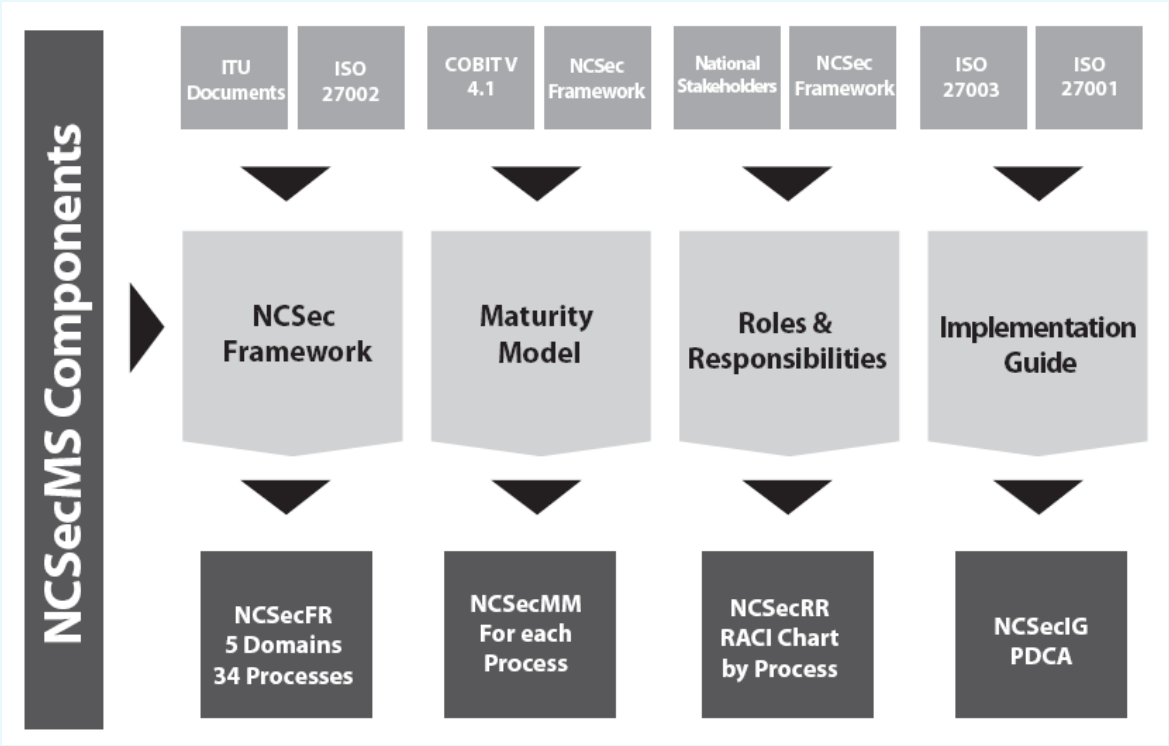
As a conclusion, we do need indicators at the national level, which link strategic national goals to IT goals, providing metrics to measure their achievement, and to identify from a Cybersecurity viewpoint the associated responsibilities of stakeholders and control process. After identifying critical Information Technology processes and controls, it becomes easier to point out vulnerabilities and demonstrate them to management. Action plans can be developed to bring these processes up to the desired target level.

We do need to follow an efficient methodology for identifying functional areas where there are ambiguities in terms of responsibilities, at the national level, bringing the differences out and resolving them through a cross-functional collaborative effort.

1.5 National Cybersecurity Management System

National Cybersecurity Management System, called "NCSecMS", can be considered as a tool the goal of which is to facilitate the achievement of National Cybersecurity, at both the national and regional levels. It consists in 4 steps, containing the following components:

Figure 2: National Cybersecurity Management System



Step 1: NCSecFR (Framework)

The best practice proposal for National Cybersecurity, called "NCSecFR", is a global framework answering the needs expressed by the ITU in its Global Cybersecurity Agenda (GCA). Fully inspired from ISO 27002 standard, it is a code of practice for Organizational Structures and Policies on Cybersecurity at the national level, consisting in 5 domains and 34 processes, in order to help building regional and international cooperation for watch, warning, and incident response.

Step 2: NCSecMM (Maturity Model)

As long as a global national framework for Cybersecurity is defined, the "NCSecMM" is associated to this best practice proposal for National Cybersecurity, called "NCSecFR". Inspired from Cobit's maturity model, it will enforce national Cybersecurity Management System implementation, showing thus what has to be done to improve for each process, at the national and regional levels.

Step 3: NCSecRR (Roles & Responsibilities)

Responsibility Charting is a technique for identifying functional areas where there are process ambiguities, bringing the differences out, and resolving them through a cross-functional collaborative effort. A "National RACI chart", called "NCSecRR", is provided, and defines, among the stakeholders, who are "Responsible", "Accountable", "Consulted" and "Informed" for each of the 34 NCSec processes. The "RACI chart" defines in detail what has to be delegated and to whom, and what kind of responsibility will be affected to one stakeholder instead of another.

Step 4: NCSecIG (Implementation Guide)

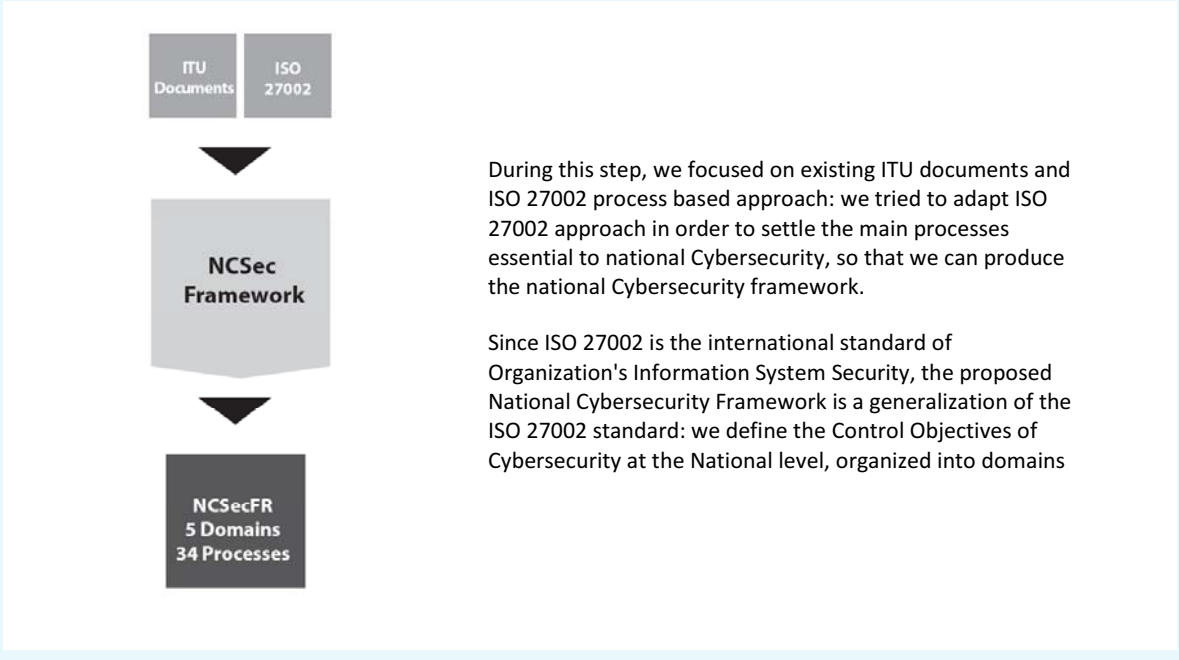
The implementation guide associated to National Cybersecurity, called "NCSecIG", offers an efficient process control mechanism, in order to guarantee a good comprehension of the interaction between these processes, using ISO 27001 and ISO 27003 approaches.

1.6 Resolution approach

In order to reach the corresponding goals of ITU, which consist in the elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on Cybersecurity, and the development of strategies for the creation of a global framework for watch, warning and incident response, we have adopted the following resolution approach for each of the 4 steps: it takes into account the already settled orientations and goals of the ITU instances, and is fully compatible with.

1.6.1 Building a framework for National Cybersecurity (NCSecFR)

Figure 3: NCSec Framework (Step 1)



We also propose a global roadmap for Cybersecurity Governance, which includes:

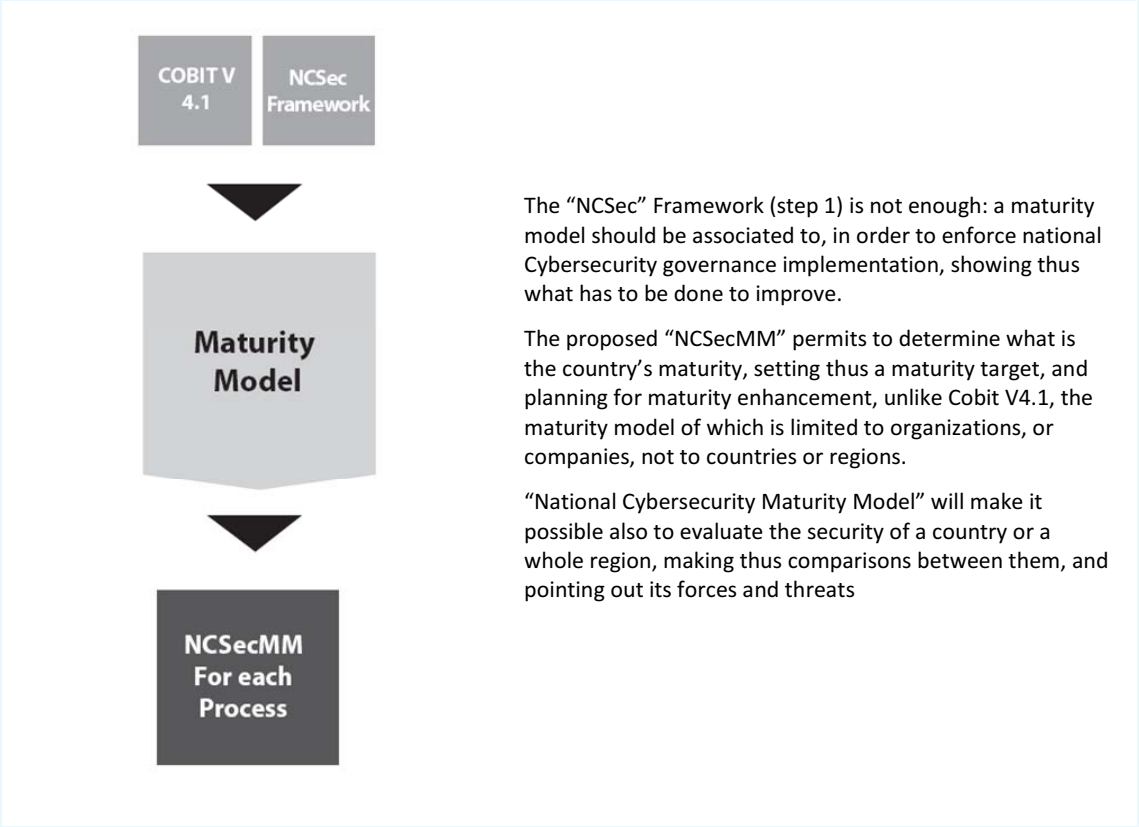
– The identification of stakeholders, involved in the application of National Cybersecurity strategy and policy;

– The definition of resources, essentially the organizational structures responsible for the implementation of National Cybersecurity processes;

– The information model, consisting in proposing National Cybersecurity performance measurement indicators: it is responsible for the monitoring of strategy implementation, resource usage, and process performance. It is based on specific information measurement criteria, leading to achieve goals measurable beyond conventional accounting.

1.6.2 National Cybersecurity Maturity Model (NCSecMM)

Figure 4: NCSec Maturity Model (Step 2)



1.6.3 Roles and Responsibilities model (NCSecRR)

Figure 5: NCSec RACI Chart (Step 3)

In this step, we identify functional areas where process ambiguities do exist, bringing the differences out, and resolving them through a cross-functional collaborative effort. It is of a main importance to define in detail what has to be delegated and to whom, and what kind of responsibility will be affected to one stakeholder instead of another.

Thus, it will aid organisations and teams identifying the responsibility for specific elements at the national level, at the process level of the NCSec Framework.

A specific National RACI chart will be proposed, defining for each stakeholder who is Responsible, Accountable, Consulted, or Informed

1.6.4 Implementation Guide (NCSecIG)

Figure 6: NCSec Implementation Guide (Step 4)

Structuring every aspect of NCSec Framework is a major priority. It is important to offer an efficient process control, in order to guarantee a good comprehension of the interaction between these processes. The Implementation Guide will make it possible to structure every process using ISO 27003 and ISO 27001 approaches:

- ISO 27003 will provide help and guidance in implementing an ISMS (Information Security Management System), including focus upon the PDCA method, with respect to establishing, implementing reviewing and improving the ISMS itself.

  ISO 27001, through the "Plan-Do-Check-Act" (PDCA) model, will be used to structure every process. It will also structure the maturity model itself. PDCA approach will be automatically used within the whole process of implementation of NCSec Framework and Maturity Model

2 National Cybersecurity Framework

2.1 How NCSec Framework meets the needs

Cybersecurity governance is to be built essentially on a **National Framework** able to address and govern cyberthreats issues at a national level. In a boundless cyberspace, it should also be able to afford the needed cooperation in a regional and international level in order to meet its goals.

A Framework for National Cybersecurity Management System mainly may rest on:

– National Legal Foundation;

– Technical Measures;

– Organizational Structures;

– Capacity Building;

– International Cooperation.

These elements are in line with the broad goals of the Global Cybersecurity Agenda (GCA), and its five (5) strategic pillars (or Work Areas).

Suggested Framework should be organized so as to meet the goals of the GCA initiative, to address the global challenges related to the five (5) Work Areas.

2.1.1 National Legal Foundation

Every country needs laws that address Cybersecurity, procedures for electronic investigations, and assistance to other countries as cyberspace is borderless. The protection of cyberspace requires updating laws and particularly criminal law, procedures and policy to address and respond to cybercrime.

The proposed National Cybersecurity Framework (NCSecFR) makes it possible to elaborate and maintain strategies for the development of model Cybersecurity legislation that is globally applicable and interoperable with existing national and regional legislative measures (Goal 1).

A certain number of sub-goals were elaborated in order to meet the identified objectives from a legal viewpoint. The proposed solution is applicable and interoperable with existing national, transnational and regional initiatives for the prevention of cyberthreats.

2.1.2 Technical Measures

It is important for a country to develop a strategy that enables the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems (Goal 3).

Without deepening in technical matters and implementation details, the proposed National Cybersecurity Framework (NCSecFR) includes sub-goals and objectives that guarantee the establishment of globally accepted security services and mechanisms at both the national and regional levels.

2.1.3 Organizational Structures

The protection of cyberspace and particularly the CIIP requires appropriate *structures or* organizations for securing cyberspace, which includes watch, warning, response and recovery efforts and the facilitation of collaboration between and among government entities at both the national and international levels.

In the proposed NCSec Framework, strategies have been elaborated in order to create appropriate national organizational structures and policies on Cybersecurity (Goal 2).

It will be important to create a focal point and mechanisms to coordinate all the efforts to serve as a focal point for coordination. The proposed NCSecFR has developed a strategy for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives (Goal 4).

2.1.4 Capacity Building

Despite increased awareness around the importance of Cybersecurity and the taken measures to improve capabilities, cyber risks continue to underlie national information networks and the critical systems they manage. Reducing that risk requires an unprecedented, active partnership among diverse components.

But raising awareness, even if it is important, is not enough. Capacity building goes far beyond awareness, because it will solve most of the problems of Cybersecurity that are due to the human dimension of cybersecurity. In fact, most of the time, humans are the weakest link of the security chain: in fact, human-being is the end user of ICT services, infrastructure and security.

Enforcing capacity building at the national level will oblige each country to develop effective legal framework, compatible at the international level. It will promote the adoption of Cybersecurity measures, and the settlement of adequate organizational structures. Also, it will enhance cooperation at national, regional and international levels.

The proposed National Cybersecurity Framework allows the development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across the sectors and amongst the players, in all the above-mentioned areas.

2.1.5 International Cooperation

In order to settle a framework of international cooperation, a national strategy based on efficient national cooperation and coordination between stakeholders is to set and determine Cybersecurity issues and consider protection of cyberspace in general and CIIP in particular as essential to national security and a nation's economic well-being.

The global nature of the legal, technical and organizational challenges related to Cybersecurity can only be properly addressed through a strategy that takes into account the role to be played by all relevant stakeholders, within a framework of international cooperation. Countries will adopt multi stakeholders approach, because governments alone cannot secure cyberspace. We propose an approach which is based on dialog, partnership and empowerment, where broad participation via Public-Private-Partnership model stands for quality and impartiality.

Cyberspace interconnects industry sectors and crosses national borders which involve:

– Coordination of a national action on the part of government authorities, the private sector, and citizens/users. Adding to that, Academia (learned society: universities, institute, R&D, etc.) contribution is required for the prevention of, preparation for, response to, and recovery from incidents;

– Cooperation and coordination with regional & international partners are also needed.

2.2 NCSec Framework

NCSec supports National Cybersecurity governance by providing a framework to ensure that:

– NCSec is aligned with the national strategy;

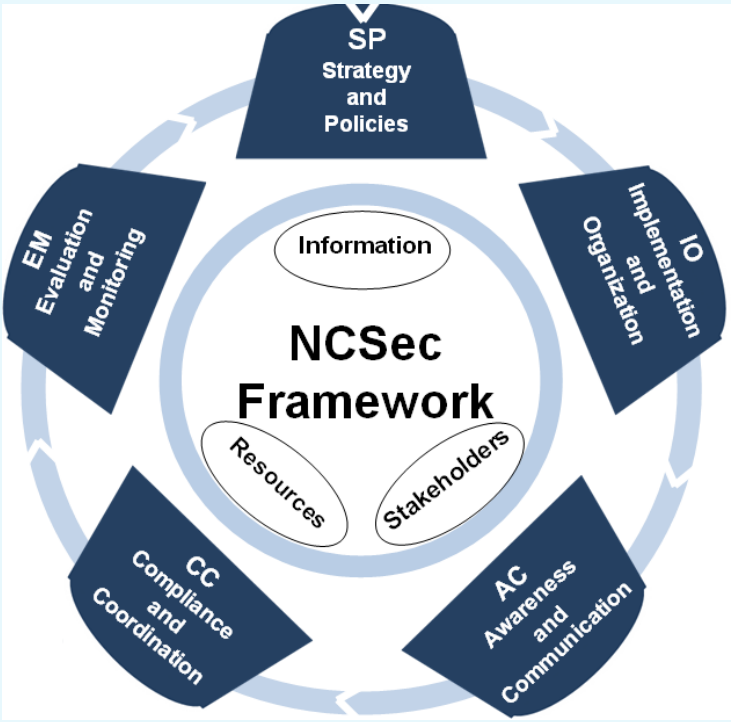
– NCSec organizational structure protects the national cyberspace with optimal costs;

– NCSec stakeholders use the cyberspace with responsibility;

– NCSec risks are managed appropriately, requiring risk awareness by all stakeholders. It also requires a clear understanding of compliance requirements, and embedding of risk management responsibilities into the organisation;

– NCSec performance measurement monitors strategy implementation, resource usage, and process performance. It is based on specific information measurement criteria, leading to achieve goals measurable beyond conventional accounting.

Figure 7: NCSec Framework model



This approach is deeply inspired from both ISO 27002 and Cobit (ISACA : IT Governance Institute): it consists in a generalization of the ISO 27002 standard at the National level, providing National Cybersecurity Management System through some key framework components. A best practice proposal for National Cybersecurity has already been defined (Debbagh and El Kettani 2008). It is a global Framework answering the needs expressed by the ITU in its Global Cybersecurity Agenda (GCA). "NCSecFR" is a code of practice for Organizational Structures and Policies on Cybersecurity at the national level, consisting in 5 domains and 34 processes, in order to help building regional and international cooperation for watch, warning, and incident response.

The NCSec Framework key components are:

– NCSec Governance Control Objectives / Focus Areas;

– NCSec Resources;

– NCSec Stakeholders;

– NCSec Information, based on the hierarchical threat classification.

The need for assurance about the national Cybersecurity, the management of Cybersecurity-related risks and increased requirements for control over information at the national level are now understood as key elements of national Cybersecurity governance. Information, Resources and Stakeholders constitute the core of National Cybersecurity Management System.

2.3 NCSec Framework : Five Domains

2.3.1 Domain 1: Strategy and Policies (SP)

This domain covers strategy, tactics and policies, which can best contribute to the achievement of the National Cybersecurity Governance. Furthermore, the realisation of the strategic vision needs to be

planned, communicated and managed for different perspectives. Finally, a proper lead institution as well as technological infrastructure risk management process should be identified.

This domain typically addresses the following questions:

– Is the National Cybersecurity Strategy defined?

– Is the government defining efficient national Cybersecurity policies?

– Did each stakeholder understand the NCSec objectives?

– How are the risk management processes understood and being integrated into the global framework, especially for CIIP?

– Is the degree of readiness of each stakeholder at the security level appropriate for implementing NCSec strategy?

2.3.2 Domain 2 : Implementation and Organisation (IO)

To realise the National Cybersecurity strategy, organizational structures need to be identified, created and should start working. These organizational structures should respect the global orientations of the national strategy. They must develop or acquire, as well as implement and integrate the policies of the national strategy. In addition, NCSec service delivery and support, management of National Cybersecurity, changes in and maintenance of existing policies are covered by this domain to make sure the NCSec framework continues to meet NCSec strategy.

This domain typically addresses the following management questions:

– Will the stakeholders meet properly the NCSec goals when implementing the NCSec strategy?

– Are NCSec services being delivered in line with NCSec strategy, for each sector/stakeholder?

– Are NCSec costs optimised?

– Are the stakeholders able to use the CyberSystems productively and safely?

– Are new stakeholders likely to deliver services that meet NCSec strategy?

– Are new stakeholders likely to apply NCSec policies on time and within budget?

2.3.3 Domain 3: Awareness and Communication (AC)

There is a need for understanding Cybersecurity in order to contribute in setting a “secure cyberspace”. Government should take a leadership role in bringing this “Culture of Cybersecurity” and in involving and supporting the efforts and contribution of all stakeholders.

This domain is concerned with the actual delivery of required NCSec services, which includes NCSec service support for stakeholders, and the NCSec operational facilities.

This domain typically addresses the following management questions:

– Are the national leaders in the government persuaded of the need for national action to address threats to and vulnerabilities?

– Is there any comprehensive awareness program promoted at the national level so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace?

– How are security awareness and communication programs and initiatives implemented for all stakeholders?

– Is there any support to civil society with special attention to the needs of children and individual users?

2.3.4 Domain 4: Compliance and Coordination (CC)

All NCSec processes need to be coordinated between stakeholders and involved organizational structures. They should also be assessed over time for their compliance with control requirements. This domain addresses NCSec regulatory compliance in order to provide governance. Continuity activity plans are covered by this domain to make sure the National Cybersecurity strategy continue to be levelled.

It typically addresses the following management questions:

– Do the organizational structures ensure that controls are effective and efficient?

– Are risk controls and compliance respected and reported?

– Are adequate confidentiality, integrity and availability in place among framework components?

2.3.5 Domain 5: Evaluation and Monitoring (EM)

All NCSec processes need to be regularly assessed over time for their quality. This domain addresses NCSec performance, monitoring of internal control among all stakeholders.

It typically addresses the following management questions:

– Is NCSec performance measured to detect problems before it is too late?

– Can NCSec performance be linked back to the strategic goals of the global NCSec framework?

– Are risk, control, compliance and performance measured and reported?

2.4 NCSec Framework : 34 Processes

The National Cybersecurity Framework (NCSecFR) consists in 34 processes divided into 5 domains, as follows:

2.4.1 Strategy and Policies Processes

Code	Process Description
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy
SP4	**Critical Information Infrastructures Protection** Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)
SP5	**Stakeholders** Identify the degree of readiness of each stakeholder regarding to the implementation of NCSec strategy & how stakeholders pursue the NCSec strategy & policies

2.4.2 Implementation and Organisation Processes

Code	Process Description
IO1	**NCSec Council** Define National Cybersecurity Council for coordination among all stakeholders, to approve the NCSec strategy
IO2	**NCSec Authority** Define Specific high level Authority for coordination among Cybersecurity stakeholders
IO3	**National CERT** Identify or establish a national CERT to prepare for, detect, respond to, and recover from national cyber incidents
IO4	**Privacy** Review existing privacy regime and update it to the on-line environment
IO5	**Laws** Ensure that a lawful framework is settled and regularly levelled
IO6	**Institutions** Identify institutions with Cybersecurity responsibilities, and procure resources that enable NCSec implementation
IO7	**National Experts and Policymakers** Identify the appropriate experts and policymakers within government, private sector and university
IO8	**Training** Identify training requirements and how to achieve them
IO9	**International Expertise** Identify international expert counterparts and foster international efforts to address Cybersecurity issues, including information sharing and assistance efforts
IO10	**Government** Implement a Cybersecurity plan for government-operated systems, that takes into account changes management, in line with NCSec strategy
IO11	**National Cybersecurity and Capacity** Manage National Cybersecurity and capacity at the national level, in line with NCSec strategy
IO12	**Continuous Service** Ensure continuous service within each stakeholder and among stakeholders, in line with NCSec strategy

2.4.3 Awareness and Communication Processes

Code	Process Description
AC1	**Leaders in the Government** Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the NCSec through policy-level discussions
AC2	**National Awareness & Communication** Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace. And ensure National Cybersecurity Communication

Code	Process Description
AC3	**Awareness Programs** Implement security awareness programs and initiatives for users of systems and networks
AC4	**Citizen and Child Protection** Support outreach to civil society with special attention to the needs of children individual users and persons with disabilities
AC5	**NCSec Culture for Business** Encourage the development of a culture of security in business enterprises
AC6	**Available Solutions** Develop awareness of cyber risks and available solutions

2.4.4 Compliance and Coordination Processes

Code	Process Description
CC1	**International Compliance & Cooperation** Consider regional and international recommendations in developing national regulations. Regional and international recommendations are voluntary. Whether or not to incorporate them into national regulations is a national matter. A regulator should be aware of relevant regional and international recommendations, but regulatory compliance with them is not required
CC2	**National Cooperation** Identify and establish mechanisms and arrangements for cooperation among government, private sector entities, university and ONGs at the national level, so that organizational structures ensure that controls are effective and efficient
CC3	**Private sector Cooperation** Encourage cooperation among groups from interdependent industries (through the identification of common threats) Encourage development of private sector groups from different critical infrastructure industries to address common security interest collaboratively with government (through the identification of problems and allocation of costs)
CC4	**Research and Development** Enhance Research and Development (R&D) activities (through the identification of opportunities and allocation of funds)
CC5	**Incidents Handling & Risk Controls** Manage incidents through national CERT to detect, respond to, and recover from national cyber incidents, through cooperative arrangement (especially between government and private sector), and respect, report risk controls
CC6	**Points of Contact** Establish points of contact (or CIRT) within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT, in order to monitor and evaluate NCSec performance in each sector

2.4.5 Evaluation and Monitoring Processes

Code	Process Description
EM1	**NCSec Observatory** Set up the National Observatory: It starts with the objective of systematically describing in detail the level of cybersecurity in the Information Society and generating specialised knowledge on the subject. It also makes recommendations and proposals defining valid trends for taking future decisions by stakeholders, especially the public powers. Within this plan of action are tasks of collecting information related to National Cybersecurity issue, that will measure and report national risk controls, compliance and performance, research, analysis, study, consultancy and dissemination
EM2	**NCSec Business Outcome Metrics for Evaluation** Define mechanisms that can be used to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance (how are we doing?)
EM3	**NCSec Assessment** Assess and periodically reassess the current state of Cybersecurity efforts and develop program priorities
EM4	**NCSec Internal Business Process Metrics** Define adequate NCSec management and technical metrics (for example confidentiality, integrity and availability) in place for each stakeholder, among framework components (what are we doing?)
EM5	**NCSec Governance** Provide National Cybersecurity Governance through the NCSecMM, especially with optimized costs and cybersystems productivity and safety

2.5 NCSec Framework Components

2.5.1 Stakeholders

NCSec stakeholders are:

– Government;

– Private Sector;

– Civil Society;

– Academia (Universities, R&D, etc.);

– Critical Infrastructure.

NCSec is a code of practice for Organizational Structures and Policies on Cybersecurity at the national level, consisting in 5 Domains and 34 processes, in order to help building regional and international cooperation for watch, warning, and incident response.

We can develop the composition of each stakeholder, in order to describe with more details the components that are involved in an NCSec process. We will present further the conditions that have to be fulfilled by each process, in order to satisfy one of the 5 levels of maturity, or to define the responsibility of each stakeholder above the National RACI chart.

For example, we have developed the involved components of the Government side:

– Government / Cabinet

– Head of Government

- National Cybersecurity Council
- Legislative Authority
- Authority in charge of ICTs
- Ministry of Interior
- Ministry of Defence
- Ministry of Finance
- Ministry of Education
- National Cybersecurity Authority
- National CERT

This approach is flexible, since we can do the same thing for the other stakeholders, by developing the components of another stakeholder whenever it is necessary.

This list will vary from country to country. Any country may have fewer or more components, or they may have different names.

2.5.1 Organizational Structures

At the time when the countries know a rapid expand in connection with digital economy, the stakes of national sovereignty and economic intelligence need a genuine strategy related to information systems security. National Cybersecurity governance is the responsibility of executives' structures, and consists in the leadership, organisational structures and processes that ensure that the national's NCSec sustains and extends the national strategies and objectives.

It is indeed duty of the State to strengthen its competences to protect the national heritage and the critical infrastructures which make it up [5]. Therefore, we propose with that aim the creation of an organization charged to enact the rules allowing the safeguarding of the National information systems.

The national resources identified in NCSec can be defined as follows:

- **National Cybersecurity Council (NCC):**

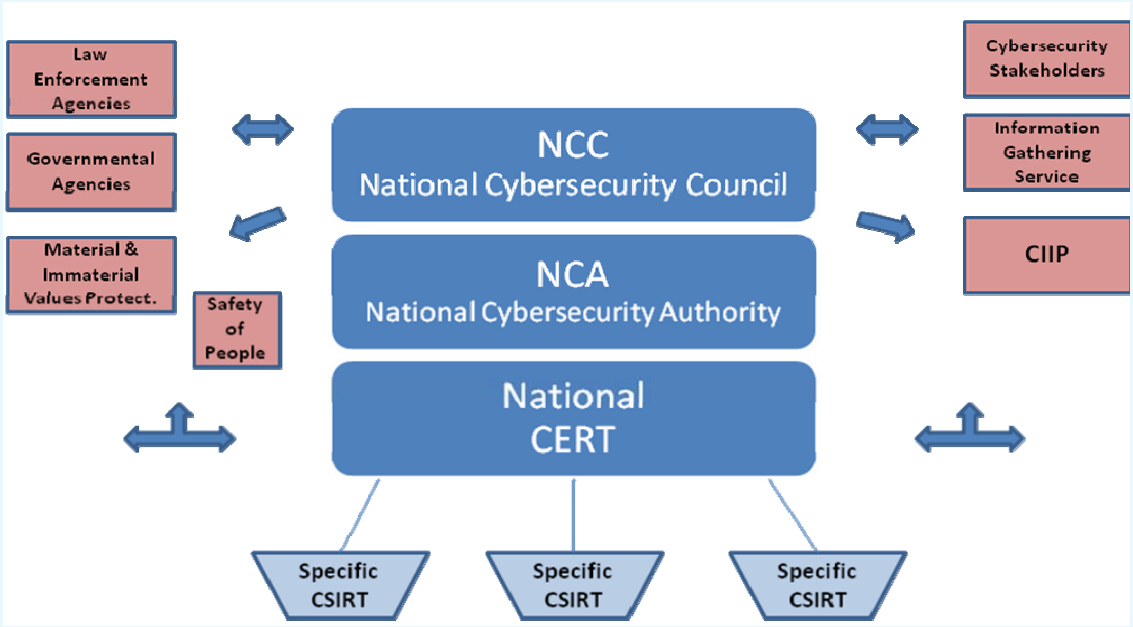
National Cybersecurity Council (NCC) will have the role of the protection of the information systems of the critical infrastructures of the country. In order to do this, the NCC will have to identify the whole companies and Administrations critical systems whose maintenance in operational condition is important. It will also enact the rules and requirements of safety to which these companies and administrations will have to meet.

For example, it involves the companies of the water or energy sector, Telecom companies, the emergency services, the bank and finance, transport, the food or of administrative services. The NCC will be also the coordinator organization of the various emergency plans and business continuity plans of these companies and Administrations.

- **National Cybersecurity Authority (NCA):**

The NCA has the role of checking of the NCC rules implementation in the administration and in the companies which compose the critical infrastructures of the country. With this intention, it may conduct any audit on its own initiative against these companies and administrations in order to ensure the compliance with these enacted rules.

Figure 8: NCSec Organizational Structure



Within the framework of monitoring the business continuity activities of the critical infrastructures, the NCA could be charged to organize various tests of the security emergency plans that already set up and to coordinate a whole security emergency plan. Thus, the whole test plan could be carried out at a frequency to be determined in order to ensure the dependences' good management between the services.

National CERT

A national CERT is an organisation which represents either a government's IT security infrastructure protection, or in some cases, a point of national co-ordination for IT security threats within a particular nation. Many countries opt for a non-nationalised CERT structure, focussing instead on providing a collaborative platform for incident handlers to share experience and knowledge, rather than a hierarchical structure.

The "CERT" will study computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.

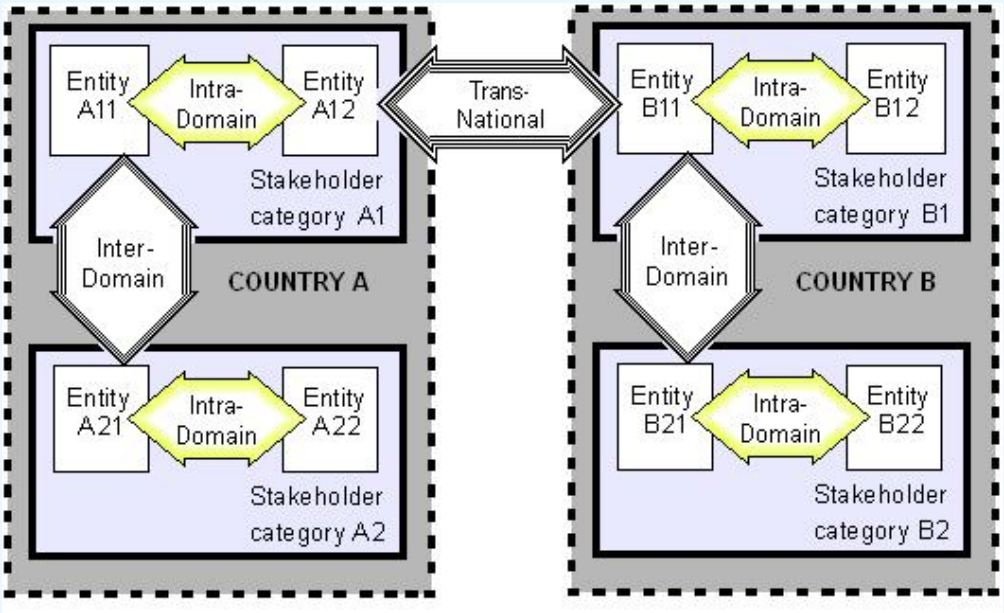
Organisations should satisfy the quality, fiduciary and security requirements for their information, as for all assets. To achieve its objectives, the organizational structures proposed may already exist in different countries, under perhaps others names. Each country has to define its own relevant structures, with specific assigned missions, functions and economic model to support them. Depending on the scale of the country, its specific organisation and functioning mode, several alternatives for organisational structures could be designed.

2.5.3 *Informations*

2.5.3.1 Hierarchical Threat Classification

The information model associated to NCSec depends on the kind of threat that is considered. The figure below shows the different levels of threat.

Figure 9: Hierarchical threat classification



We can distinguish 4 levels of threat:

– Internal (inside an organisation);

– Intra-Domain (between 2 organisations of the same stakeholder category);

– Inter-Domain (between 2 organisations from 2 different stakeholders in the same country);

– Transnational (between 2 organisations from 2 different countries).

2.5.3.2 NCSec Information criteria

To satisfy NCSec goals, information needs to conform to certain control criteria, which are defined as National Cybersecurity requirements. Based on the broader quality, fiduciary and security requirements, six distinct information criteria are combined with the 4 hierarchical levels of threats:

NCSec Framework Processes		Importance		Requirements							Levels of threat			
				Effectiveness	Confidentiality/ Secret	Integrity	Availability	Compliance	Reliability		Internal	Intra-Domain	Inter-Domain	Transnational
NCSec Strategy and Policies Processes														
SP1	NCSec Strategy	H		*		*	*	*	*		*	*		
SP2	Lead Institutions	M		*		*	*				*			*
SP3	NCSec Policies	M									*	*	*	
SP4	CIIP	H		*	*	*	*	*	*		*	*	*	*
SP5	Stakeholders	L		*			*		*		*	*		
NCSec Implementation and Organisation Processes														
IO1	NCSec Council	M		*				*	*				*	*
...	...													
IO12	Continuous Service	H		*		*	*	*	*		*	*	*	
Awareness and Communication Processes														
AC1	Leaders in the Gov.	M		*		*	*	*				*	*	*
...	...													
AC6	Available Solutions	H		*		*		*	*		*	*		
Compliance and Coordination Processes														
CC1	International Compl. & Coop.	H		*		*	*	*	*					*
...	...													
CC6	Points of Contact	L		*		*	*		*		*	*	*	*
Evaluation and Monitoring Processes														
EM1	National Observatory	M		*		*	*		*		*	*	*	
...	...													
EM5	NCSec Governance	H		*		*	*	*	*				*	*

NCSec information criteria have the following objectives:

– Effectiveness deals with information being relevant and pertinent to the NCSec process as well as being delivered in a timely, correct, consistent and usable manner;

– Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources:

– Confidentiality concerns the protection of sensitive information from unauthorised disclosure;

– Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with policies and expectations;

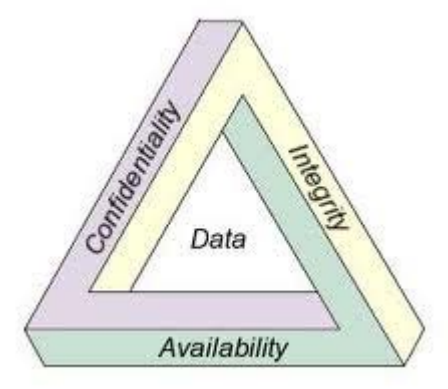
– Availability relates to information being available when required by the NCSec strategy and policies now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities;

– Compliance deals with complying with those laws, regulations and contractual arrangements to which the NCSec process is subject;

– Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

5.9.3.3 Confidentiality, Integrity and Availability

Figure 10: Confidentiality, integrity and availability



The important aspect of National Cybersecurity is to preserve the confidentiality, integrity and availability of a national's information. Loss of one or more of these attributes, can threaten the continuity of many Agencies and Organisations.

Confidentiality: Assurance the certain information are shared only among authorised organisations. The classification of the information should determine is confidentiality and hence the appropriate safeguards.

Integrity: Assurance that the information is authentic and complete. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it).

Availability: Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

2.5.3.4 Classification levels of Confidentiality

Classified information is sensitive information to which access is restricted by law or regulation to particular groups of persons. There are typically several levels of sensitivity, with differing clearance requirements. This sort of hierarchical system of secrecy is used by virtually every national government. The act of assigning the level of sensitivity to data is called data classification.

The purpose of classification is ostensibly to protect information from being used to damage or endanger national security. Classification formalises what constitutes a "state secret" and accords different levels of protection based on the expected damage the information might cause in the wrong hands.

Classification levels

Although the classification systems vary from country to country, most have levels corresponding to the following British definitions (from the highest level to lowest):

Top Secret (TS)

The highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if made publicly available.

Secret

Such material would cause "grave damage" to national security if it were publicly available.

Confidential

Such material would cause "damage" or be "prejudicial" to national security if publicly available.

Restricted

Such material would cause "undesirable effects" if publicly available. Some countries do not have such a classification.

Each country or region need to implement the specific strategy related to confidentiality of national information, by law or regulation. And it’s necessary to define the national authority for managing this issue.

3 NCSec Maturity Model

3.1 How the Maturity Model meets the needs

It is important for a country or a whole region to consider how well cyber-security is being managed. In response to this, a national cyber-security framework must be developed for improvement in order to reach the appropriate level of management and control. This approach gains cost-benefit balance in the long term, answering the following related questions:

– What is neighbour country peers doing, and how are we placed in relation to them?

– What can be considered as acceptable national cyber-security best practice, and how are we placed with regard to these practices?

– Can we be said to be doing enough, based upon these comparisons?

– How do we identify what is required to be done to reach an adequate level of management and control over our NCSec processes?

It can be difficult to supply meaningful answers to these questions, because there are actually few benchmarking initiatives and self-assessment tools in response to the need to know what to do in an efficient manner at the national level. But if we start from NCSec’s processes taken from the 5 high-level

control objectives, the process owner (stakeholder) should be able to incrementally benchmark against that control objective, affording to the following information:

– A relative measure of where the stakeholder is, in comparison with the NCSec strategy

– A manner to efficiently decide where to go

– A tool for measuring progress against the strategic goals

3.2 Maturity Model approach

3.2.1 COBIT Framework Maturity Model (source: ISACA – ITGI)

"Senior managers in corporate and public enterprises are increasingly asked to consider how well IT is being managed. In response to this, business cases require development for improvement and reaching the appropriate level of management and control over the information infrastructure. While few would argue that this is not a good thing, they need to consider the cost-benefit balance and these related questions:

– What are our industry peers doing, and how are we placed in relation to them?

– What is acceptable industry good practice, and how are we placed with regard to these practices?

– Based upon these comparisons, can we be said to be doing enough?

– How do we identify what is required to be done to reach an adequate level of management and control over our IT processes?

It can be difficult to supply meaningful answers to these questions. IT management is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner.

Starting from COBIT's processes, the process owner should be able to incrementally benchmark against that control objective. This responds to three needs:

1. A relative measure of where the enterprise is

2. A manner to efficiently decide where to go

3. A tool for measuring progress against the goal Maturity modelling for management and control over IT processes is based on a method of evaluating the organisation, so it can be rated from a maturity level of non-existent (0) to optimised (5).

This approach is derived from the maturity model that the Software Engineering Institute (SEI) defined for the maturity of software development capability. Although concepts of the SEI approach were followed, the COBIT implementation differs considerably from the original SEI, which was oriented toward software product engineering principles, organisations striving for excellence in these areas and formal appraisal of maturity levels so that software developers could be 'certified'.

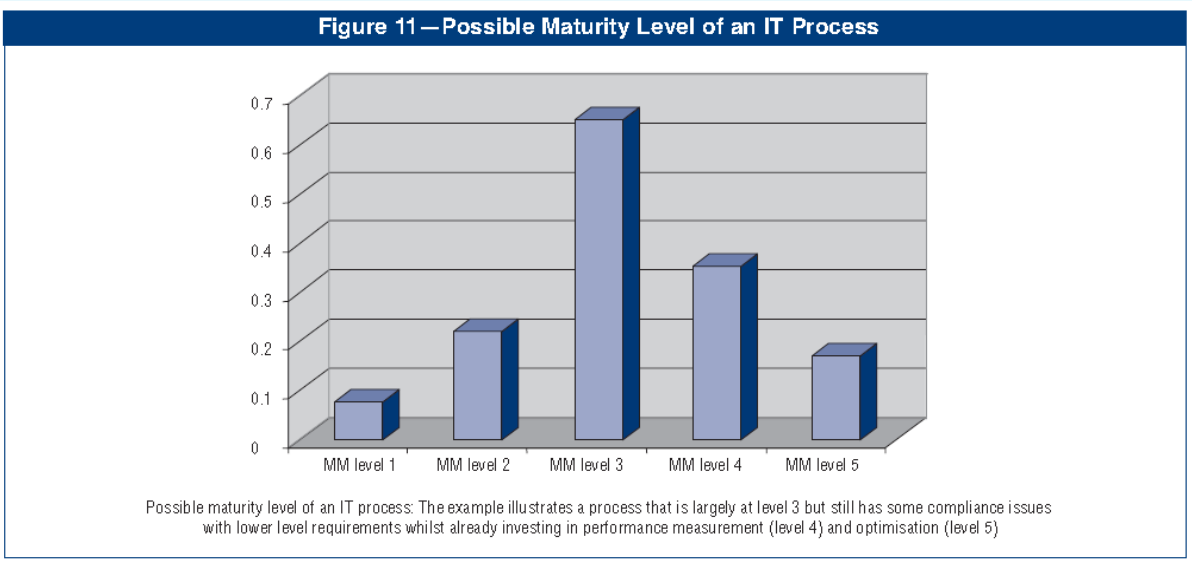
In COBIT, a generic definition is provided for the COBIT maturity scale, which is similar to CMM but interpreted for the nature of COBIT's IT management processes. A specific model is provided from this generic scale for each of COBIT's 34 processes.

Whatever the model, the scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable because, in general, the purpose is to identify where issues are and how to set priorities for improvements. The purpose is not to assess the level of adherence to the control objectives.

The maturity levels are designed as profiles of IT processes that an enterprise would recognise as descriptions of possible current and future states. They are not designed for use as a threshold model, where one cannot move to the next higher level without having fulfilled all conditions of the lower level.

With COBIT's maturity models, unlike the original SEI CMM approach, there is no intention to measure levels precisely or try to certify that a level has exactly been met. A COBIT maturity assessment is likely to result in a profile where conditions relevant to several maturity levels will be met, as shown in the example graph in figure 11.

Figure 11: Possible maturity level of an IT process

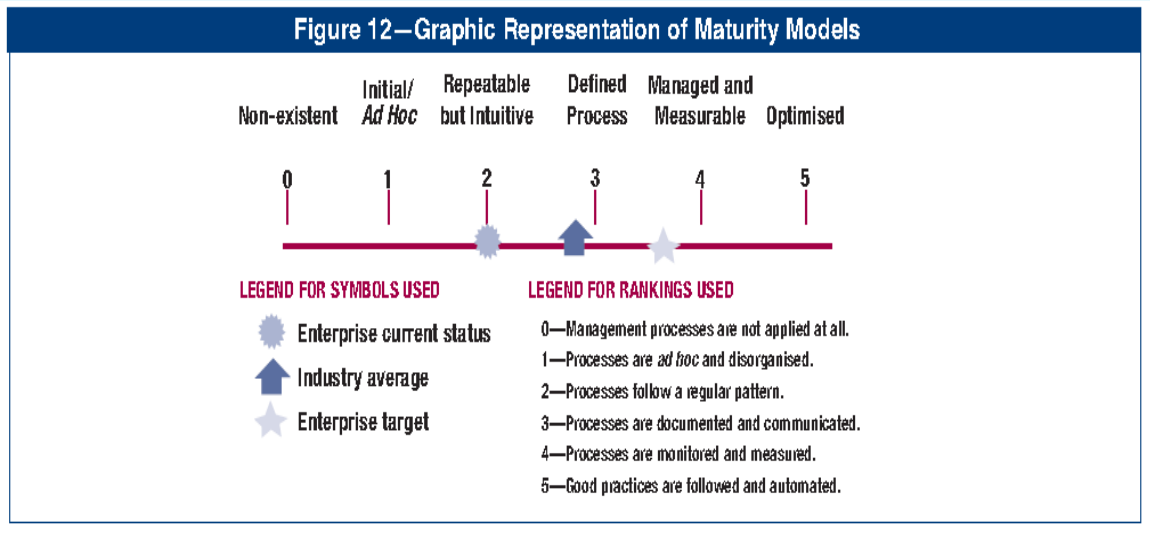


This is because when assessing maturity using COBIT's models, it will often be the case that some implementation will be in place at different levels even if it is not complete or sufficient. These strengths can be built on to further improve maturity. For example, some parts of the process can be well defined, and, even if it is incomplete, it would be misleading to say the process is not defined at all. Using the maturity models developed for each of COBIT's 34 IT processes, management can identify:

– The actual performance of the enterprise—Where the enterprise is today
– The current status of the industry—The comparison
– The enterprise's target for improvement—Where the enterprise wants to be
– The required growth path between 'as-is' and 'to-be'

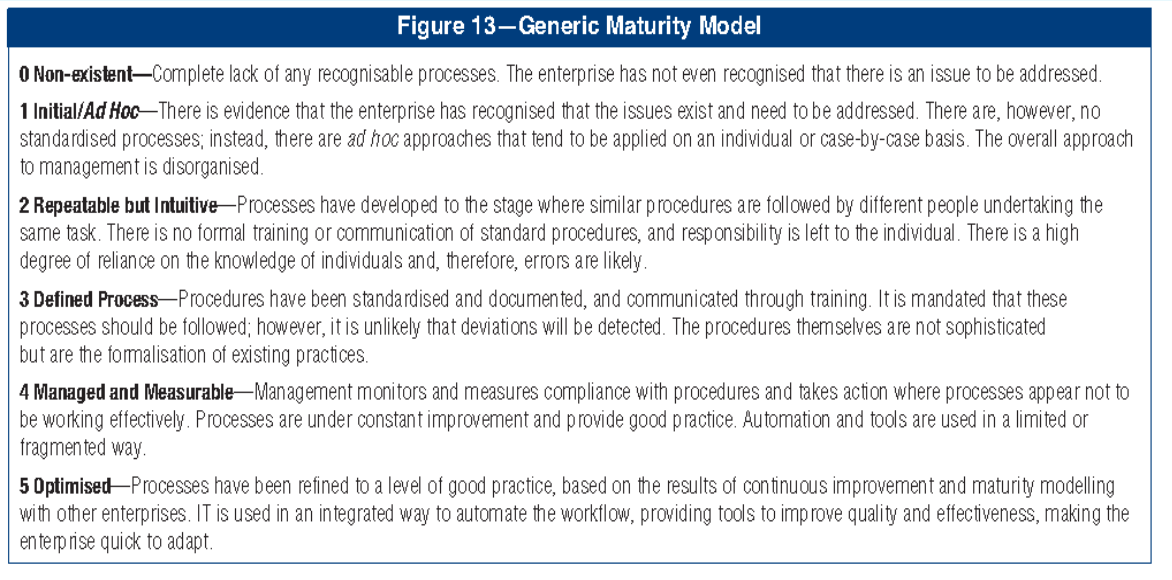
To make the results easily usable in management briefings, where they will be presented as a means to support the business case for future plans, a graphical presentation method needs to be provided (figure 12).

Figure 12: Graphic representation of maturity models



The development of the graphical representation was based on the generic maturity model descriptions shown in figure 13.

Figure 13: Generic Maturity Model



COBIT is a framework developed for IT process management with a strong focus on control. These scales need to be practical to apply and reasonably easy to understand. The topic of IT process management is inherently complex and subjective and, therefore, is best approached through facilitated assessments that raise awareness, capture broad consensus and motivate improvement. These assessments can be performed either against the maturity level descriptions as a whole or with more rigour against each of the individual statements of the descriptions. Either way, expertise in the enterprise's process under

review is required. The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed. The scale includes 0 because it is quite possible that no process exists at all. The 0-5 scale is based on a simple maturity scale showing how a process evolves from a non-existent capability to an optimised capability.

However, process management capability is not the same as process performance. The required capability, as determined by business and IT goals, may not need to be applied to the same level across the entire IT environment, e.g., not consistently or to only a limited number of systems or units. Performance measurement, as covered in the next paragraphs, is essential in determining what the enterprise's actual performance is for its IT processes. Although a properly applied capability already reduces risks, an enterprise still needs to analyse the controls necessary to ensure that risk is mitigated and value is obtained in line with the risk appetite and business objectives. These controls are guided by COBIT's control objectives.

The maturity model is a way of measuring how well developed management processes are, i.e., how capable they actually are. How well developed or capable they should be primarily depends on the IT goals and the underlying business needs they support. How much of that capability is actually deployed largely depends on the return an enterprise wants from the investment.

For example, there will be critical processes and systems that need more and tighter security management than others that are less critical. On the other hand, the degree and sophistication of controls that need to be applied in a process are more driven by the enterprise's risk appetite and applicable compliance requirements. The maturity model scales will help professionals explain to managers where IT process management shortcomings exist and set targets for where they need to be. The right maturity level will be influenced by the enterprise's business objectives, the operating environment and industry practices. Specifically, the level of management maturity will depend on the enterprise's dependence on IT, its technology sophistication and, most important, the value of its information.

A strategic reference point for an enterprise to improve management and control of IT processes can be found by looking at emerging international standards and best-in-class practices. The emerging practices of today may become the expected level of performance of tomorrow and, therefore, are useful for planning where an enterprise wants to be over time. The maturity models are built up starting from the generic qualitative model (see figure 13) to which principles from the following attributes are added in an increasing manner through the levels:

– Awareness and communication
– Policies, plans and procedures
– Tools and automation
– Skills and expertise
– Responsibility and accountability
– Goal setting and measurement.

3.2.2 Resolution Approach

NCSecMM consists in linking national cybersecurity strategy to strategic national goals, providing metrics and maturity model levels to measure their achievement, and to identify the associated responsibilities of stakeholders and control objective process. This approach is derived from the maturity model that the Software Engineering Institute defined for the maturity of software development capability.

As long as a global national framework for cyber-security is defined (NCSecFR), the National Cybersecurity Maturity Model, called « NCSec », is associated to this best practice proposal for National Cybersecurity. But we have to choose the level of granularity that will be associated to the proposed maturity model.

We can distinguish 3 levels of granularity:

– Level 1: High Level Control Objectives (associated to NCSec domains, such as SP, IC, AC, CC and EM);

– Level 2: Process (Each of the 34 processes has a High Level Control Objective);

– Level 3: Detailed Control Objectives (Each process has a number of detailed control objectives);

The scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable because, in general, the purpose is to identify where issues are and how to set priorities for improvements. The proposed maturity model is based on level 2 : We evaluate the national cyber-security, so that each of the 34 NCSec processes can be classified itself from a level of non-existent (0) to optimised (5). The scale includes 0 because it is quite possible that no process exists at all.

The proposed NCSecMM permits to determine what the country's maturity is. Setting thus a maturity target, and planning for maturity enhancement.

It contains the following levels:

0. Non existent: There is no recognition of the need for National Cybersecurity Framework, and there is a high risk of national control deficiencies and incidents.

1. Initial: The need for a NCSec Framework has been recognized. There are ad hoc approaches that might be applied on a case by case basis, instead of using standardized processes among the different stakeholders, whom are not aware of their responsibilities.

2. Repeatable but intuitive: Similar procedures are followed by different stakeholders undertaking the same task, and are very close to NCSec processes. There is no formal training or communication of standard procedures, and responsibility is left individually to each organization. Stakeholders might not be aware of their responsibilities, and errors are likely.

3. Defined process: Procedures have been standardised and documented in conformity with NCSec framework, and communicated through training. However, each stakeholder will decide whether to follow these processes or not. The procedures are not sophisticated: they formalize existing practices. Stakeholders are aware of their responsibilities.

4. Managed and measurable: compliance can be measured and monitored through standardized procedures. It is possible to take action where processes seem to work badly. Processes are under constant management and provide good practice. Automation and tools are used in a limited or fragmented way.

5. Optimized: As a consequence of continuous improvement and maturity modelling with other stakeholders (at the national level) and countries (at the transnational level), processes have been refined to the level of best practice. NCSec framework is used in an integrated way to automate the national strategy, providing tools to improve quality and effectiveness, making the whole country quick to adapt.

3.2.3 ISO 27001

In order to define the maturity levels of each process, ISO 27001 process approach will be followed. It enables an efficient process control, and a good comprehension of the interaction between these processes, and the inputs and outputs that "glue" these processes together. ISO 27001 suggests structuring every process using the "Plan-Do-Check-Act" (PDCA) model.

This means that, in order to reach maturity level 5, any NCSec process should be:

- Planned (PLAN)
- Implemented, operated, and maintained (DO)
- Monitored, measured, audited, and reviewed (CHECK)
- Improved (ACT)

PDCA model will be run in the NCSec Maturity Model in order to structure every aspect of NCSec Framework. Not only PDCA model will be used to structure every process, but it will also structure the maturity model itself. PDCA approach will be automatically used within the whole process of implementation of NCSec framework and maturity model.

3.2.4 Example

If we organize the processes through domains (corresponding to the 5 Domains of NCSec framework), each process should respect the PDCA approach, and thanks to this, the maturity of the process will be evaluated.

For example, let's consider the first process SP1 of the first domain: process SP1 is associated to the national Cybersecurity strategy, and consists in “Promulgating and endorsing a National Cybersecurity Strategy”.

Process SP1 is in conformance with level 5 if the following conditions are respected:

– the NCSec strategy is “announced and planned”, and

– the NCSec strategy is “operational”, and

– the NCSec strategy is under a “regular review”, and

– the NCSec strategy is under “continuous improvement”.

More precisely, in level 5, there is an integrated performance measurement system linking security performance to NCSec strategic goals by global application of the NCSec information criteria scorecard. Continuous improvement is a way of life.

3.3 Maturity Model by Process

We will present in this section the conditions that have to be fulfilled by each process, in order to satisfy one of the 5 levels of maturity.

3.3.1 Strategy and Policies Process

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy	Recognition of the need for a National Cybersecurity strategy	NCSec strategy is announced & planned.	NCSec strategy is operational for all key activities	NCSec strategy is under regular review	NCSec strategy is under continuous improvement, and has been refined to the level of best practice.
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category	Some institutions have an individual cyber-security strategy	Lead institutions are announced for all key activities	Lead institutions are operational for all key activities	Lead institutions are under regular review	Lead institutions in NCSec implementation are under continuous improvement.
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy	Ad hoc & isolated approaches to process, policies & practices	Similar & common processes are announced & planned	Process, policies and procedures are defined, documented, and operational & approved for all key activities. Standards are adopted.	Policies are under constant review and provide good practice, through measurement indicators. All aspects of the process & policies are repeatable.	Integrated policies & procedures: end-to-end improvement transnational best practices & standards are applied
SP4	**Critical Information Infrastructures** Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)	Recognition of the need for a process of risk management of CII.	The CII are identified and their protection planning. Risk management process is announced.	Risk management process is approved and operational for all CII.	CII Risk management is complete and process reproducibility. Good practices are used throughout the measurement indicators.	The process of risk management related to the CII evolved by incorporating best practices and enable continuous improvement

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
SP5	**Stakeholders** Identify the degree of readiness of each stakeholder regarding to NCSec strategy implementation & how stakeholders pursue the NCSec strategy & policies	Recognition of the need for the measurement of the degree of readiness of each stakeholder	Measurement process of the degree of readiness is announced & planned	Measurement process of the degree of readiness is operational for all key activities	The degree of readiness of each stakeholder is under regular review, and leads to good practice. It is measured through indicators.	continuous improvement of the measurement ps, and generalization to all stakeholder categories

3.3.2 Implementation and Organisation Process

Code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
IO1	**NCSec Council** Define National Cybersecurity Council for coordination between all stakeholders, to approve the NCSec strategy	Recognition of the need for a NCSec Council	NCSec Council is announced & planned	NCSec Council is operational, & approved NCSec strategy for all key activities	NCSec Council is monitored, audited & reviewed	NCSec Council is under continuous improvement
IO2	**NCSec Authority** Define Specific high level Authority for coordination among Cybersecurity stakeholders	Recognition of the need for a NCSec Authority	NCSec Authority is announced & planned	NCSec Authority is operational, & is coordinating between all key activities	NCSec Authority is monitored, audited & reviewed	NCSec Authority is under continuous improvement
IO3	**National CERT** Identify or establish a national CERT to prepare for, detect, respond to, and recover from national cyber incidents	Recognition of the need for a National CERT	CERT is announced & planned	National CERT is operational, & managing national cyber incidents between all key activities	National CERT is monitored, audited & reviewed	National CERT is under continuous improvement
IO4	**Privacy** Review existing privacy regime and update it to the on-line environment	Recognition of the need for a privacy regime	Privacy regime is announced & planned	Privacy regime is operational, between all key activities	Privacy regime is monitored, audited & reviewed	Privacy regime is updated & under continuous improvement

Code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
IO5	**Laws** Ensure that a lawful framework is settled and regularly levelled	Recognition of the need for a lawful framework	Lawful framework announced & planned	Lawful framework is implemented, operated, and maintained for all key activities	Lawful framework monitored, audited & reviewed	Lawful framework is under continuous improvement & regularly levelled
IO6	**Institutions** Identify institutions with Cybersecurity responsibilities, and procure resources that enable NCSec implementation	Ad hoc & isolated institutions have cyber-security responsibilities	Institutions with cyber-security responsibilities are announced, & resources are planned	Implement, operate & maintain NCSec in identified institutions in all key activities	NCSec implemen-tation is monitored, audited, measured & reviewed in identified institutions	NCSec Processes have evolved to automated workflows, which are under continuous improvement
IO7	**National Experts and Policymakers** Identify the appropriate experts and policymakers within government, private sector and university	Ad hoc & isolated experts and policy makers are identified without any coordination	Experts & policy makers are identified & announced within stake-holders	Appropriate experts & policymakers implement, operate & maintain NCSec in all key activities	Experts & policymakers audit, measure & review NCSec in identified institutions (PV, PB & University)	Experts & policymakers improve continuously NCSec in government, private sector & university
IO8	**Training** Identify training requirements and how to achieve them	Ad hoc & isolated training initiatives contributing to cyber-security in organiza-tional structures	Training needs are identified, announced, and planned for NCSec	Training sessions are organised, in all key activities in order to form appropriate qualified human resources	Training sessions are audited and review. Their impact on NCSec implementation is measured.	The content of training sessions is continuously improved in relation with NCSec new needs
IO9	**International Expertise** Identify international expert counterparts and foster international efforts to address Cybersecurity issues, including information sharing and assistance efforts	Ad hoc & isolated international experts and policy makers are identified without any coordination	International Experts are identified & announced by N-CERT, in coordination with sectorial-CERTs	Appropriate international experts address Cybersecurity issues, operate & maintain NCSec in all key activities	International Experts audit, measure & review NCSec in identified institutions (PV, PB & University)	International Experts propose continuous improvements regarding to NCSec in government, private sector & university

Code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
IO10	**Government** Implement a Cybersecurity plan for government-operated systems, that takes into account changes management, in line with NCSec strategy	Ad hoc & isolated change management measures are identified without any coordination	change management measures are identified announced and planned in the NCSec strategy	change management measures are operate, implemented & maintain in all key activities	Government operated systems are audited and reviewed from a change mgt viewpoint	change mgt measures are under continuous improvement
IO11	**National Cybersecurity and Capacity** Manage National Cybersecurity and capacity at the national level, in line with NCSec strategy	Each stakeholder assumes his responsibility, and is usually held accountable,even if this is not formally agreed. There is confusion about responsibility when problems occur and a culture of blame tends to exist.	Process responsibility and accountability are planned & defined. Process owners have been identified by NCA. The process owner is unlikely to have the full authority to exercise the responsibilities.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities, under the supervision of N-CERT. A reward culture is in place that motivates positive action.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the sectorial-CIRTs in a consistent fashion.	NCSec & capacity is improved at the national level, in coordination between NCA and N-CERT
IO12	**Continuous Service** Ensure continuous service within each stakeholder and among stakeholders, in line with NCSec strategy	Ad-hoc service is provided by some stakeholders	Stakeholders announce and plan continuous services	Continuous service is implemented in coordination with sectorial-CIRT	Service quality is measured & monitored by NCA	Service quality is improved, in coordination with N-CERT, and in respect to NCA guidelines

3.3.3 Awareness and Communication Process

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
AC1	**Leaders in the Government** Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the NCSec through policy-level discussions	Ad-hoc policy level discussions are initiated by some influential stakeholders	The National Cyber-security Council announces and plans policy-level discussion initiatives at the national level, corresponding to the National Strategy	The NCAuthority implements, operates & maintains discussions with all stakeholders, in all key activities	The National CERT monitors, measures, audits and reviews actions to address threats and vulnerabilities	NCC, in association with NCA & N-CERT, improves the Strategy & Policies, through official meetings, conferences &workshops
AC2	**National Communication** Promote a comprehensive national Cybersecurity communication program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace	Recognition of the need for the process is emerging. There is sporadic communication of the issues. Recognition of the development of communication between stakeholders	There is understanding of the full requirements for NCSec. NCA announces and plans a national communication programme	sectorial-CIRTs implement, operate and maintain communication strategy for each stakeholder, in coordination with N-CERT	National communication strategy is monitored by sectorial-CIRTs, and measured, audited and reviewed by N-CERT	National Communication Strategy is improved by N-CERT. Its efficiency is measured, audited and reviewed by the NCA
AC3	**Awareness Programs** Implement security awareness programs and initiatives for users of systems and networks	Ad-hoc security awareness programmes are implemented for users of systems and networks Recognition of the need for security awareness prg	There is understanding of the full requirements for awareness programme. N-CERT announces and plans an awareness program dedicated to users of systems & networks	local-CERTs implement, operates & maintain a specific awareness programs & initiatives, covering all stakeholders, in all key activities, in coordination with N-CERT	Security awareness programmes in use, are monitored by N-CERT. Its efficiency is measured, audited and reviewed by the NCA	The awareness programs in all key activities are improved, in relation with different stakeholders, based on audits.

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
AC4	**Citizens and Child Protection** Support outreach to civil society with special attention to the needs of children and individual users and persons with disabilities	Recognition of the need for security awareness programme dedicated to civil society, especially children & individual users	There is understanding of the full requirements for civil awareness programme. Specific citizen-CIRT announces and plans an awareness program	Citizen-CIRT implements, operates & maintains a specific awareness program & initiatives, in coordination with N-CERT	Awareness program in use, is monitored by Citizen-CIRT. Its efficiency is measured, audited and reviewed by the N-CERT	Awareness program is improved by N-CERT. Its efficiency is measured, audited and reviewed by the National Cybersecurity Authority (NCA)
AC5	**NCSec Culture for Business** Encourage the development of a culture of security in business enterprises	Recognition of the need for the NCSec culture in business enterprises. There is sporadic communication of the issues. There is awareness of the need to act at the business level.	There is understandingof the full requirements for NCSec culture at the national level.N-CERT in coordination with private sector CIRT announces and plans a national culture programme dedicated to business.	N-CERT, in coordination with local & sectorial CISRTs implements, operates & maintains a NCSec culture programme, covering all business enterprises, in all key business activities	Business NCSec culture programme is monitored by N-CERT. Its efficiency is measured, audited and reviewed by NCA	The business NCSec culture programme is improved in all activities with all business enterprises
AC6	**Available Solutions** Develop awareness of cyber risks and available solutions	Ad-hoc S&T activities are initiated by some stakeholders (Universities, etc.)	A national research programme is planned and settled. Potential researchers are identified.	National research program is implemented, in association with specific laboratories, research centres, and answering the NCSec strategy & policies	Research results are measured, monitored and audited.	The best research programs are renewed , and results are improved

3.3.4 Compliance and Coordination Process

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
CC1	**International Compliance & Cooperation** Ensure regulatory compliance with regional and international recommendations, standards	Ad-hoc compliance initiatives are initiated by some stakeholders	Compliance initiatives are planned by lead institutions among stakeholders	Compliance initiatives are implemented, operated & maintained by lead institutions among stakeholders	Compliance initiatives are monitored, measured, audited & measured by lead institutions among stakeholders	Compliance initiatives are under improvement by lead institutions among stakeholders, and have evolved to best practice
CC2	**National Cooperation** Identify and establish mechanisms and arrangements for cooperation among government, private sector entities, university and ONGs at the national level, so that organizational structures ensure that controls are effective and efficient	Ad-hoc mechanisms for cooperation are initiated by some stakeholders	Mechanisms for cooperation are planned by lead institutions among stakeholders	Mechanisms for cooperation are implemented, operated & maintained by lead institutions among stakeholders	Mechanisms for cooperation are monitored, measured, audited & measured by lead institutions among stakeholders	Mechanisms for cooperation are under improvement by lead institutions among stakeholders, and have evolved to best practice
CC3	**Private sector Cooperation** Encourage cooperation among groups from interdependent industries (through the identification of common threats) Encourage development of private sector groups from different critical infrastructure industries to address common security interest collaboratively with government	Ad-hoc private sector cooperation initiatives are initiated by some stakeholders belonging to private sector	Private sector cooperation initiatives are planned by some stakeholders belonging to private sector	Private sector cooperation initiatives are implemented, operated & maintained by some stakeholders belonging to private sector	Private sector cooperation initiatives are monitored, measured, audited & measured by some stakeholders belonging to private sector	Private sector cooperation initiatives are under improvement by some stakeholders belonging to private sector. They have evolved to best practice

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
CC4	**Research and Development** Enhance Research and Development (R&D) activities (through the identification of opportunities and allocation of funds)	Ad-hoc S&T activities are initiated by some stakeholders (Universities, etc.)	A national research programme is planned and settled. Potential researchers are identified.	National research program is implemented, in association with specific laboratories, research centers, and answering the NCSec strategy & policies	Research results are measured, monitored and audited.	The best research programs are renewed , and results are improved
CC5	**Incidents Handling & Risk Controls** Manage incidents through national CERT to detect, respond to, and recover from national cyber incidents, through cooperative arrangement and respect, report risk controls	Ad-hoc Incidents Handling & Risk Controls are managed by some stakeholders	Incidents Handling & Risk Controls management is planned by lead stakeholders	Incidents Handling & Risk Controls management is implemented, operated & maintained by stakeholders	Incidents Handling & Risk Controls management is monitored, measured, audited & measured by stakeholders	Incidents Handling & Risk Controls management is under improvement, and has evolved to best practice
CC6	**Points of Contact** Establish points of contact (or CIRT) within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT, in order to monitor and evaluate NCSec performance in each sector	Ad-hoc points of contact have been established within government, industry and university to facilitate consultation	Points of contact (or CIRT) have been planned within lead institutions for each stakeholder (government, industry and university) to facilitate consultation, cooperation and information exchange with national CERT	Points of contact (or CIRT) have been implemented, operated & maintained within each stakeholder (government, industry and university) to facilitate consultation, cooperation and information exchange with national CERT	Points of contact (or CIRT) are established within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT. They monitor, measure, audit and evaluate NCSec performance in each sector	Points of contact (or CIRT) are under improvement within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT. They have evolved to the level of best practice and improve NCSec performance in each sector

3.3.5 Evaluation and Monitoring Processes

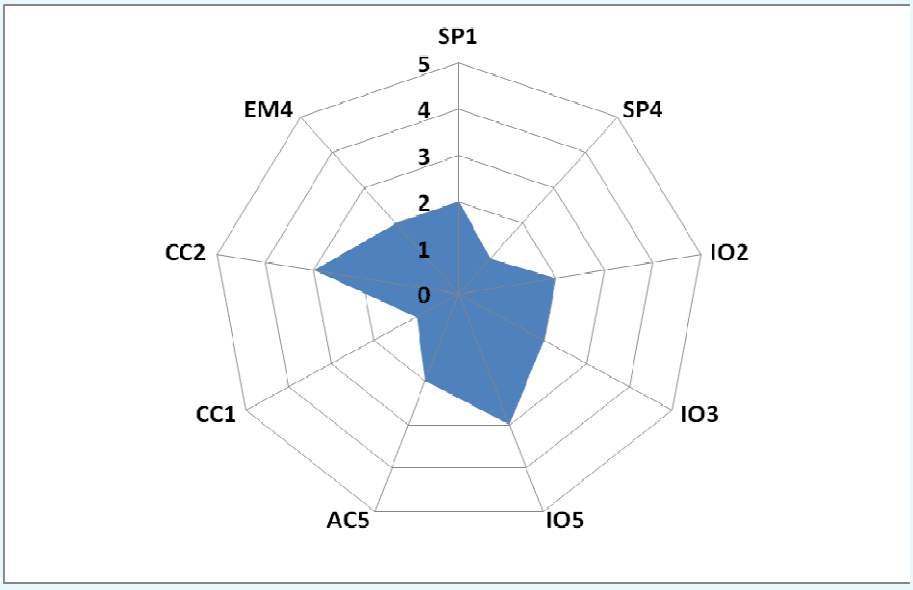
code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
EM1	**NCSec Observatory** Set up the National Observatory: It starts with the objective of systematically describing in detail the level of cybersecurity in the Information Society and generating specialised knowledge on the subject. It also makes recommendations and proposals defining valid trends for taking future decisions by stakeholders, especially the public powers. Within this plan of action are tasks of collecting information related to National Cybersecurity issue, that will measure and report national risk controls, compliance and performance, research, analysis, study, consultancy and dissemination	Goals are not clear and no measurement takes place, or Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.	Effectiveness goals and measures are identified and planned by NCA, and there is a clear link to NCSec strategic goals. These choices are communicated to N-CERT, who will be responsible for this task. Measurement processes emerge, but are not consistently applied.	Information criteria (Efficiency, effectiveness, etc.) are measured and communicated and linked to NCSec goals, by N-CERT, in coordination with sectorial-CERT. The NCSec balanced scorecard is implemented in all key activities and sectors, based on standardised best practice.	There is an integrated performance measurement system linking NCSec performance to National priorities, by global application of the IT balanced scorecard, in a global structure called NCSec observatory, settled by N-CERT.	Measurement process is under continuous improvement, in coordination with NCA. Results are communicated regularily to NCC.
EM2	**NCSec Business Outcome Metrics for Evaluation** Define mechanisms that can be used to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance (who are we doing?)	Ad-hoc NCSec Business Outcome Metrics are defined to coordinate the activities of the lead institution, the government, the private sector and civil society	NCSec Business Outcome Metrics are planned to coordinate the activities of the lead institution, the government, the private sector and civil society	NCSec Business Outcome Metrics are implemented, operated & maintained to coordinate the activities of the lead institution, the government, the private sector and civil society	NCSec Business Outcome Metrics are monitored, measured, & audited to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance	NCSec Business Outcome Metrics are under improvement to coordinate the activities of the lead institution, the government, the private sector and civil society. They have evolved to the level of best practice

code	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
EM3	**NCSec Assessment** Assess and periodically reassess the current state of Cybersecurity efforts and develop program priorities	Recognition of the need for the development of program priorities	NCA announces and plans a formal & structured roadmap for program priorities	N-CERTs, in coordination with NCA, implement, operate and maintain the program priorities defined by NCA	Program priorities are monitored by N-CERT, in coordination with NCA, and measured, audited and reviewed by NCC	National program priorities are improved by NCA. Its efficiency is measured, audited and reviewed by the NCC
EM4	**NCSec Internal Business Process Metrics** Define adequate NCSec management and technical metrics (for example confidentiality, integrity and availability) in place for each stakeholder, among framework components (what are we doing?).	Ad-hoc NCSec Internal Business Process Metrics (technical metrics) are defined for each some stakeholders	Ad-hoc NCSec Internal Business Process Metrics (technical metrics) are planned for each stakeholders	Ad-hoc NCSec Internal Business Process Metrics (technical metrics) are implemented, operated & maintained for each stakeholders	Ad-hoc NCSec Internal Business Process Metrics (technical metrics) are monitored, measured, & audited for each stakeholders	Ad-hoc NCSec Internal Business Process Metrics (technical metrics) are under improvement for each stakeholder. They have evolved to the level of best practice
EM5	**NCSec Governance** Provide National Cybersecurity Governance, especially with optimized costs and cybersystems productivity and safety	Each stakeholder assumes his governance, and is usually held accountable, even if this is not formally agreed.	NCA defines process responsibility and accountability are planned & defined among resources and stakeholders. Process owners have been identified by NCA. The process detailed control objectives are defined and the RACI chart is defined.	Process responsibility and accountability are accepted and working in a way respecting the RACI chart. A reward culture is in place that motivates positive action.	Process owners are empowered to make decisions and take action in respect to RACI chart. The acceptance of responsibility has been cascaded down throughout stakeholders' components in a consistent fashion.	NCSec & capacity is improved at the national level, in coordination between all stakeholders and resources (NCC, NCA and N-CERT)

3.3 Country Assessment

To assess the maturity level of a country to its National Cybersecurity Strategy, we propose to retain 10 major processes in order to conduct an inventory at any given time, as shown in the "radar" below, which will compare different countries and assess the evolution of a country between two dates.

Figure 14: "Radar" - Inventory of National Cybersecurity Strategy



Legend:

SP1: National Cybersecurity Strategy

SP4: Critical Information Infrastructures Protection

IO2: National Cybersecurity Authority

IO3: National-CERT

IO5: Cyber Laws

AC5: Awareness Programme

CC1: International Cooperation

CC2: National Coordination

EM4: Cybersecurity Governance

4 NCSec Roles and Responsabilities

Within a global need to settle National Cybersecurity Governance, the RACI chart should be associated to a global framework. This approach has already been used in COBIT, and has proved its efficiency (IT Governance Institute 2005): COBIT framework includes a certain number of components, such as the “framework”, the “domains”, the “processes”, the “maturity model” and the “RACI chart”. COBIT is dedicated to the organizational level, but it isn't applicable at the national level.

4.1 How the RACI Matrix meets the needs

We do need to follow an efficient methodology for identifying functional areas where there are ambiguities in terms of responsibilities, at the national level, bringing the differences out and resolving them through a cross-functional collaborative effort.

Responsibility Charting enables managers from the same or different organizational levels or programs to actively participate in a focused and systematic discussion about process related descriptions of the

actions. These actions must be accomplished in order to deliver a successful end product or service. But no “Responsibility Charting” models are dedicated to National Cybersecurity.

Responsibility Chart is a 5-Step Process (Smith and Erwin 2005): First, we have to identify processes. Second, the stakeholders, resources and information useful to chart should be determined. The RACI chart can then be developed, by completing the Chart Cells. Overlaps should be then resolved. At last, gaps should be also resolved. We will follow this methodology in order to build and produce the RACI chart table.

4.2 RACI chart approach

The RACI model is a relatively straightforward tool used to clarify roles, responsibilities, and authority among stakeholders involved in managing or performing processes; especially during organizational change process. It is useful to describe what should be done by whom to make a transformation process happen (Kelly 2006).

A RACI chart is a table that describes the roles and responsibilities of various stakeholders in operating a process. It is especially useful to help them managing more efficiently a function during the design or re-design of processes, by highlighting decisions. It also clarifies overlapping, redundant, “bottle-necked,” or inconsistent responsibilities. It makes it easier to structure and distribute responsibility and authority. It finally establishes clear lines of communication; reduces duplication of efforts. From a timing viewpoint, it is useful but not necessary to have identified stakeholders prior to applying RACI. But RACI can be applied anytime. If confusion impedes progress during the project implementation, RACI may point to the source of problems and to solutions.

Within the context of NCSec framework, “RACI Chart” will clarify roles and responsibilities of the different stakeholders, at the national level. For each of the 34 processes of NCSec framework, it will associate to the list of stakeholder’s information about roles they have in relation to those processes.

For each process, one or more letters taken from the acronym ‘RACI’ will be associated to each stakeholder, depending on his role(s) and responsibility. This acronym stands for:

– Responsible (R): Those who do work to achieve the process, including Support, which is to provide resources to complete the task in its implementation.

– Accountable (A): Those who are ultimately accountable to the correct completion of the task. It stands for the final approving authority. Accountable authority must approve work that Responsible authority provides before it is OK. There must be only one Accountable specified for each process.

– Consulted (C): Those whose opinions are sought, in a two-way communication. It stands for the authority that is asked for their input, and has information and/or capability necessary to complete the work.

– Informed (I): Those who are kept up-to-date on progress, under a one-way communication. It stands for the authority that must be told about the work, and notified of results, but needs not be consulted.

Very often the role specified as "Accountable" can be also specified "Responsible”. But it is generally recommended that each role for each process receives at most one of the participatory role types. If double participatory types appear in the RACI chart, it means that the roles have not yet been truly resolved. It is then necessary to clarify each role on each task.

4.3 NCSec RACI methodology

The chosen methodology in the case of NCSec RACI chart will not be that different of the classical one. It will consist in completing the Chart Cells, after having identified who has the (R), (A), (C), (I) for each process. As a general principle, every process should preferably have one and only one (R). Otherwise, a

gap occurs when a process exists with no (R), and an overlap occurs when multiple stakeholders have an (R) for a given process.

We will begin with the (A). Guidelines for designating roles are:

– Designate one point (role, position) of Accountability (A) for each process;

– Assign responsibility (R) at the level closest to the action or knowledge required for the task. Verify that any shared responsibilities are appropriate;

– Ensure that appropriate stakeholders are Consulted (C) and Informed (I), but limit these roles to necessary involvement only.

4.4 Example

Now, let's take for example the first process of the first domain SP (Strategy and Policies) of NCSec framework. If we use the RACI technique to identify responsibilities and role combination in Process SP1 ("Promulgate & endorse a National Cybersecurity Strategy"), we have the following distribution:

– The government is accountable (A), especially the National Cybersecurity Council (NCC), for the promulgation of the NCSec Strategy. It is also responsible (R) for the endorsement of the NCSec Strategy;

– At this level, Critical Infrastructure is consulted (C), because it has information and capability necessary to complete the promulgation of the NCSec Strategy, especially when it is under continuous improvement;

– Private sector is also consulted (C), because it has information and capability necessary to complete the promulgation of the NCSec Strategy;

– Civil Society and Academia remain Informed (I), because they are kept up-to-date on progress, under a one-way communication. They must be notified of results, but need not be consulted. The following table shows the RACI chart associated to process SP1.

4.5 RACI Matrix by Process

4.5.1 Strategy and Policies Process

code	Process Description	GovernMntCabinet	Head Of Gvt	Nat.Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Auth	Civil Soc	Trade union	PrivateSector	Academia	Crit. Infra	Nat.CERT	CSIRTs
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy	I	A	C	C	R	C	C	C	I	I	R		I	I		I		
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category	I	I	A	C	R	C	C	I	I		R		C	C	C	C		
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy			A	C	R	C	I	C	I		R			I		I		
SP4	**Critical Infrastructures** Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)			A		R	R	C	I			R				C	R	I	
SP5	**Stakeholders** Identify the degree of readiness of each stakeholder regarding to the implementation of NCSec strategy & how stakeholders pursue the NCSec strategy & policies			A		C	C	I	I			R	C	C	C	C	C	C	I

4.5.2 Implementation and Organisation Process

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat.Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Auth	Civil Soc	Trade union	Private Sector	Academia	Crit. Infra	Nat.CERT	CSIRTs
IO1	**NCSec Council** Define National Cybersecurity Council for coordination between all stakeholders, to approve the NCSec strategy	A	R		C	R	C	C	I	I									
IO2	**NCSec Authority** Define Specific high level Authority for coordination among Cybersecurity stakeholders	I	A	R		R	C	C	C	I									
IO3	**National CERT** Identify or establish a national CERT to prepare for, detect, respond to, and recover from national cyber incidents	I		A		R	C	C	I	I		R				C	C		
IO4	**Privacy** Review existing privacy regime and update it to the on-line environment	A		I	C	R	C		R			R		I	C	I	C	I	
IO5	**Laws** Ensure that a lawful framework is settled and regularly levelled	A		I	C	R	C		R			R			C	I	C	I	
IO6	**Institutions** Identify institutions with Cybersecurity responsibilities, and procure resources that enable NCSec implementation	I		A		R	C		I	R		R			C		C	I	I

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat.Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Auth	Civil Soc	Trade union	Private Sector	Academia	Crit. Infra	Nat.CERT	CSIRTs
IO7	**National Experts and Policymakers** Identify the appropriate experts and policymakers within government, private sector and university	I		I		R	I	I				A			R	R	I	C	C
IO8	**Training** Identify training requirements and how to achieve them					R	I				C	A	I	I	C	R	C	C	C
IO9	**International Expertise** Identify international expert counterparts and foster international efforts to address Cybersecurity issues, including information sharing and assistance efforts			I		C	I	I				A			I	R	C	R	C
IO10	**Government** Implement a Cybersecurity plan for government-operated systems, that takes into account changes management, in line with NCSec strategy			A	I	R	C	C		C		R			I	I	C	R	I
IO11	**National Cybersecurity and Capacity** Manage National Cybersecurity and capacity at the national level, in line with NCSec strategy	C		A	I	R	C	I		I		R			I	I	I	R	
IO12	**Continuous Service** Ensure continuous service within each stakeholder and among stakeholders, in line with NCSec strategy			I		C	I					A	C	I	C	C	C	R	

4.5.3 Awareness and Communication Process

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	NatCybsec Auth	Civil Soc	Trade union Syndicat	Private Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
AC1	**Leaders in the Government** Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the NCSec through policy-level discussions	C	A	I	I	R	C	I				R							
AC2	**NCSec Communication** Ensure National Cybersecurity Communication and …			A		C	I			I	R	R	I	I	C	R		R	R
	… National Awareness Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace			A	I	R	C			I	R	R	R	R	R	C		C	C
AC3	**Awareness Programs** Implement security awareness programs and initiatives for users of systems and networks			A	I	R	C			C	R	R		I	R	R	I	R	C
AC4	**Citizens and Child Protection** Support outreach to civil society with special attention to the needs of children and individual users and persons with disabilities			A		C					R	R	R			R		C	I

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	NatCybsec Auth	Civil Soc	Trade union Syndicat	Private Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
AC5	**NCSec Culture for Business** Encourage the development of a culture of security in business enterprises			I		C	I					A		C	R	C		R	R
AC6	**Available Solutions** Develop awareness of cyber risks and available solutions					C						A	I		I	R		R	R

4.5.4 Compliance and Coordination Process

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Aut	Civil Soc	Trade union Syndic	Private Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
CC1	**International Compliance & Cooperation** Ensure regulatory compliance with regional and international recommendations, standards	I		A		C	C	I				R			I	C		R	
CC2	**National Cooperation** Identify and establish mechanisms and arrangements for cooperation among government, private sector entities, university and ONGs at the national level, so that organizational structures ensure that controls are effective and efficient	C		A		R	I			I		R	C	I	C	C	I	R	
CC3	**Private sector Cooperation** Encourage cooperation among groups from interdependent industries (through the identification of common threats) Encourage development of private sector groups from different critical infrastructure industries to address common security interest collaboratively with government (through the identification of problems and allocation of costs)					C						A		I	R	C		R	R
CC4	**Research and Development** Enhance Research and Development (R&D) activities (through the identification of opportunities and allocation of funds)			I		R	I	I		R		A			C	R		C	I

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Aut	Civil Soc	Trade union Syndic	Private Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
CC5	**Incidents Handling & Risk Controls** Manage incidents through national CERT to detect, respond to, and recover from national cyber incidents, through cooperative arrangement (especially between government and private sector), and respect, report risk controls	C				R	I					A			R	C	C	R	R
CC6	**Points of Contact** Establish points of contact (or CIRT) within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT, in order to monitor and evaluate NCSec performance in each sector			I		C	I					A			R	R		R	C

4.5.5 Evaluation and Monitoring Process

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Aut	Civil Soc	Trade union Syndic	Privat E Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
EM1	**NCSec Observatory** Set up the National Observatory: It starts with the objective of systematically describing in detail the level of cybersecurity in the Information Society and generating specialised knowledge on the subject. It also makes recommendations and proposals defining valid trends for taking future decisions by stakeholders, especially the public powers. Within this plan of action are tasks of collecting information related to National Cybersecurity issue, that will measure and report national risk controls, compliance and performance, research, analysis, study, consultancy and dissemination			I		C	C	I		I	C	A	C		C	C	C	R	C
EM2	**NCSec Business Outcome Metrics for Evaluation** Define mechanisms that can be used to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance (who are we doing?)			A	I	C	C	I	C	I	C	R		I	C	I	C	C	

code	Process Description	Govern Mnt Cabinet	Head Of Gvt	Nat. Cyb Council	Legisl Auth	ICTs Authority	Min of Int	Min of Def	Min of Just	Min of Fin	Min of Edu	Nat Cybsec Aut	Civil Soc	Trade union Syndic	Privat E Sector	Academia	Crit.Infra	Nat.CERT	CSIRTs
EM3	**NCSec Assessment** Assess and periodically reassess the current state of Cybersecurity efforts and develop program priorities			A		C	C					R			I	C	C	R	
EM4	**NCSec Internal Business Process Metrics** Define adequate NCSec management and technical metrics (for example confidentiality, integrity and availability) in place for each stakeholder, among framework components (what are we doing?).			I		C	C	I		I	C	A			C	C	C	R	C
EM5	**NCSec Governance** Provide National Cybersecurity Governance, especially with optimized costs and cybersystems productivity and safety	I	I	A	I	R	C	I	C	I		R			I	I	I	C	I

5 NCSec Implementation Guide

5.1 How NCSecIG meets the need

The purpose of the implementation guide is to assist any/all stakeholders in the NCSec to implement a traceability system in line with the NCSec Framework, NCSec Maturity Model, and NCSec Responsibility charting.

Any/all stakeholders from the NCSec framework that want to implement a National Cybersecurity Governance traceability system, will use this this implementation guide, such as Government, Private Sector, Critical Infrastructure, Academia, and Civil Society.

The target audience of this guideline is any component of the previous stakeholders. In addition, this implementation guide can be used by Member States of ITU, to support the implementation efforts of their local stakholders, within a self-assessment process.

5.2 Resolution Approach

5.2.1 ISO 27003

ISO 27003 provides help and guidance in implementing an ISMS (Information Security Management System), including focus upon the PDCA method, with respect to establishing, implementing reviewing and improving the ISMS itself.

ISO committee SC27 will oversee the development, as with other information security standards. Its suggested title at the present time is: "Information technology - Security techniques. Information security management system implementation guidance".

The originally mooted broad table of contents is:

1. Introduction
2. Scope
3. Terms & Definitions
4. CSFs (Critical success factors)
5. Guidance on process approach
6. Guidance on using PDCA
7. Guidance on Plan Processes
8. Guidance on Do Processes
9. Guidance on Check Processes
10. Guidance on Act Processes
11. Inter-Organization Co-operation

5.2.2 ISO 27001

ISO IEC 27001 also uses a process approach. The process approach is a management strategy. When managers use a process approach, it means that they control their processes, the interaction between these processes, and the inputs and outputs that "glue" these processes together. It means that they manage by focusing on processes and on inputs and outputs. ISO IEC 27001 suggests that you use a process approach to manage and control your ISMS processes.

In general, a process uses resources to transform inputs into outputs. In every case, inputs are turned into outputs because some kind of work or activity is carried out. And because the output of one process often becomes the input of another process, inputs and outputs are really the same thing.

ISO IEC 27001 suggests that you structure every ISMS process using the Plan-Do-Check-Act (PDCA) model. This means that every process should be:

– Planned (PLAN)

– Implemented, operated, and maintained (DO)

– Monitored, measured, audited, and reviewed (CHECK)

– Improved (ACT).

The PDCA model runs through every aspect of the ISO IEC 27001 standard. The standard not only recommends that the PDCA model be used to structure every ISMS process, it was also used to structure the standard itself. And since it was used to structure the standard, you will automatically use a PDCA approach as you use the standard to develop your own ISMS.

5.2.3 Main Steps

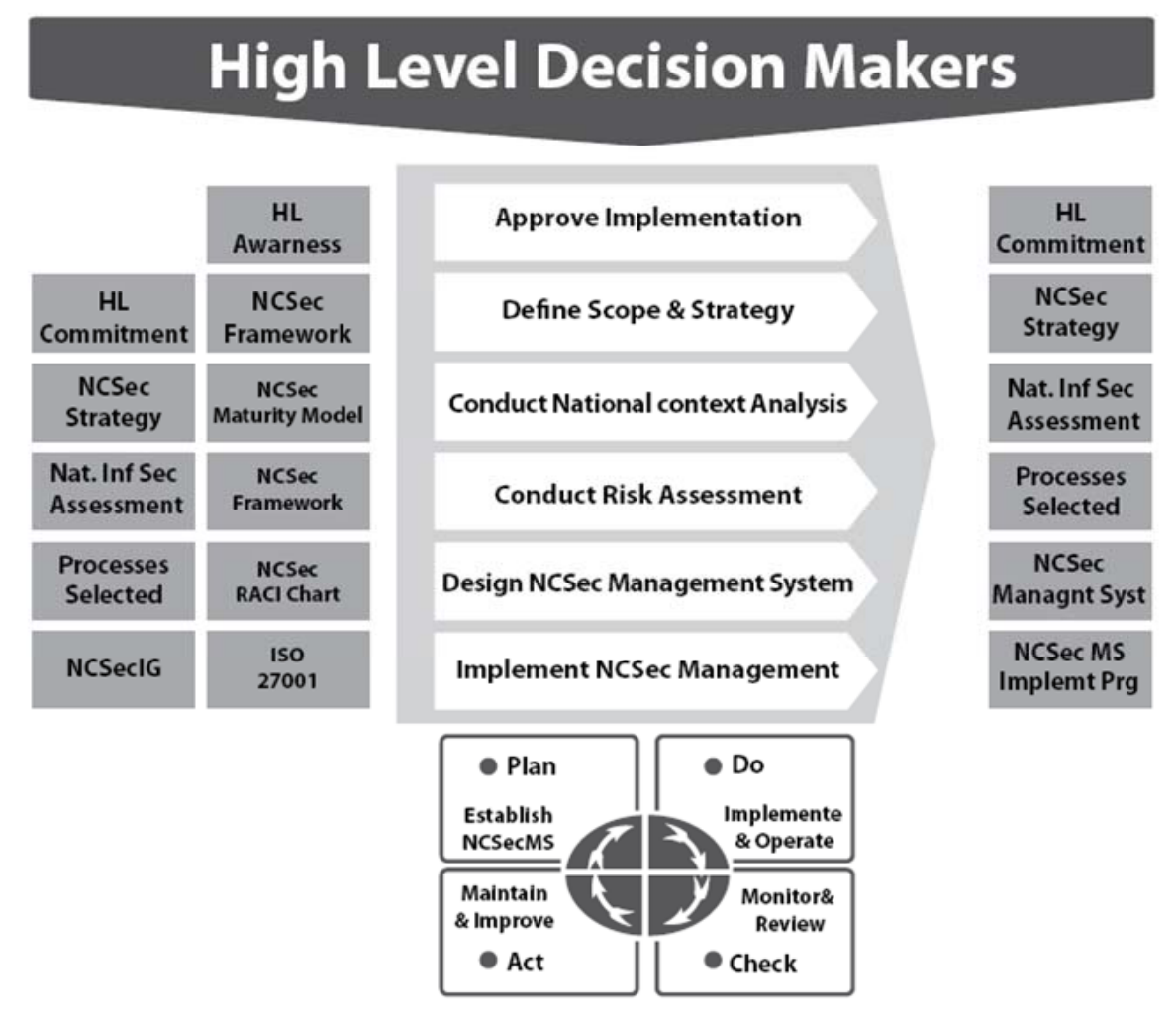
The implementation guide consists in six main steps, which are all based on the PDCA approach:

Figure 15: Implementation Guide Steps

5.2.4 Resolution Approach

The adopted resolution approach is inspired from the proposed National Cybersecurity Management System, called “NCSecMS” (Figure 2), and combined with its components. In fact, since the “NCSecMS” is a tool the goal of which is to facilitate the achievement of National Cybersecurity, the implementation guide will stick to its main principles, at both the national and regional levels.

Figure 16: NCSecIG resolution approach



5.3 Implementation Guide

5.3.1 Implementation Approval

A - Overview on approval for implementation

B - Define Objectives and National Requirements for Cybersecurity

At this level should be defined with the high level leaders of the country what are the objectives to be achieved through the establishment of NCSec Governance.

And the definition of these goals will require the analysis of Cybersecurity's needs for the country.

C - Define Initial NCSec Governance scope

This approach is to determine the initial scope to be covered by the NCSecMS, and especially to define the key components to be included but also those excluded, in order to clarify the directions to be taken by policy makers.

D - Obtain a high level Decision Makers approval

This step is crucial, because it present coverage of the NCSecMS scope to policymakers, in order to obtain their approval. This decision will be concurrent with the commitment of decision makers in the country to implement the NCSecMS which will be developed.

At the end of this stage, two documents will be produced:

– The Government High Level commitment

– The Mission Letter for responsible of the establishment of NCSec Management System.

5.3.2 Define scope and strategy

A - Overview on defining NCSecMS and strategy

B - Defining National Cyberspace boundaries

The head of the establishment of NCSecMS, must define the limits of national cyberspace, its development and its interactions with other countries. This cyberspace is divided into coverage areas, their nature as well as relevant stakeholders.

C - Completing boundaries for NCSecMS scope

From the initial scope, defined in the first phase, and analysis of national context of cyberspace, it is to detail the scope of NCSecMS.

This approach will be to define in detail both the inclusions and the exclusions, to avoid any ambiguity in the implementation of NCSecMS.

D - Developing the NCSec Strategy

After defining the scope to cover, and based on the NCSec Framework, the responsible must develop the strategy for implementation of MS NCSec to meet the objectives previously defined by the High Level Decisoin Makers of the country.

5.3.3 Conduct National context analysis

A - Overview on conducting National context analysis

B - Defining Information security requirements

Relying on the strategy for implementation of the components of the scope and NCSec Framework, it is clearly defined by what are the needs of information security for the country.

The list of needs will take into account the level of use of networks and information systems, and decide on priorities.

C - Defining Critical Information Infrastructure Protection (CIIP)

The information systems of critical infrastructure require attention, as they must be handled with priority. Disruptions of critical infrastructure can have very serious consequences throughout the country.

D - Generating an National Information Security Assessment

The main objective of the analysis of country context is to develop an assessment of the level of information protection at the national level. This assessment will be made from NCSec Maturity Model and give rise to a report detailing the strengths and weaknesses in information security and the maturity of key processes.

5.3.4 Conduct National Risk Assessment

A - Overview on conducting Risk Assessment

B - Risk Assessment description

On the basis of NCSec Framework and the National Information Security Assessment ", this step will develop descriptions of risk factors, mapping or associating them with types of risk, e.g. human factors, organizational and technological at the national level for a particular country..

C - Conducting Risk Assessment

The list of risks established beforehand, will be an evaluation which will be based on the likelihood and impact of each risk. And starting, tools of analysis it will be developed priorities of the risks would be covered, taking into account the severity of their impact.

D - Plan Risk treatment

The analysis and risk assessment will enable us to select the process NCSec Framework, which must be implemented to mitigate and monitor risks priorities.

5.3.5 Design NCSec Management System

A - Overview on designing the NCSecMS

B - Defining Organizational Structures

From the selected process and NCSec Roles & Responsibility (RACI Chart) will be to define the organizational structures that exist or to be put in place to support the implementation of key processes.

At this stage, it is also to identify critical infrastructure and key institutions that bear the NCSec strategy.

C - Designing the monitoring and measuring

At this stage managers describe all processes related to the implementation of NCSec Management System. It is also to define the set of indicators to measure changes in the establishment of NCSecMS.

D - Producing the NCSecMS implementation Program

After setting, organizational structures and processes related to implementation, it describes the program implementation.

This program will be divided into projects with an overall planning for implementation, and for each of them, the roles and responsibilities of stakeholders will be defined.

5.3.6 Implement NCSec Management System

A - Overview on implementing the NCSecMS

B - Setting up the implementation Management System

Before launching the program implementation of NCSecMS, we must implement the "Program Steering Committee" will ensure that governance and oversight of the entire program and will be assisted by a PMO (Project Management Office).

C - Carrying out implementation Projects

The Program Executive Committee will launch the various projects taking into account the priorities defined in advance. For each project, it is to define the "Project Steering Committee", the scope, deadlines and budgets. A mission letter will be submitted for each designated project manager. Project managers will be assisted by the PMO to implement their projects.

D - Documenting the procedures and Control

All components of NCSecMS will be reflected in a clear and accessible documentation. All procedures will be described, as well as performance indicators and monitoring

6 Conclusion

We have proposed a National Cybersecurity Management System applicable to Cybersecurity Governance at both national and regional levels.

Taking in consideration the boundless nature of cyberspace, this framework would build synergies between different actors at the National, Regional and Global levels to achieve stated goals.

Our approach is aligned with the objectives expressed by the ITU in the Global Cybersecurity Agenda (Section 7.1), and we used the HLEG work initiated by the Secretary General as a starting point.

This system will help a country or a whole region to determine how well Cybersecurity is being managed, through self-assessment based on a well-defined Maturity Model. The National Cybersecurity Management Framework would allow countries and regions to reach adequate levels of management and control through continuous improvement, taking in consideration cost benefits of short and long term objectives.

7 Additional resources

7.1 NCSec Framework Vs Global Cybersecurity Agenda Domains

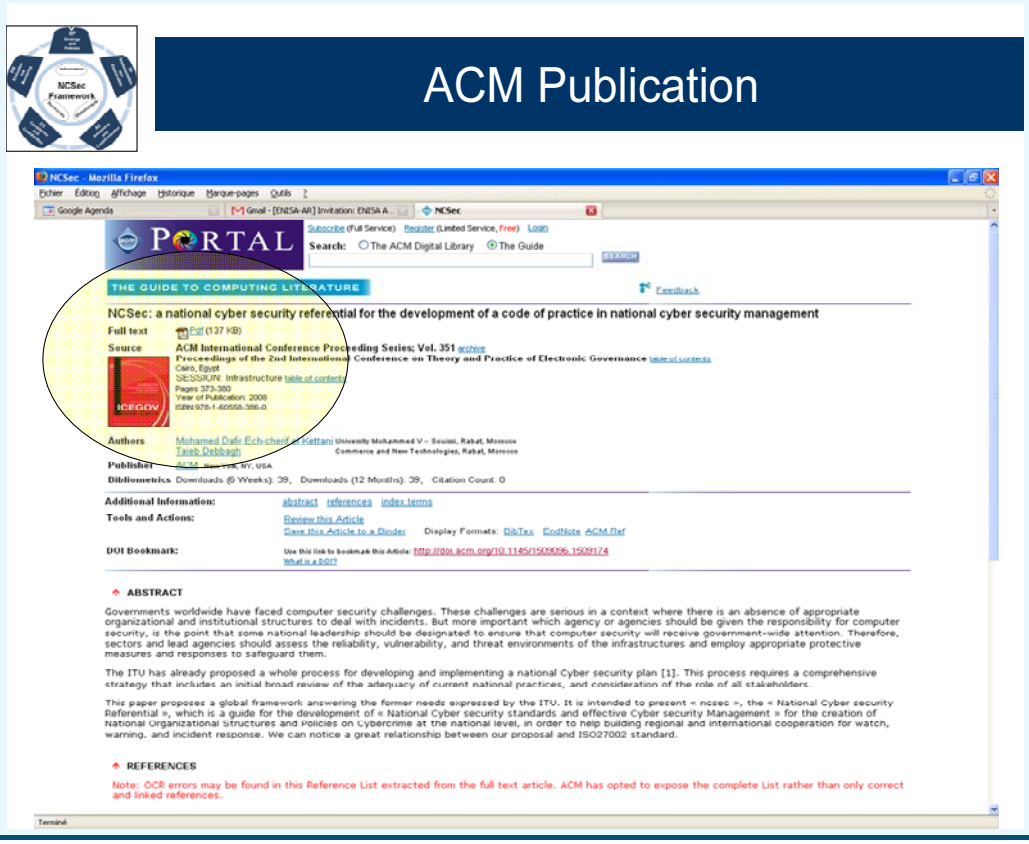
Proc	Strategy and Policies Processes	Legal	Technical	Org Structures	Capacity Building	Intern Coop
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy			X		
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category			X		
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy			X		
SP4	Critical Information Infrastructures Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)		X			
SP5	**Stakeholders** Identify the degree of readiness of each stakeholder regarding to the implementation of NCSec strategy & how stakeholders pursue the NCSec strategy & policies			X		

Proc	Implementation and Organization Processes	Legal	Technical	Org Structures	Capacity Building	Intern Coop
IO1	**NCSec Council** Define National Cybersecurity Council for coordination among all stakeholders, to approve the NCSec strategy			X		
IO2	**NCSec Authority** Define Specific high level Authority for coordination among cybersecurity stakeholders			X		
IO3	**National CERT** Identify or establish a national CERT to prepare for, detect, respond to & recover from national cyber incidents			X		
IO4	**Privacy** Review existing privacy regime and update it to the on-line environment	X				
IO5	**Laws** Ensure that a lawful framework is settled and regularly levelled	X				
IO6	**Institutions** Identify institutions with cybersecurity responsibilities, and procure resources that enable NCSec implementation			X		
IO7	**National Experts and Policymakers** Identify the appropriate experts and policymakers within government, private sector and university				X	
IO8	**Training** Identify training requirements and how to achieve them				X	
IO9	**International Expertise** Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts					X
IO10	**Government** Implement a cybersecurity plan for government-operated systems, that takes into account changes management, in line with NCSec strategy			X		
IO11	**National Cybersecurity and Capacity** Manage National Cybersecurity and capacity at the national level, in line with NCSec strategy			X		
IO12	**Continuous Service** Ensure continuous service within each stakeholder and among stakeholders, in line with NCSec strategy		X			

	Awareness and Communication Processes	Legal	Technical	Org Structures	Capacity Building	Intern Coop
AC1	**Leaders in the Government** Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the NCSec through policy-level discussions				X	
AC2	**National Communication** Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace. And ensure National Cybersecurity Communication				X	
AC3	**Awareness Programs** Implement security awareness programs and initiatives for users of systems and networks				X	
AC4	**Citizen and Child Protection** Support outreach to civil society with special attention to the needs of children and individual users and persons with disabilities				X	
AC5	**NCSec Culture for Business** Encourage the development of a culture of security in business enterprises				X	
AC6	**Available Solutions** Develop awareness of cyber risks and available solutions		X			
	Compliance and Coordination Processes	**Legal**	**Technical**	**Org Structures**	**Capacity Building**	**Intern Coop**
CC1	**International Compliance & Cooperation** Ensure regulatory compliance with regional and international recommendations, standards					X
CC2	**National Cooperation** Identify and establish mechanisms and arrangements for cooperation among government, private sector entities, university and ONGs at the national level, so that organizational structures ensure that controls are effective and efficient			X		
CC3	**Private sector Cooperation** Encourage cooperation among groups from interdependent industries (through the identification of common threats) Encourage development of private sector groups from different critical infrastructure industries to address common security interest collaboratively with government (through the identification of problems and allocation of costs)			X		
CC4	**Research and Development** Enhance Research and Development (R&D) activities (through the identification of opportunities and allocation of funds)				X	

	Compliance and Coordination Processes	Legal	Technical	Org Structures	Capacity Building	Intern Coop
CC5	**Incidents Handling & Risk Controls** Manage incidents through national CERT to detect, respond to, and recover from national cyber incidents, through cooperative arrangement (especially between government and private sector), and respect, report risk controls		X			
CC6	**Points of Contact** Establish points of contact (or CIRT) within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT, in order to monitor and evaluate NCSec performance in each sector			X		
	Evaluation and Monitoring Processes	**Legal**	**Technical**	**Org Structures**	**Capacity Building**	**Intern Coop**
EM1	**NCSec Observatory** Set up the NCSec observatory, that will measure and report NCSec risk controls, compliance and performance before it is too late			**X**		
EM2	**NCSec Business Outcome Metrics for Evaluation** Define mechanisms that can be used to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance (how are we doing?)		**X**			
EM3	**NCSec Assessment** Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities		**X**			
EM4	**NCSec Governance** Provide National Cybersecurity Governance, especially with optimized costs and cybersystems productivity and safety			**X**		
EM5	**NCSec Internal Business Process Metrics** Define adequate NCSec management and technical metrics (for example confidentiality, integrity and availability) in place for each stakeholder, among framework components (what are we doing?).		**X**			

7.2 ICEGOV 08 Cairo / 2nd International conference for theory and practice of Electronic Governance



7.3 ECEG 09 London / 9th European Conference on e-Government

ECEG 2009

9th European Conference on e-Government
Westminster Business School, University of Westminster, London, UK
29-30 June 2009

NCSecMM: A National Cyber Security Maturity Model for an Interoperable "National Cyber Security" Framework

Taïeb Debbagh, Mohamed Dafir Ech-Cherif El Kettani

Abstract: Security Maturity Model is a systematic approach that replaces traditional security metrics. There is more than one Security Maturity Model (SMM, COBIT, CERT/CSO, ISM3), and each of them has only five levels of maturity, providing the blueprint for a complete security program, telling management the order in which to implement security elements (ISM3 Consortium 2007), and leading toward the use of best practice standards (e.g., BS 17799). But very few of them are dedicated to National Cybersecurity.

We propose in this paper a "National CyberSecurity Maturity Model", that will make it possible to evaluate the security of a country or a whole region, making thus comparisons between them, and pointing out its forces and threats.

7.4 ECIW 09 Lisbon / 8th European Conference on Information Warfare and Security

ECIW 2009

8th European Conference on Information Warfare and Security
Military Academy, Lisbon & the University of Minho, Braga, Portugal.
6-7 July 2009

A National RACI Chart for an Interoperable "National Cyber Security" Framework

Taïeb Debbagh, Mohamed Dafir Ech-Cherif El Kettani

Abstract: Governments worldwide have faced serious Cyberterrorism threats, in a context where interoperability of "TransNational CyberSecurity Plans" is quite absent, in order to deal with incidents. It is important to know which agency or agencies should be given the responsibility for "National Cybersecurity", in order to ensure that computer security will receive government-wide attention. Therefore, sectors and lead agencies should assess the reliability, vulnerability, and threat environments of the infrastructures and employ appropriate protective measures and responses to safeguard them.

Responsibility Charting is a technique for identifying functional areas where there are process ambiguities, bringing the differences out, and resolving them through a cross-functional collaborative effort. We provide in this paper a "National RACI chart" that defines for each National Cyber Security process, who is "Responsible", "Accountable", "Consulted" and "Informed". The "RACI chart" defines in detail what has to be delegated and to whom, and what kind of responsibility will be affected to one stakeholder instead of another. Thus, it will aid organisations and teams identifying the responsibility for specific elements at the national level.

Acronyms

CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructures Protection
CISRT	Computer Information Security Response Team
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and related Technologies
GCA	Global Cybersecurity Agenda
HLEG	High Level Experts Group
NCSecFR	National Cybersecurity Framework
NCSecIG	National Cybersecurity Implementation Guide
NCSecMM	National Cybersecurity Maturity Model
NCSecMS	National Cybersecurity Management System
NCSecRR	National Cybersecurity Roles and Responsibilities
RACI	Responsible, Accountable, Consulted, Informed
PDCA	Plan, Do, Check, Act

Annex D: Best practices for Cybersecurity – Internet Service Provider (ISP) Network Protection Best Practices

Abstract

An industry working group in the United States addressed the area of Internet Service Provider (ISP) Network Protection, with a focus on addressing "bots" and "botnets", which are serious and growing problems for end-users and ISP networks. Botnets are formed by maliciously infecting end-user computers and other devices with bot[10] software through a variety of means, and surreptitiously controlling the devices remotely to transmit onto the Internet spam and other attacks (targeting both end-users and the network itself).

The working group examined potentially relevant existing Best Practices (BPs), and in consultation with industry and other experts in the field, identified additional Best Practices to address this growing problem.

The Working Group identified 24 Best Practices to address protection for end-users as well as the network. The Best Practices in this Annex, are organized into the logical steps required to address botnets. The first step is Prevention (12 BPs), followed by Detection (5 BPs), Notification (2 BPs), and then Mitigation (3 BPs). Finally, 2 BPs on Privacy Considerations were identified to address the handling of customer information in botnet response. The BPs identified are primarily for use by ISPs that provide service to consumer end-users on residential broadband networks but may apply to other end-users and networks as well.

Sector Members are encouraged to have their respective subject matter experts review these Best Practices for applicability. It is critical to note that Best Practices in general are not applicable in every situation because of multiple factors, and such a caveat applies to the work product of the Working Group. Therefore, the Best Practices set out below are intended to be voluntary in nature for ISPs, and may not apply in all contexts (and thus for a host of reasons should not be made mandatory). With this understanding, the Working Group recommends that the Best Practices be implemented by ISPs, where applicable, in order to address the growing botnet problem in consumer end-user devices and ISP networks.

[10] (from the word "robot")

1 Introduction

The most pressing area of the botnet problem lies in consumer-focused residential broadband networks. Although botnets are also a concern with business-focused networks and service, the business arrangements in that context are far more diverse than in the residential consumer market, and there is already more activity in the business context in response to botnets. The focus for this Report is thus on identifying Best Practices for ISPs that provide services to consumers on residential broadband networks.

Notwithstanding this focus, many of the Best Practices identified here would also be valuable practices to apply in non-consumer, non-residential network contexts. In light of the complexity and diversity of individual networks, and the fast-changing nature of the botnet security threats, individual networks should be able to respond to security threats in the manner most appropriate for their own network.

The Best Practices should not be viewed as an exhaustive list of all steps that ISPs could take to address botnets and compromised computers. Indeed, many service providers take additional steps in response to the botnet problem, and many are often assessing what new or additional techniques should be considered – beyond the foundational measures suggested below.

2 Objective, Scope, and Methodology

2.1 Objective

This report investigates current practices that ISPs use to protect their networks from harms caused by the logical connection of computer equipment, as well as desired practices and associated implementation obstacles. These efforts address techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem.

The report focuses on the relationship between ISPs and end users in the residential broadband context (the problem of botnet–compromised, end-user devices) and identifies Best Practices for ISPs that are effective in addressing end-user device compromise.

2.2 Scope

Security flaws in the hardware and/or software used by consumers coupled with poor or non-existent system administration practices by end-users have resulted in an epidemic of compromised computers, many of which can be remotely controlled as a part of what are frequently called ‘botnets.’ Once compromised, the owners of these computers are put at risk as their personal information and communications can be monitored.

As used here “computer equipment” includes a wide variety of personal equipment (e.g., servers, PCs, smart phones, home routers, etc.) as well as household devices with embedded IP network connectivity. “Logical connection” refers to end-user data communications protocol signaling and transmission. Harms result from the ability to degrade the communications infrastructure though malicious protocol exchanges and information transmission and their computing power and Internet access can be exploited by those controlling the botnet. Armies of these compromised computers can also be used together to disseminate spam, store and transfer illegal content, and to attack the servers of government and private entities with massive, distributed denial of service (DDoS) attacks.

This report investigates current practices that ISPs use to protect their networks from harms caused by the logical connection of computer equipment as well as desired practices and associated implementation obstacles. The work addresses techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem. The report proposes recommendations for best practices and actions that could be taken to help overcome implementation obstacles.

The following is a summary of findings from expert presentations and consultations:

– Botnet compromise of end-user devices is a significant problem that affects all ISPs - large and small.

– Botnet malware is rapidly proliferating into end-user devices.

– A rapid increase in botnet infections and technological sophistication appears to have been driven by the funding of botnet technology by sophisticated criminal elements.

– Botnet malware technology, infections, and the resulting impacts resulting from them are moving faster than ISP industry methods and technologies have, to date, been able to respond to.

– Botnets are a complex issue involving both end-user and network issues.

– ISP efforts to address botnets must include cooperation and information sharing among ISPs in order to fully address the problem.

– There are existing Best Practices (including some IETF RFCs) that address certain aspects of botnets (e.g., concerning responses to spam), but no comprehensive approach has been identified or widely implemented (at least in United States networks).

– Botnet detection methods raise issues of end-user privacy which need to be considered when developing approaches to the botnet problem.

– The problem of botnets in end-user devices can be substantially improved by implementation of these Best Practices, as applicable, by ISPs serving consumers on residential broadband networks.

2.3 Next Steps

This report sets a foundation for ISPs to address bots in end-user devices on residential broadband networks, helping to reduce the impact of botnet attacks on the network. Possible next steps in dealing with bots and botnets could be to widen the scope of this work to include attack vectors which exploit network vulnerabilities to propagate bots and provide for obfuscation of botnet Command and Control channels. Although this report touches on this area based on initial work in DNS, dynamic space, and spam, this work could be expanded to include improved protection from social engineering vulnerabilities, the infection of public web sites with bot-related Trojans and other malware, and further work on the network detection and isolation of bot Command and Control traffic.

As mentioned in the Recommendations section, these Best Practices should be reviewed frequently and updated to reflect the latest technology and methods in dealing with botnets. In addition, additional best practice work could be valuable in network-focused areas beyond the residential broadband networks that formed the focus of this Report.

2.4 Creation of New Best Practices

Best Practices have been categorized in terms of the logical steps required to address botnets. The Best Practice categories include Prevention, Detection, and Notification of end-users, Mitigation, and Privacy Considerations in detecting bots and notifying end-users. The Best Practices are included in this Annex.

2.4.1 Prevention Best Practices

The twelve Prevention Best Practices are aimed at preventing botnet infections in end-user devices and major impacts to ISP networks. For end-users, the main focus is on how ISPs can help residential broadband end-users prevent bot malware infections from occurring in their devices and networks. This is accomplished by identifying Best Practices for end-user awareness and education of the importance of good Internet hygiene, e.g., keeping operating systems and applications up to date, being aware of social engineering scams, etc., and the use of anti-virus software to aid in malware and bot detection. ISP personnel need to keep abreast of the latest botnet technology and malware in order to effectively

address botnet issues. Network prevention Best Practices address bot exploits of the Domain Name System, dynamic address space, and the prevention of bot-originated spam (which helps to spread bots and other malware and create network congestion.)

2.4.2 Detection Best Practices

The five Detection Best Practices are aimed at providing effective ISP bot detection capabilities and sharing information among ISPs. Because of the increasing sophistication of botnets and the rapidly changing technologies being utilized in botnets, maintaining effective detection methods and sharing of information are critical to addressing botnet deployments. Also, the need for utilizing non-interfering detection methods and timely execution are also addressed.

2.4.3 Notification Best Practices

Once a bot infection is detected, the end-user needs to be notified so that mitigation action can be taken. The two Notification Best Practices are aimed at maintaining effective notification methods and ensuring that critical service information is conveyed to end-users who likely have a bot infection on their device or network. It is suggested that a good balance be struck between the certainty of the detection and the speed of notification.

2.4.4 Mitigation Best Practices

Three Mitigation Best Practices are aimed at mitigating bots on end-user devices and the protection of end-users and the network from botnet attacks. Mitigation Best Practices address the need for the ISP to notify end-users by providing information on how to address a likely bot infection. Best Practices are also identified for ISP cooperation in the face of critical cyber incidents that can be caused by a botnet attack, as well as the potential need for the temporary isolation of actively attacking bots to reduce the possibility of adverse end-user or network impact (recognizing that such action should only be used as a "last resort" or in other critical circumstances, and that any use should be sensitive to the needs of the affected users).

2.4.5 Privacy Considerations Best Practices

Some of the Prevention, Detection, Notification, and Mitigation Best Practices raise the recurring issue of protecting end-user information. To address these concerns, the report offers two Best Practices focused on end-user privacy issues. The first deals with respecting consumers' privacy with regard to exposed customer information in addressing bot infections and attacks and the second suggests a multi-pronged strategy in designing technical measures that protect the privacy of customer information.

3 Analysis, Findings and Recommendations

3.1 Analysis

The report defines Best Practices in terms of the logical steps required to address botnets. Prevention Best Practices are those aimed at preventing botnet infections and the impact on ISP networks. Detection Best Practices are aimed at ISP detection of botnet infections and attacks. Notification Best Practices are targeted at notifying end-users of possible botnet infections. Mitigation Best Practices are aimed at mitigating end-user device botnet infections and the network impact.

3.2 Findings

Botnets represent a rapidly shifting malware landscape of infection, command and control, and attack capability fueled primarily by the desire for economic gains by those who develop and deploy these botnets – often sophisticated criminals. Weaknesses in end-user devices as well as a lack of understanding

and thus protective reactions by end-users themselves are largely responsible for the massive infections caused by sophisticated malware infection vectors.

Once infected with malware, botnets are formed when bot malware is activated on the infected device. The bot then establishes a connection with the botnet "command and control" system and then typically goes dormant to reduce the risk of detection while it awaits attack orders from the botnet owner. The level of sophistication has grown to the point where bots can often be updated with new versions of bot malware to add new attack capabilities and obfuscation techniques.

The botnet is comprised of all the infected bots under a common command and control. The bot malware itself is sometimes polymorphic, defying signature base detection at the device level. Use of sophisticated command and control mechanisms, including the use of peer-to-peer technology, makes bot and botnet detection challenging. Command and control mechanisms exploit weaknesses in the ISP and Internet infrastructure, e.g., DNS, to avoid detection of command and control traffic and to creatively provide infection vectors to spread the bot malware.

Once the end-user device becomes part of a botnet, threats exist to both the end-user and the ISP network. End-user personal information, such as identity, bank accounts, and credit card information, can be compromised; the ISP network can be exposed to denial of service attacks, spam, and other network related attacks.

To address these problems, the botnet lifecycle needs to be disrupted and mitigation of device bot malware needs to be addressed. This report looks at end-user and end-user device issues, and some key network weaknesses that support botnet proliferation and exacerbate the impact of botnets.

The problem of botnets may be substantially mitigated by implementation, as applicable, of the suggested Best Practices in the residential broadband context. By looking at botnets from the perspective of Prevention, Detection, Notification, and Mitigation, a comprehensive program can be established which should have a significant impact on botnets and their impact on end-users and ISP networks. Most botnet control strategies examined have some, but not all, elements of the Best Practices.

These findings support the contention that botnet technology and deployment have, to date, moved faster than ISP industry methods to address them. One common theme within the findings is that cooperation with the end-user and other ISPs is critical in effectively dealing with this issue. There are no silver bullets that can completely eradicate this problem. Rather a partnership with end-users and other ISPs is required to address botnets in a comprehensive way.

3.3 Recommendations

The report suggests that the rapid growth of botnets in end-user devices has been faster than the ability to effectively address the problem, hence significant work beyond the implementation of Best Practices is strongly encouraged. The following recommendations resulted from the research and Best Practice work of the Group:

– Because of the rapid growth of botnets and the rapidly changing technology, botnet Best Practices for ISPs should be revisited at least every two years.

– Standard methods for sharing information with end users and among ISPs should be better defined.

– Protection (and discarding) of customer information that may be collected by ISPs while addressing botnets is an important issue that warrants continued attention.

– ISP implementation of the botnet Best Practices should be benchmarked to get a better idea how ISPs are dealing with the botnet problem.

Additional possible policy actions are:

– The creation, perhaps with government funding, of an anti-botnet website available to end users to assist in the removal of botnet malware from their device, similar to the anti-botnet centers created in Germany (see http://botfrei.de) and Japan (see, https://www.ccc.go.jp/en_ccc/);

– The creation of a cybersecurity public information campaign that includes botnet awareness;

– The creation of a Computer Emergency Readiness Team (CERT) Information and Resource Center, available to ISPs and end users, devoted to botnet detection, mitigation, etc.; and

– Improvements in technology for network detection of botnet command and control and exploitation of traffic could be encouraged through research at government or other sites.

4 Conclusions

This report identifies 24 Best Practices to address bot-infected, end-user devices and the impact of botnets on end-users and ISP networks. These BPs form a foundation for addressing this growing problem and are for consideration by ISPs that provide service to consumers on residential broadband networks. Potential future work includes regularly reviewing these BPs to keep them up-to-date and to potentially expand the scope of future Best Practice work to identify Best Practices aimed at addressing the spread of bot malware through the network and detecting and disrupting botnet command and control traffic.

The new Best Practices are organized in areas of Prevention (12 BPs), Detection (5 BPs), Notification (2 BPs), and Mitigation (3 BPs). In addition, 2 BPs were identified in the area of Privacy Considerations concerning customer information in the context of addressing botnets.

It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, these Best Practices are intended to be voluntary for the ISPs. Mandating a particular set of practices could contribute to suboptimal network operation and reliability, or result in other negative consequences.

With these qualifications, this report recommends that the Best Practices set out in this Annex be implemented, as applicable, by ISPs in order to address the growing botnet problem in consumer end-user devices and ISP networks.

Introduction to Best Practices

These Best Practices are statements that describe guidance for the best approach to addressing a concern. They incorporate industry cooperation that engaged vast expertise and considerable resources. The implementation of Best Practices is intended to be voluntary. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area addressed by the Best Practice.

Mandated implementation of these Best Practices is not consistent with their intent. The appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often not apparent to those lacking this prerequisite knowledge and experience. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. For these reasons, this report does not recommend here that government authorities impose these best practices on industry, e.g. by regulations.

Prevention Best Practices

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

A.1 BP Number: Prevention 1

Stay Informed about Botnet/Malware Techniques:

ISPs should stay informed about the latest botnet/malware techniques so as to be prepared to detect and prevent them.[11]

A.2 BP Number: Prevention 2

ISP Provision of Educational Resources for Computer Hygiene / Safe Computing:

ISPs should provide or support third-party tutorial, educational, and self-help resources for their customers to educate them on the importance of safe computing and help them develop safe practices safe computing.[12] ISPs' users should know to protect end user devices and networks from unauthorized access through various methods, including, but not limited to:

– Use legitimate security software that protects against viruses and spywares;

– Ensure that any software downloads or purchases are from a legitimate source;

– Use firewalls;

– Configure computer to download critical updates to both the operating system and installed applications automatically;

– Scan computer regularly for spyware and other potentially unwanted software;

– Keep all applications, application plug-ins, and operating system software current and updated and use their security features;

– Exercise caution when opening e-mail attachments;

– Be careful when downloading programs and viewing Web pages;

– Use instant messaging wisely;

– Use social networking sites safely;

– Use strong passwords;

– Never share passwords.

---

[11] BP Prevention 1: References/Comments: See the following document for more information: www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf

More information can also be found at: isc.sans.edu/index.html

www.us-cert.gov/

www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

[12] BP Prevention 2: References/Comments: More information can be found at:

National Cybersecurity Alliance - www.staysafeonline.org/

OnGuard Online -www.onguardonline.gov/default.aspx

Department of Homeland Security - StopBadware – www.stopbadware.org/home/badware_prevent

Comcast.net Security - security.comcast.net/

Verizon Safety & Security - www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_safety

Qwest Incredible Internet Security site: www.incredibleinternet.com/

Microsoft - www.microsoft.com/security/pypc.aspx

A.3 BP Number: Prevention 3

ISP Provision of Anti-Virus/Security Software:

ISPs should make available anti-virus/security software and/or services for its end-users.[13] If the ISP does not provide the software/service directly, it should provide links to other software/services through its safe computing educational resources.

A.4 BP Number: Prevention 4

Protect DNS Servers:

ISPs should protect their DNS servers from DNS spoofing attacks and take steps to ensure that compromised customer systems cannot emit spoofed traffic (and thereby participate in DNS amplification attacks). [14] Defensive measures include:

– managing DNS traffic consistent with industry accepted procedures;
– where feasible, limiting access to recursive DNS resolvers to authorized users;
– blocking spoofed DNS query traffic at the border of their networks, and
– routinely validating the technical configuration of DNS servers by, for example,
– utilizing available testing tools that verify proper DNS server technical configuration.

A.5 BP Number: Prevention 5

Utilize DNSSEC

ISPs should use Domain Name System (DNS) Security Extensions (DNSSEC) to protect the DNS.[15] ISPs should consider, at a minimum, the following:

sign and regularly test the validity of their own DNS zones,

routinely validate the DNSSEC signatures of other zones;

employ automated methods to routinely test DNSSEC-signed zones for DNSSEC signature validity.

---

[13] BP Prevention 3: References/Comments: None

[14] BP Prevention 4: References/Comments:

Widely accepted DNS traffic management procedures are discussed in the following document:

www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_201006.pdf

Security issues on recursive resolvers are discussed in IETF BCP 140/ RFC 5358. Responses to spoofed traffic, including spoofed DNS traffic, are discussed in IETF BCP 38/RFC 2827.

Some tools examining different aspects of DNS server security include:

dnscheck.iis.se/

recursive.iana.org/

www.dnsoarc.net/oarc/services/dnsentropy

www.iana.org/reports/2008/cross-pollination-faq.html

[15] BP Prevention 5: References/Comments: More information can be found at:

www.dnssec.net

www.dnssec-deployment.org

A.6 BP Number: Prevention 6

Encourage Use of Authenticated SMTP/Restrict Outbound Connections to Port 25

ISPs should encourage users to submit email via authenticated SMTP on port 587, requiring Transport Layer Security (TLS) or other appropriate methods to protect the username and password.[16] In addition, ISPs should restrict or otherwise control inbound and outbound connections from the network to port 25 (SMTP) of any other network, either uniformly or on a case by case basis, e.g., to authorized email servers.

A.7 BP Number: Prevention 7

Authentication of Email:

ISPs should authenticate all outbound email using DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF).[17] Authentication should be checked on inbound emails; DKIM signatures should be validated and SPF policies verified.

A.8 BP Number: Prevention 8

Immediately Reject Undeliverable Email:

ISPs should configure their gateway mail servers to immediately reject undeliverable email, rather than accepting it and generating non-delivery notices (NDNs) later, in order to avoid sending NDNs to forged addresses.[18]

A.9 BP Number: Prevention 9

Blocking e-mail from Dynamic Space:

ISPs should not accept e-mail that originates from mail servers in dynamically-assigned IP address blocks, and should consider using one of the available services that identify such blocks. [19]

---

[16] BP Prevention 6: References/Comments: See the following document for more information: www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

[17] BP Prevention 7: References/Comments: See the following document for more information: www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_200807.pdf

More information can be found at: www.dkim.org/

www.openspf.org

[18] BP Prevention 8: References/Comments: By rejecting undeliverable email, the gateway mail will inform the sending mail server, which can apply local policy regarding whether or not to notify the message sender of the non-delivery of the original message. See the following document for more information:

www.maawg.org/sites/maawg/files/news/MAAWG-BIAC_Expansion0707.pdf

[19] BP Prevention 9: References/Comments: None

A.10 BP Number: Prevention 10

Share Dynamic Address Space Information:

ISPs should share lists of their dynamic IP addresses with operators of DNS Block Lists (DNSBLs) and other similar tools. Further, such lists should be made generally available, such as via a public website.[20]

A.11 BP Number: Prevention 11

Make Dynamic IPv4 Space Easily Identifiable by Reverse DNS Pattern:

ISPs should make IPv4 dynamic address space under their control easily identifiable by reverse DNS pattern, preferably by a right-anchor string with a suffix pattern chosen so that one may say that all reverse DNS records ending in <*.some.text.example.com> are those that identify dynamic space.[21]

A.12 BP Number: Prevention 12

Make Dynamic Address Space Easily Identifiable by WHOIS:

ISPs should make all dynamic address space under their control easily identifiable by WHOIS or RWHOIS lookup.[22]

Detection Best Practices

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

---

[20] BP Prevention 10: References/Comments: More information can be found at:

www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf

www.spamhaus.org/pbl/

www.mail-abuse.com/nominats_dul.html

[21] BP Prevention 11: References/Comments: Refer to related Best Practice Prevention 5.

[22] BP Prevention 12: Reference/Comments: See the following document for more information:

www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf

Refer to related Best Practice Prevention 4.

A.13 BP Number: Detection 1

Communicate Implementation of Situational Awareness and Protective Measures with other ISPs:

ISPs should make reasonable efforts to communicate with other operators and security software providers, by sending and/or receiving abuse reports via manual or automated methods.[23] These efforts could include information such as implementation of "protective measures" such as reporting abuse (e.g., spam) via feedback loops (FBLs) using standard message formats such as Abuse Reporting Format (ARF). Where feasible, ISPs should engage in efforts with other industry participants and other members of the internet ecosystem toward the goal of implementing more robust, standardized information sharing in the area of botnet detection between private sector providers.

A.14 BP Number: Detection 2

Maintain Methods to Detect Bot/Malware Infection:

ISPs should maintain methods to detect likely malware infection of customer equipment. Detection methods will vary widely due to a range of factors.[24] Detection methods, tools, and processes may include but are not limited to: external feedback, observation of network conditions and traffic such as bandwidth and/or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of customers on a more detailed level.

A.15 BP Number: Detection 3

Use Tiered Bot Detection Approach:

ISPs should use a tiered approach to botnet detection that first applies behavioral characteristics of user traffic (cast a wide net), and then applies more granular techniques (e.g., signature detection) to traffic flagged as a potential problem.[25]

---

[23] BP Detection 1: References/Comments: See the following document for more information:

www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf. Vulnerabilities can be reported in a standardized fashion using information provided at nvd.nist.gov/

Also see

puck.nether.net/mailman/listinfo/nsp-security

ops-trust.net/

www2.icsalabs.com/veris/

[24] BP Detection 2: References/Comments: See

www.team-cymru.org

www.shadowserver.org

www.abuse.ch

www.cbl.abuseat.org

[25] BP Detection 3: References/Comments: This technique should help minimize the exposure of customer information in detecting bots by not collecting detailed information until it is reasonable to believe the customer is infected. Looking at user traffic using a “wide net” approach can include external feedback as well as other internal approaches.

A.16 BP Number: Detection 4

Do Not Block Legitimate Traffic:

ISPs should ensure that detection methods do not block legitimate traffic in the course of conducting botnet detection, and should instead employ detection methods which seek to be non-disruptive and transparent to their customers and their customers' applications.[26]

A.17 BP Number: Detection 5

Bot Detection and the Corresponding Notification Should Be Timely:

ISPs should ensure that bot detection and the corresponding notification to end users be timely, since such security problems are time-sensitive.[27] If complex analysis is required and multiple confirmations are needed to confirm a bot is indeed present, then it is possible that the malware may cause some damage, to either the infected host or remotely targeted system (beyond the damage of the initial infection) before it can be stopped. Thus, an ISP must balance a desire to definitively confirm a malware infection, which may take an extended period of time, with the ability to predict the strong likelihood of a malware infection in a very short period of time. This "definitive-vs.-likely" challenge is difficult and, when in doubt, ISPs should err on the side of caution by communicating a likely malware infection while taking reasonable steps to avoid false notifications.

Notification Best Practices

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

A.18 BP Number: Notification 1

Notification to End Users:

ISPs should develop and maintain critical notification methods to communicate with their customers that their computer and/or network has likely been infected with malware.[28] This should include a range of options in order to accommodate a diverse group of customers and network technologies. Once an ISP has detected a likely end user security problem, steps should be undertaken to inform the Internet user that they may have a security problem. An ISP should decide the most appropriate method or methods for providing notification to their customers or internet users, and should use additional methods if the chosen method is not effective. The range of notification options may vary by the severity and/or criticality of the problem. Examples of different notification methods may include but are not limited to:

---

[26] BP Detection 4: References/Comments: None

[27] BP Detection 5: References/Comments: None

[28] BP Notification 1: References/Comments:

An ISP decision on the most appropriate method or methods for providing notification to one or more of their customers or Internet users depends upon a range of factors, from the technical capabilities of the ISP, to the technical attributes of the ISP's network, cost considerations, available server resources, available organizational resources, the number of likely infected hosts detected at any given time, and the severity of any possible threats, among many other factors. The use of multiple simultaneous notification methods is reasonable for an ISP but may be difficult for a fake anti-virus purveyor.

Mitigation BP 3 provides information on how to address the malware infection.

email, telephone call, postal mail, instant messaging (IM), short messaging service (SMS), and web browser notification.

A.19 BP Number: Notification 2

Notification Information to End Users:

ISPs should ensure that botnet notifications to subscribers convey critical service information rather than convey advertising of new services or other offers.[29]

Mitigation Best Practices

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

BP Number: Mitigation 1

Industry Cooperation During Significant Cyber Incidents:

ISPs should maintain an awareness of cybersecurity threat levels and, when feasible, cooperate with other organizations during significant cyber incidents, helping to gather and analyze information to characterize the attack, offer mitigation techniques, and take action to deter or defend against cyber attacks as authorized by applicable law and policy.[30]

A.21 BP Number: Mitigation 2

Temporarily Quarantine Bot Infected Devices:

ISPs may temporarily quarantine a subscriber account or device if a compromised device is detected on the subscribers' network and the network device is actively transmitting malicious traffic.[31] Such quarantining should normally occur only after multiple attempts to notify the customer of the problem (using varied methods) have not yielded resolution. In the event of a severe attack or where an infected host poses a significant present danger to the healthy operation of the network, then immediate quarantine may be appropriate. In any quarantine situation and depending on the severity of the attack or danger, the ISP should seek to be responsive to the needs of the customer to regain access to the network. Where feasible, the ISP may quarantine the attack or malicious traffic and leave the rest unaffected.

---

[29] BP Notification 2: References/Comments: This best practice is to help ensure that the notification message is not confused with other communications the customer may receive from the provider and help underscore the seriousness of the situation.

[30] BP Mitigation 1: References/Comments: In the United States, for example, the National Cyber Incident Response Plan - The National Cyber Risk AlertLevel (NCRAL) is currently envisioned as a 4-level system in order to facilitate synchronization with several other alert level systems, such as the IT-ISAC, SANS and those from security vendors. Significant Cyber Incidents are generally labeled as Severe (level 1) and Substantial (level 2).

[31] BP Mitigation 2: References/Comments:

The temporary delay of web pages for the purpose of providing web browser notification, as suggested above in the Notification Best Practices (see section 6.1.18), does not constitute a "quarantine" as used in this Best Practice.

Some information regarding quarantine technology can be found at:

www.trustedcomputinggroup.org/developers/trusted_network_connect

A.22 BP Number: Mitigation 3

Provide a Web Site to Assist with Malware Remediation:

ISPs should, either directly or indirectly, provide a web site to assist customers with malware remediation.[32]

Remediation of malware on a host means to remove, disable, or otherwise render a malicious bot harmless. For example, this may include but is not limited to providing a special web site with security-oriented content that is dedicated for this purpose, or suggesting a relevant and trusted third-party web site. This should be a security-oriented web site to which a user with a bot infection can be directed to for remediation. This security web site should clearly explain what malware is and the threats that it may pose. Where feasible, there should be a clear explanation of the steps that the user should take in order to attempt to clean their host, and there should be information on how users can strive to keep the host free of future infections. The security web site may also have a guided process that takes non technical users through the remediation process, on an easily understood, step-by-step basis. The site may also provide recommendations concerning free as well as for-fee remediation services so that the user understands that they have a range of options, some of which can be followed at no cost.

Privacy Best Practices

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

A.23 BP Number: Privacy Considerations 1

Privacy Considerations in Botnet Detection, Notification, and Remediation:

Because technical measures to (a) detect compromised end-user devices, (b) notify end-users of the security issue, and (c) assist in addressing the security issue, may result in the collection of customer information (including possibly "personally identifiable information" and other sensitive information, as well as the content of customer communications), ISPs should ensure that all such technical measures address customers' privacy, and comply and be consistent with all applicable laws and corporate privacy policies.[33]

A.24 BP Number: Privacy Considerations 2

Measures to Protect Privacy in Botnet Response:

In designing technical measures for identification, notification, or other response to compromised end-user devices ("technical measures"), ISPs should pursue a multi-prong strategy to protect the privacy of customers' information, including but not limited to the following:[34]

– ISPs should design technical measures to minimize the collection of customer information;

– In the event that customer information is determined to not be needed for the purpose of responding to security issues, the information should promptly be discarded;

---

[32] BP Mitigation 3: References/Comments: None

[33] BP Privacy Considerations 1: References/Comments: None

[34] BP Privacy Considerations 2: References/Comments: None

- Any access to customer information collected as a result of technical measures should at all times be limited to those persons reasonably necessary to implement the botnet-response security program of the ISP, and such individuals' access should only be permitted as needed to implement the security program;
- In the event that temporary retention of customer information is necessary to identify the source of a malware infection, to demonstrate to the user that malicious packets are originating from their broadband connection, or for other purposes directly related to the botnet-response security program, such information should not be retained longer than reasonably necessary to implement the security program (except to the extent that law enforcement investigating or prosecuting a security situation, using appropriate procedures, has requested that the information be retained); and
- The ISP's privacy compliance officer, or another person not involved in the execution of the security program, should verify compliance by the security program with appropriate privacy practices.

References

Alliance for Telecommunications Industry Solutions (ATIS) - http://www.atis.org/

Anti-Botnet - http://botfrei.de

Comcast.net Security - http://security.comcast.net/

Composite Blocking List - http://cbl.abuseat.org

Cyber Clean Center - https://www.ccc.go.jp/en_ccc/

Department of Homeland Security – http://www.dhs.gov/files/programs/gc_1158611596104.shtm

Department of Homeland Security – United States Computer Emergency Readiness Team (US-CERT) - http://www.us-cert.gov/

DNS Check – http://dnscheck.iis.se/

DNS Security Extensions Securing the Domain Name System (DNSSEC) - http://dnssec.net

DNSSEC - https://www.dnssec-deployment.org

Domain Name System Operations Analysis and Research Center (DNS-OARC) – https://www.dns-oarc.net/oarc/services/dnsentropy

DomainKeys Identified Mail (DKIM) - http://www.dkim.org/

International Telecommunication Union Botnet Mitigation Toolkit – http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

Internet Assigned Numbers Authority Cross Pollination Check - http://recursive.iana.org/

Internet Assigned Numbers Authority FAQs on Cache Poisoning and Cross Pollination – http://www.iana.org/reports/2008/cross-pollination-faq.html

Internet Storm Center - http://isc.sans.edu/index.html

Messaging Anti-Abuse Working Group (MAAWG.org) – Code of Conduct – http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Common Best Practices – http://www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_200907.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Email Authentication – http://www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Expansion and Clarification of the BIAC & MAAWG Best Practices for Internet Service Providers and Network Operators – http://www.maawg.org/sites/maawg/files/news/MAAWGBIAC_Expansion0707.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Managing Port 25 – http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Methods for Sharing Dynamic Address Space – http://www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf

Messaging Anti-Abuse Working Group (MAAWG.org) – Overview of DNS Security – www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf

Microsoft – http://www.microsoft.com/security/pypc.aspx

National Cybersecurity Alliance – http://www.staysafeonline.org/

National Vulnerability Database – National Institute of Standards and Technology – http://nvd.nist.gov/

NSP Security Forum (NSP-SEC) – http://puck.nether.net/mailman/listinfo/nsp-security

OnGuard Online – http://www.onguardonline.gov/default.aspx

OPSEC-Trust – https://www.ops-trust.net/

Qwest Incredible Internet Security Site – http://www.incredibleinternet.com/

Shadowserver Foundation – http://www.shadowserver.org

Spamhaus Policy Block List - http://www.spamhaus.org/pbl/

SPF Project – http://openspf.org

StopBadware – http://www.stopbadware.org/home/badware_prevent

Swiss Security Blog – http://abuse.ch

Team Cymru Research NFP – http://www.team-cymru.org

Trend Micro Maps – http://www.mail-abuse.com/nominats_dul.html

Trusted Computing Group – http://www.trustedcomputinggroup.org/developers/trusted_network_connect

U.S. Commerce Department's National Institute of Standards and Technology (NIST) – http://www.nist.gov/index.html

Verizon Enterprise Risk and Incident Sharing (VERIS) – https://www2.icsalabs.com/veris/

Verizon Safety & Security – http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_safety

Annex E: Best practices for Cybersecurity – Training Course on Building and Managing National Computer Incident Response Teams (CIRTs)

Best Practices for National Cyber Security

Aspects of Building & Managing National Computer Incident Response Teams (CIRT)

These training materials are based on these reports:
International Telecommunications Union, *Best Practices for National Cybersecurity: Building a National Computer Security Incident Management Capability*, ITU-D Rapporteur's Group Meeting on Question 22-1/1 Geneva, 5-6 May 2011.

International Telecommunications Union, *Best Practices for National Cybersecurity: Managing a National CSIRT with Critical Success Factors*, ITU-D Rapporteur's Group Meeting on Question 22-1/1 Geneva, 5-6 May 2011.

Topics

Building a National CIRT
- Setting the Context: National Cyber Security
- Roles of a National CIRT
- Goals for Building National CIRTs

National CIRT Management
- Challenges Facing National CIRTs
- Introduction to Critical Success Factors

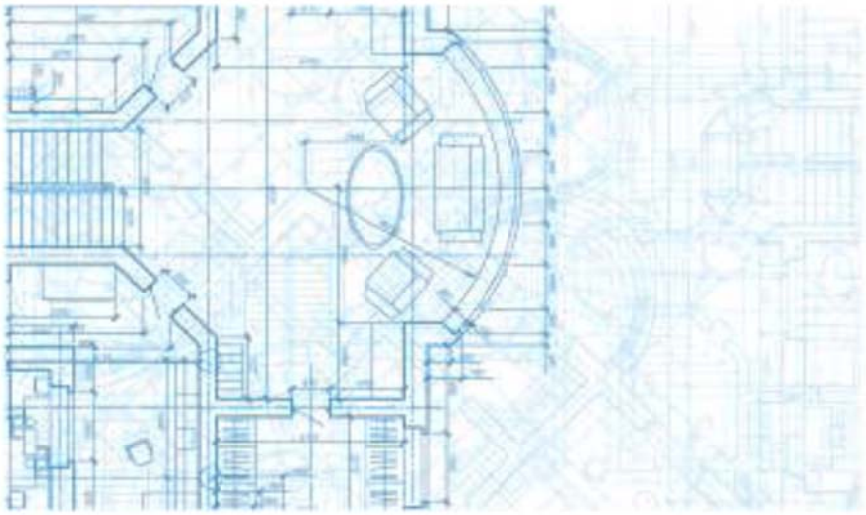
Identifying Critical Success Factors (CSFs) for an Organization

Using Critical Success Factors in National CIRT Management
- Selecting Services
- Identifying Measurement Priorities

Summary

2

BUILDING A NATIONAL CIRT



What is a National CIRT?

A National CIRT coordinates incident management and facilitates an understanding of cyber security issues for the national community.

Usually officially appointed by the government

Are unique because of their cyber perspective on how to protect and sustain

- National and economic security
- Government operations
- Critical infrastructure operations and functions

Can serve one or many constituencies, including

- Government organizations
- Critical infrastructures
- The public in general

May have different names in different countries, such as Computer Security Incident Response Team or Computer Emergency Response Team

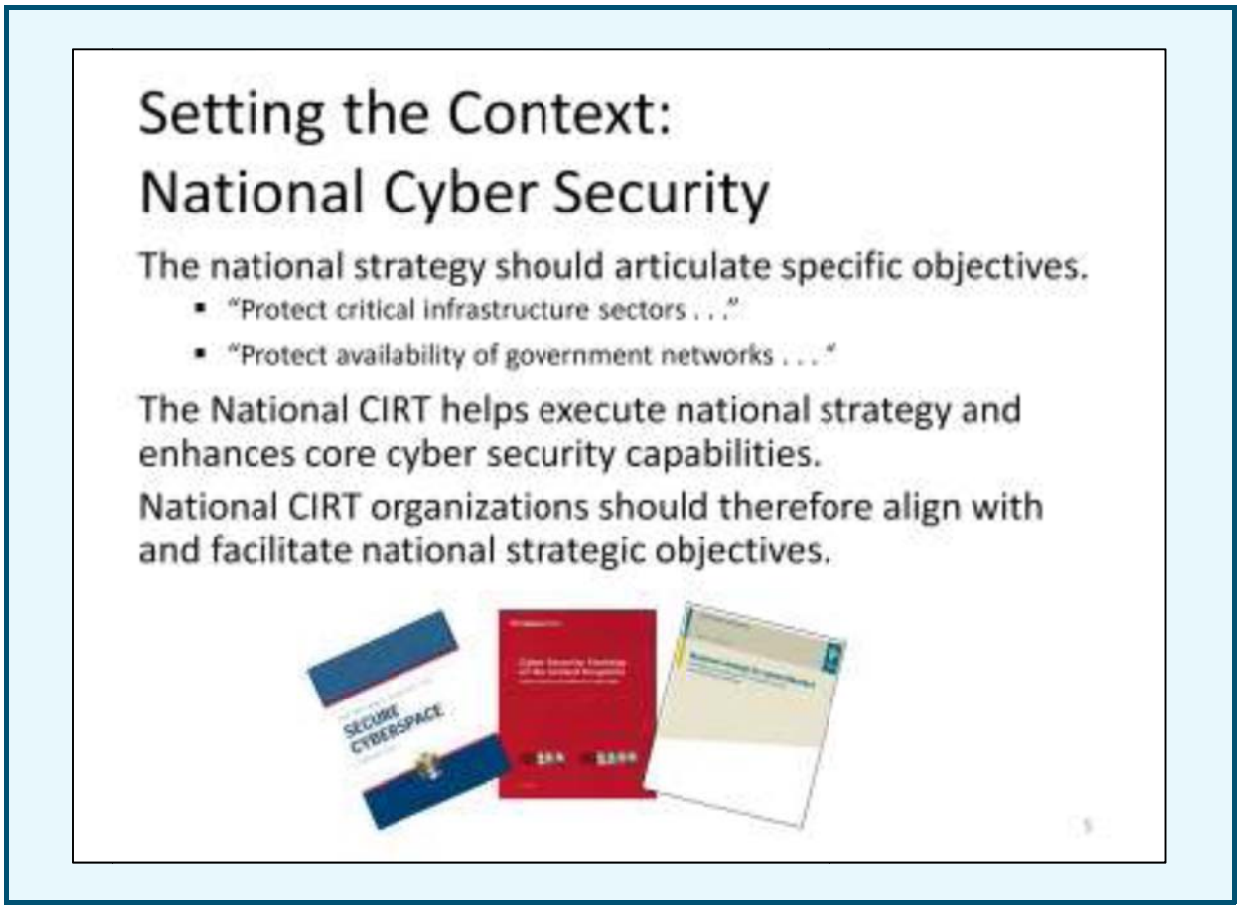
National CIRTs are concerned with supporting the cyber resilience of their country or economy.

National incident management organizations frequently go by different names. In these materials, "National CIRT" is used because it is in common use. While the specific names of cyber incident management organizations vary, the choice of name may be relevant to the organization's relationship with members of the response community. It is also not unusual for nations to have more than one National CIRT. Depending on the country's government and other structural factors, there may be a natural preference for certain constituencies to be served by different organizations. The most obvious example is where a government operates a CIRT under the military or defense establishment and a separate organization to serve the public or the private owners of critical infrastructure*.

*__Note__: Organizations and countries around the world have **defined** Critical Infrastructure (CI) differently in but all reflect CI's importance to the society. For example:

Germany: Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."

Japan: "Critical infrastructure which offers the highly irreplaceable service in a commercial way is necessary for people's normal lives and economic activities, and if the service is discontinued or the supply is deficient or not available, it will seriously influence people's lives and economic activities."



This course is not intended as a review or discussion of national cybersecurity strategy. However, National CIRTs should ideally reflect and support their country's security strategy.

Creating a national strategy for cybersecurity is the first step in establishing a national program. The goals that a nation identifies and promotes through its strategy give the program a consistent vision and

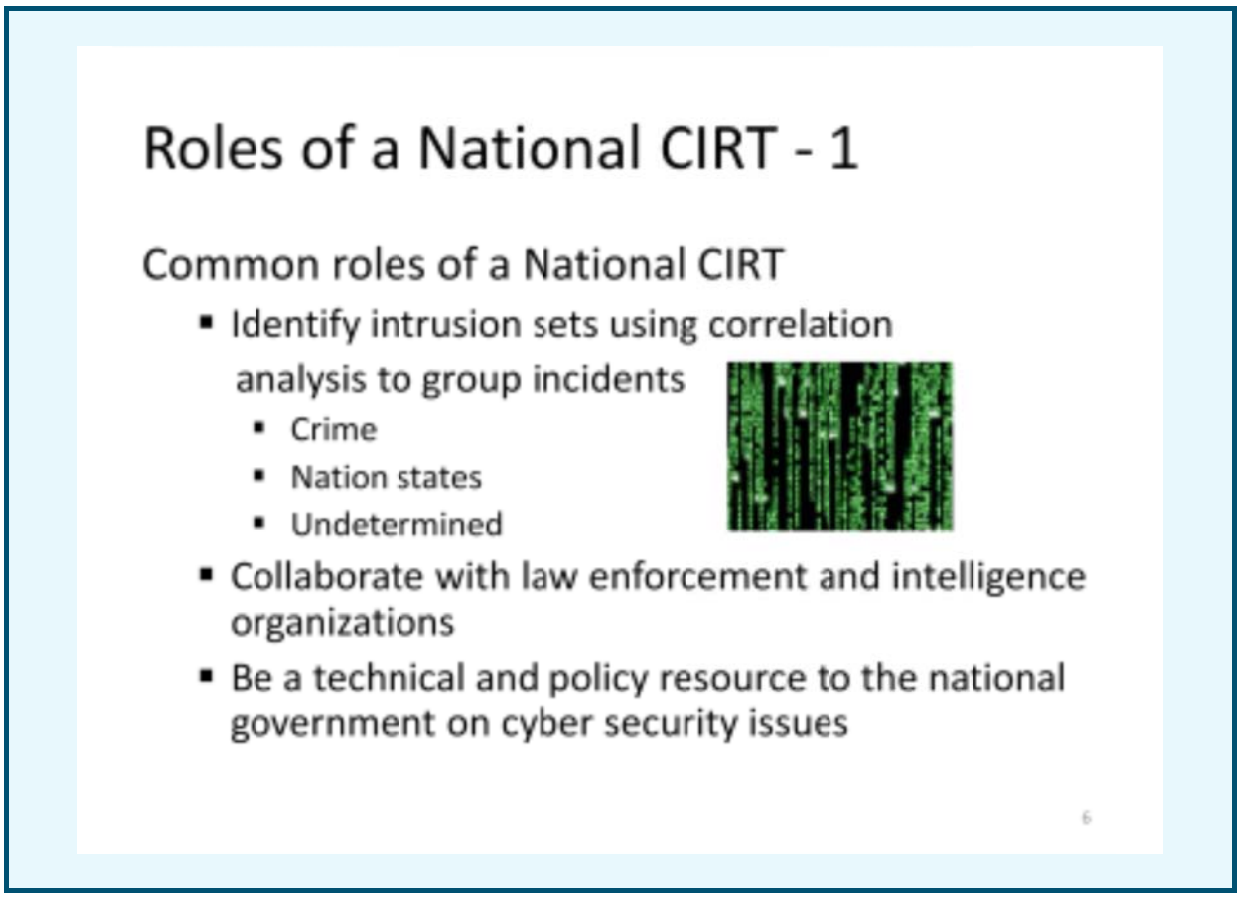
establish a clear direction. The national strategy should stress the benefits of a culture of cybersecurity, integrate security fundamentals, such as raising awareness, and emphasize cooperative relationships among national stakeholders. The national strategy may also serve as a backdrop for the creation of laws that relate to cybersecurity; for instance in the areas of computer crime, the protection of intellectual property, and privacy. Finally the national strategy should reconcile the need for security with the need to honor citizens' rights and the nation's cultural values and norms.

A frequently asked question is, must a nation have a complete, cogent cybersecurity strategy before instantiating a National CIRT? Generally the answer is no, and it has often been the case that the National CIRT has helped the national government develop and refine their strategy after operating for some years.

A National CIRT capability may also fall under a different government strategy.

The three documents pictured are:

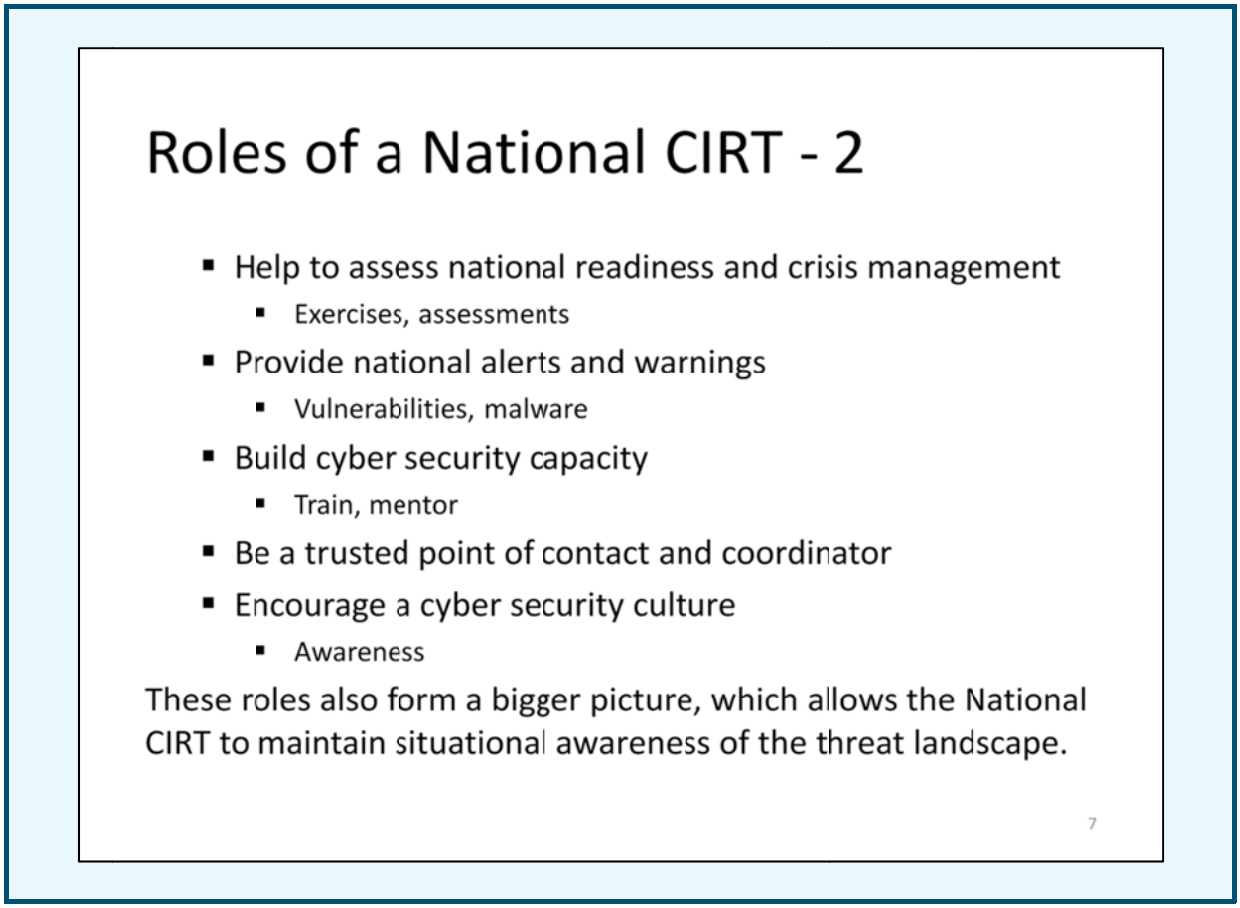
1. U.S.' National Strategy to Secure Cyberspace www.us-cert.gov/reading_room/cyberspace_strategy.pdf
2. U.K.'s Cybersecurity Strategy of the United Kingdom www.cabinetoffice.gov.uk/media/216620/css0906.pdf
3. Norwegian's (Norsk) Nasjonal strategi for cybersikkerhet https://www.nsm.stat.no/Documents/andre_dokumenter/Nasjonal%20strategi%20for%20cybersikkerhet.pdf



A variety of organizations have CIRTs. Here are the national-level roles that a National CIRT provides to the government and to the nation that organizational CIRTs typically do not. This slide is not meant to imply that all National CIRTs must provide all of these services. These are simply the kinds of services that a National CIRT would provide.

Analyze computer security incident information ... Examples include correlations and analysis based on malware type and behavior, social engineering methods and signatures, IP addresses used – and many others.

Be a technical resource ... The National CIRT acts as the government's "go-to" organization on questions of cyber-security.



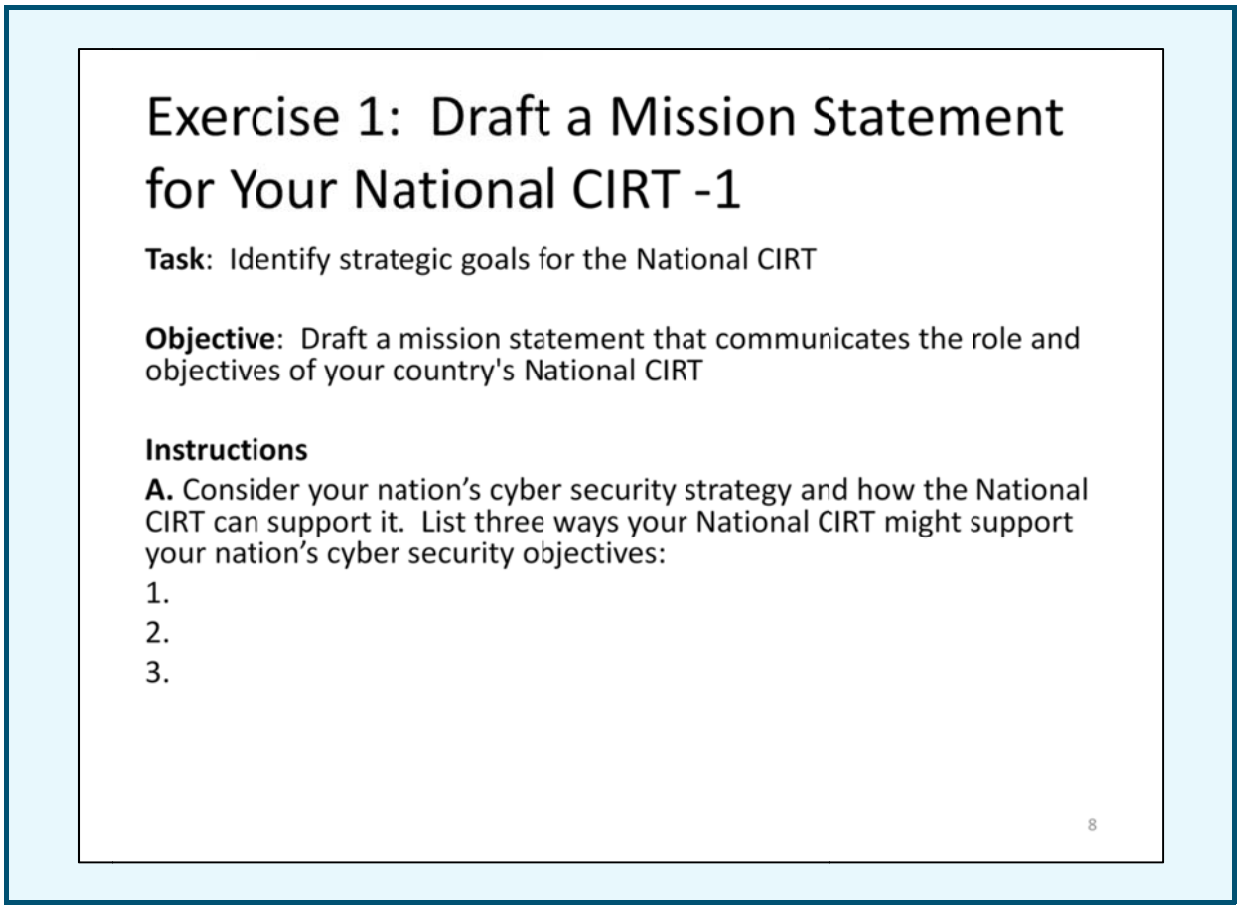
Help to assess ... the National CIRT can help to assess national readiness. It does so by integrating risk information from major stakeholders and constituents, and play a key role in development and execution of exercises.

Alerts and Warning ... One of the key roles, the National CIRT establishes warning channels. It builds relationships with key stakeholder organizations to relay alerts and warnings about security vulnerabilities and threats. The National CIRT also alerts and warns the general public about computer security problems.

Build cybersecurity capacity ... Externally, the National CIRT builds capacity by engaging with other National CIRTs to build their capabilities through the sharing of best practices, training, etc. Internally, the National CIRTs can help organizational CIRTs in the nation in a variety of ways including advice, training, best practices, or in some cases staffing.

Be a trusted national point of contact ... The National CIRTs acts as the nation's representative in the international computer security response community.

Encourage a cybersecurity culture ... The National CIRT has a role to play in fostering a cybersecurity culture, in reinforcing the role everyone plays in cybersecurity.



A Mission Statement is the purpose of an organization. It defines the organizations reason for existence. It generally includes three key pieces of information:

1) identity of stakeholders, constituents, or customers

2) the purpose of an organization

3) the value/advantage/service provided.

For National CIRTs this would include:

1) Constituents of the CIRT

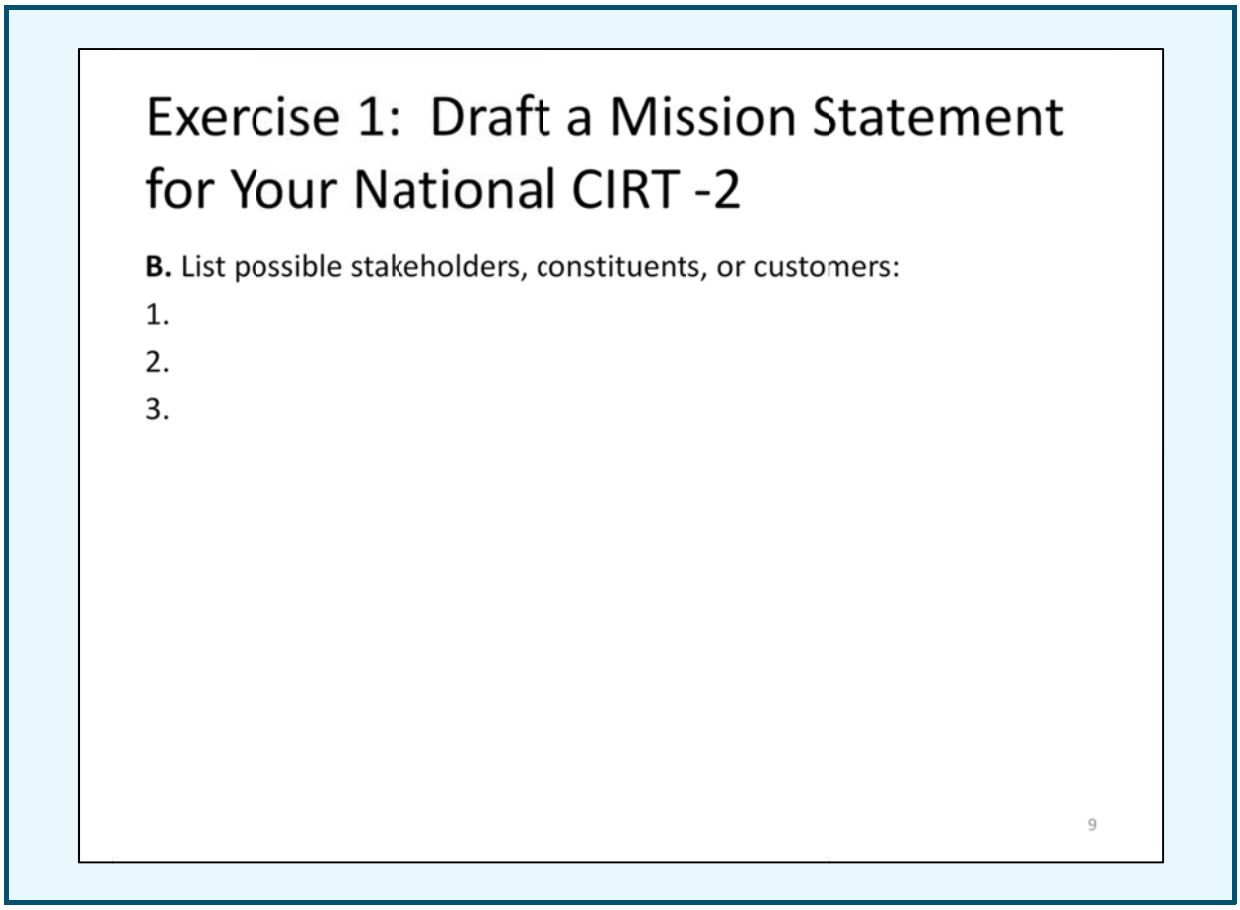
2) *Contribution made to the Constituents*

3) *Distinction of the CIRT from other providers of similar services*

As an example, Japan Computer Emergency Response Team Coordination Center

http://www.jpcert.or.jp/english/about.html

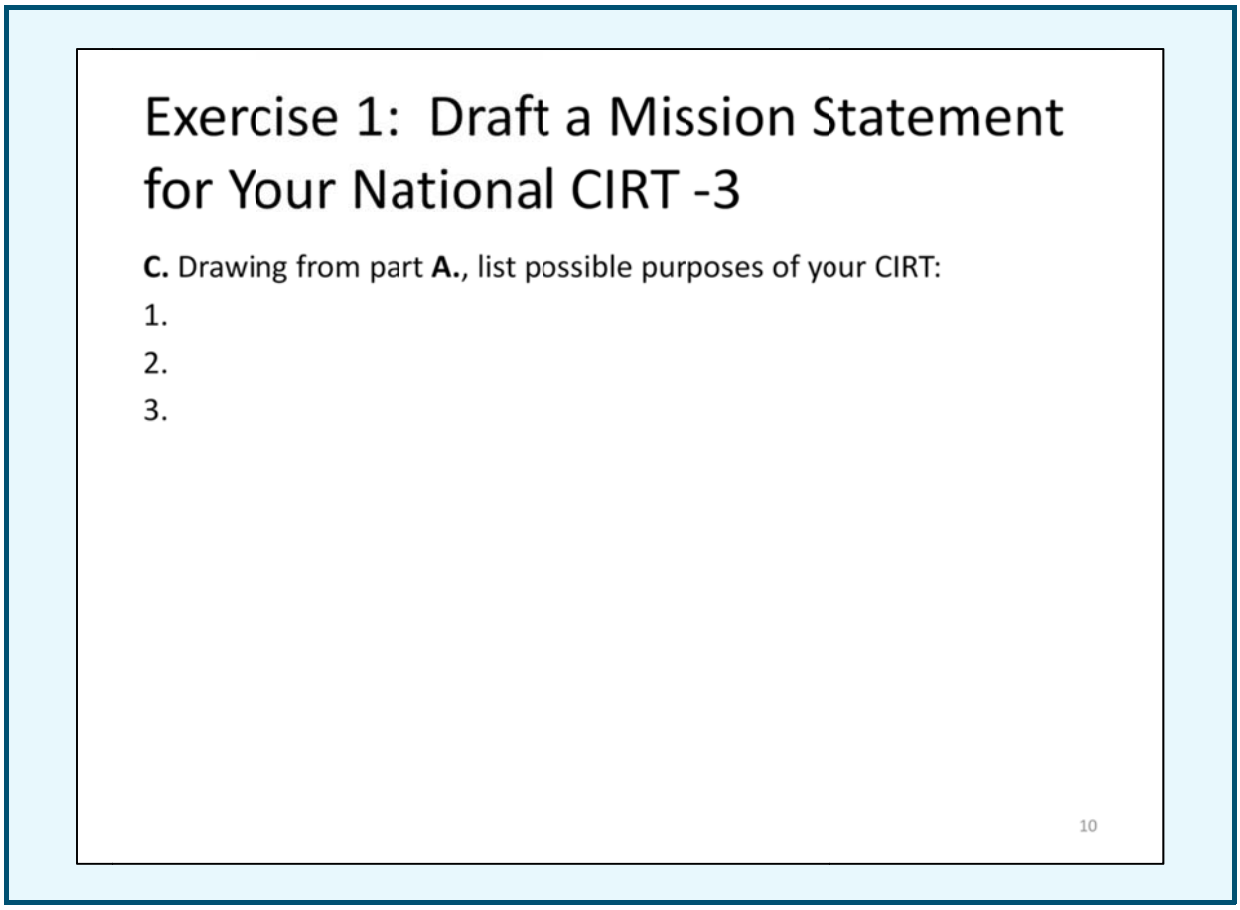
"**JPCERT/CC is a first CIRT (Computer Security Incident Response Team) established in Japan.** The organization *coordinates* with network service providers, security vendors, government agencies, as well as the industry associations. As such, *it acts as a "CIRT of the CIRTs"* in the Japanese community. In Asia Pacific region, **JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team)** *and provides a secretariat function* for APCERT. Globally, as a *member of Forum of Incident Response and Security Teams (FIRST),* JPCERT/CC *coordinates its activities* with the **trusted** CIRTs worldwide."



The follow examples are from rfc 2350 section 3 "Information, Policies and Procedures" from: CERT.at, SI-CERT, CZ.NIC-CIRT, KIT-CERT, Team Cymru, ID-SIRTII, IRISS-CERT, HANCERT, CERT-RU, CIRCL

Commonly Used Terms for Constituents:

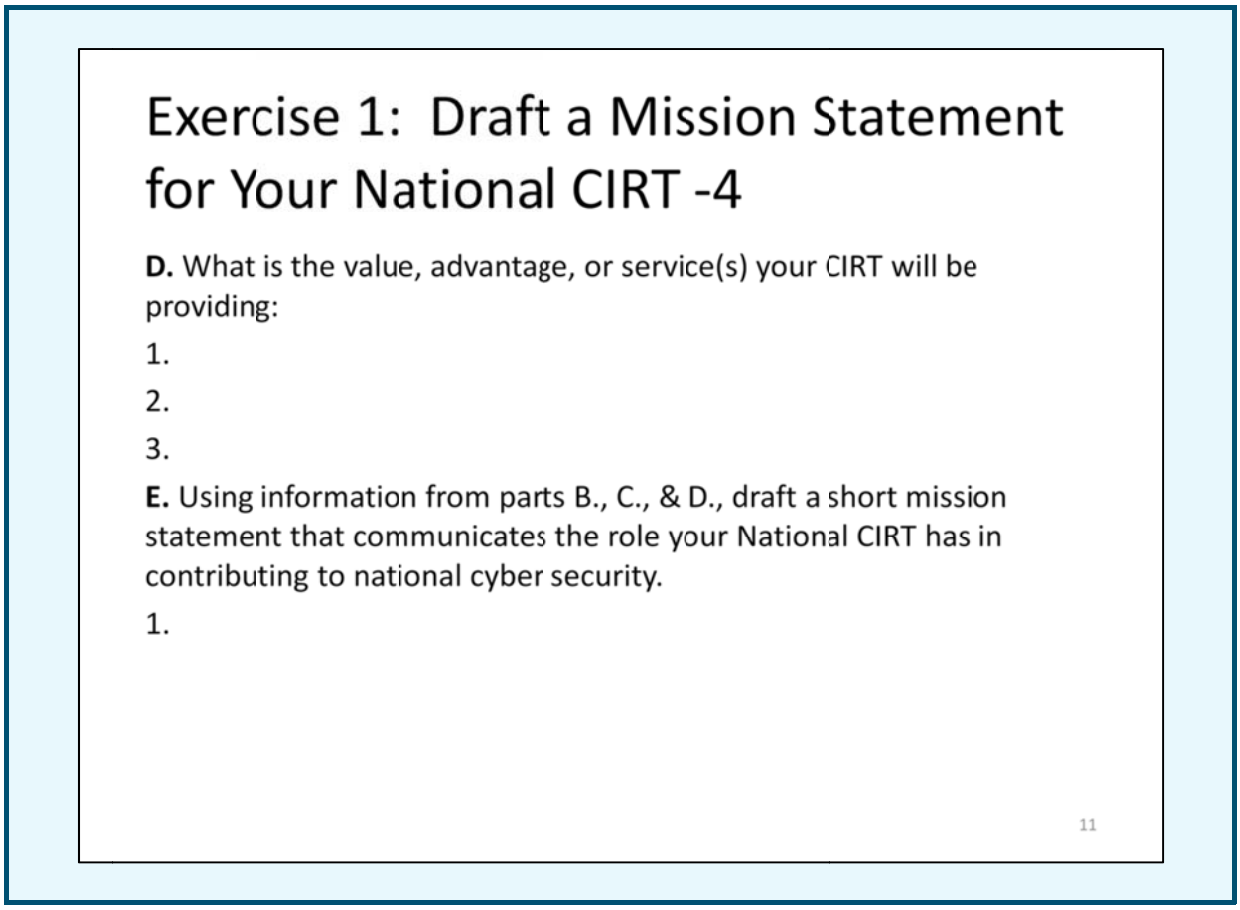
- "national level in Austria"
- "systems and networks located in Slovenia"
- "general public"
- "Karlsruhe Institute of Technology community"
- "organizations"
- "national level in Indonesia"
- "Irish based organisations and citizens"
- "information processing facilities"
- "Radboud University of Nijmegen".



The follow examples are from rfc 2350 section 3 "Information, Policies and Procedures" from: CERT.at, SI-CERT, CZ.NIC-CIRT, KIT-CERT, Team Cymru, ID-SIRTII, IRISS-CERT, HANCERT, CERT-RU, CIRCL

Commonly use terms for Contribution:

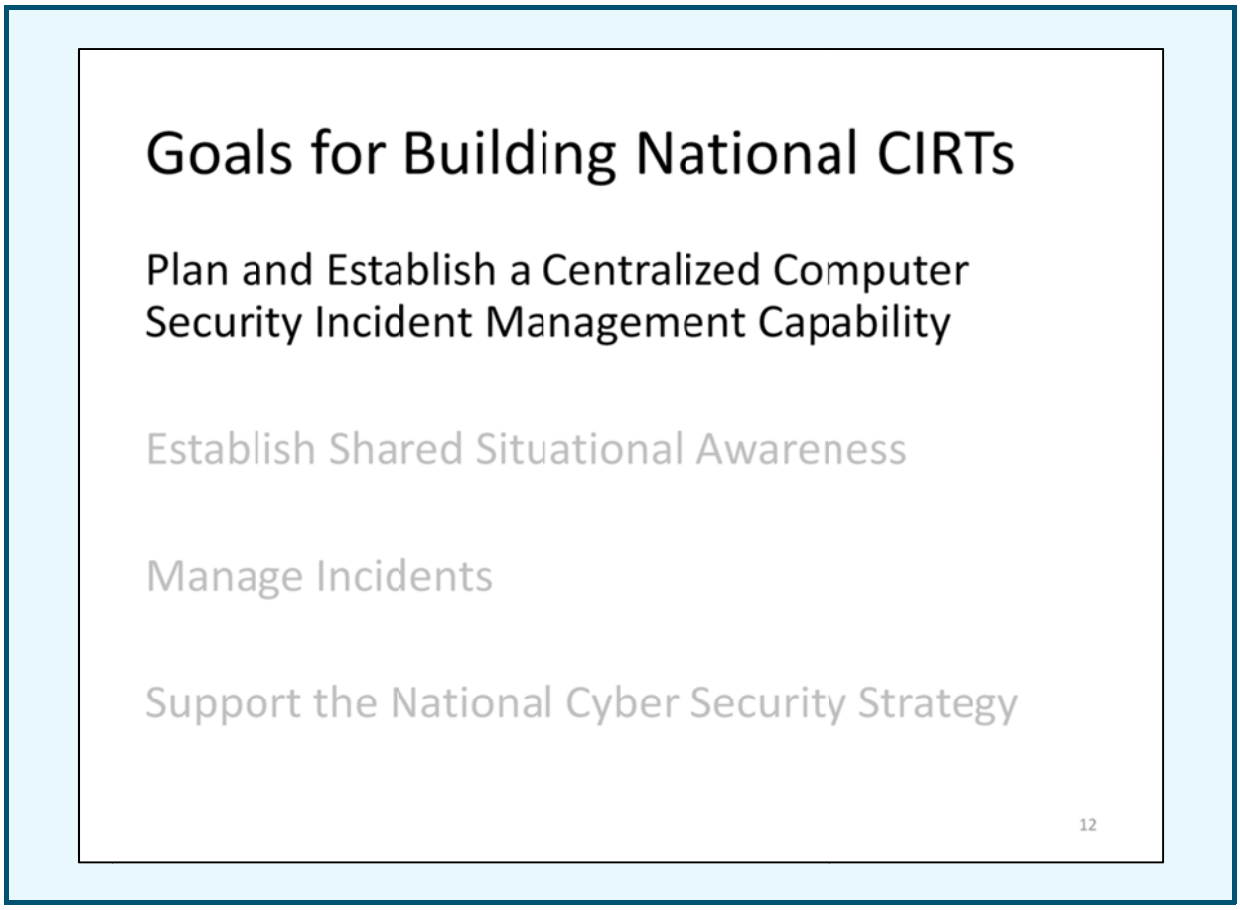
- "coordinate security efforts and incident response"
- "assistance in computer and network security incident handling and provides incident coordination functions for all incidents involving systems and networks"
- "raising awareness on issues of network and information security and provides advisories and alerts to the general public"
- "implementing proactive measures to reduce the risk of such incidents to occur."
- "coordinate security efforts and incident response for critical infrastructure and IT-security problems on a national level"
- "provide a range of high quality information security based services"
- "provide information security prevention, response and mitigation strategies"
- "coordinate the prevention and resolution of security incidents"
- "coordinate the resolution of IT security incidents"
- "help prevent such incidents from occurring"
- "coordinate communication among national and international incident response teams during security emergencies…"
- "provide a security related alert and warning system for national ICT users".



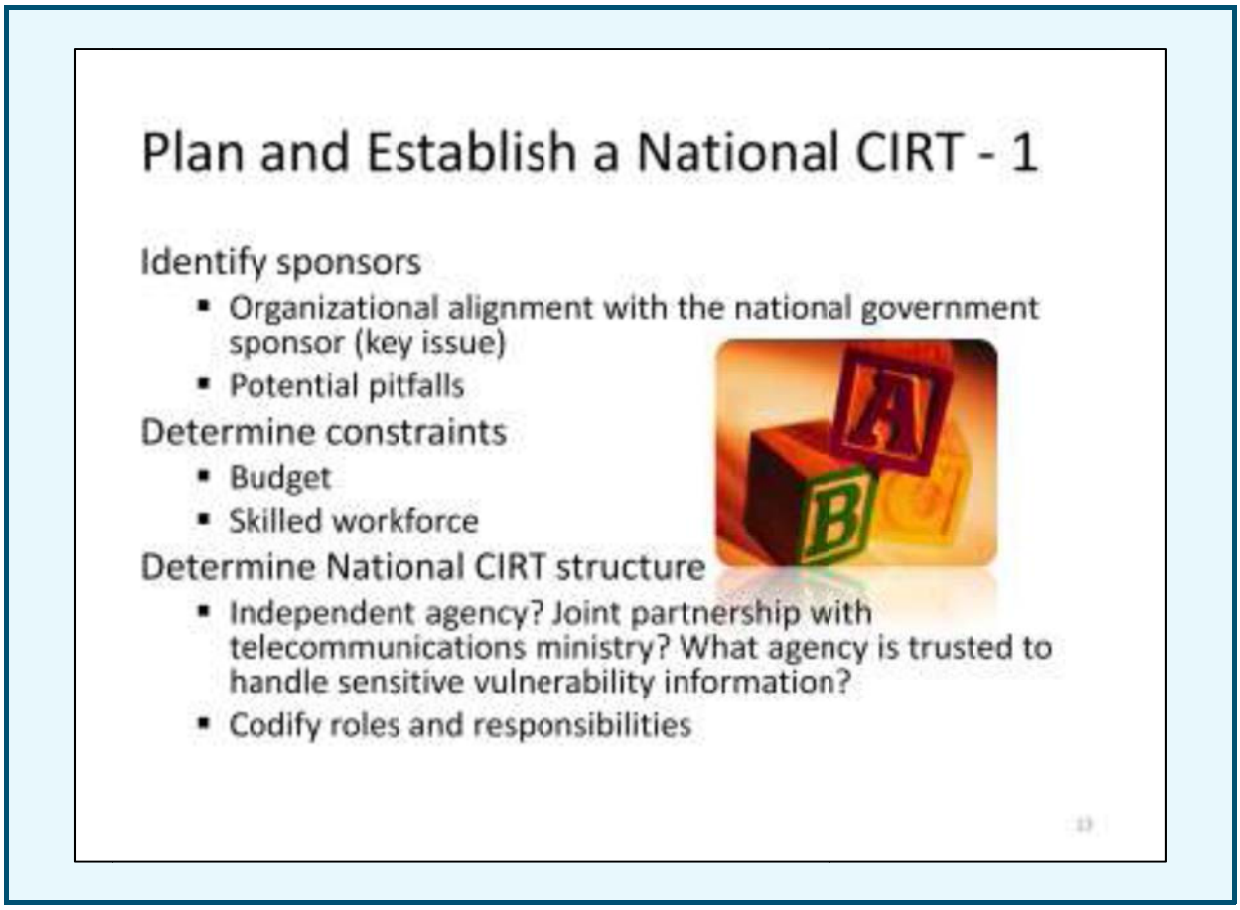
The follow examples are from rfc 2350 section 3 "Information, Policies and Procedures" from: CERT.at, SI-CERT, CZ.NIC-CIRT, KIT-CERT, Team Cymru, ID-SIRTII, IRISS-CERT, HANCERT, CERT-RU, CIRCL

Commonly used terms for Distinction:

- "offers assistance … in Slovenia"
- "solve incidents within .CZ DNS"
- "members of the KIT community"
- "researching the 'who' and 'why' of malicious Internet activity worldwide"
- "helps organizations identify and eradicate problems in their networks"
- "in accordance with industry recognised standards and compliance requirements"
- "become a recognised centre of information security excellence for national and international organisations to refer to".



Before the first cybersecurity incident can be managed, the capability must itself be established in an organizational form such as a National CIRT. Having a sole source or point of contact for computer security incidents and cybersecurity issues provides a number of benefits. A single organization provides stakeholders with a known source of information. A National CIRT can also provide the government with a conduit for coherent, consistent messaging on cybersecurity issues. With a single National CIRT, government departments have a source for technical information to support their individual functional areas. Finally, the National CIRT can encourage the discussion about cybersecurity and facilitate international cooperation on this issue. In some nations, unique considerations may dictate that there are multiple National CIRTs, or even an incident management capability that is spread across several organizations.



Identify Sponsors

In order to succeed, a National CIRT must have adequate sponsorship and commitment to resourcing.

– Executive sponsorship is critically important to the success of the National CIRT.

– Organizational alignment is very important between the government sponsor and the National CIRT to avoid potential pitfalls. For instance, what if a regulatory agency wants to be the host? Will the constituency be willing to share information with their regulator? In some countries the answer may be "certainly", in others perhaps not. In some situations there may be considerations involving human resources that dictate a certain agency taking the lead, for instance if one agency has the authority to pay the salary needed to attract the right talent to the organization.

Determine constraints

The sponsor of a National CIRT must have a clear understanding of what the staffing, technical, budget, and other constraints are. CIRTs in many organizations are often faced with budget shortfalls. A guiding principle is for the organization to perform a few core services well, rather than attempting to provide a broad array of services.

Determine the National CIRT structure

A National CIRT can be structured in a number of different ways, such as: an independent agency with limited operating partnerships, a joint operation with national telecommunications providers, or an integral part of the national military defense establishment. Some National CIRTs have also been started by universities.

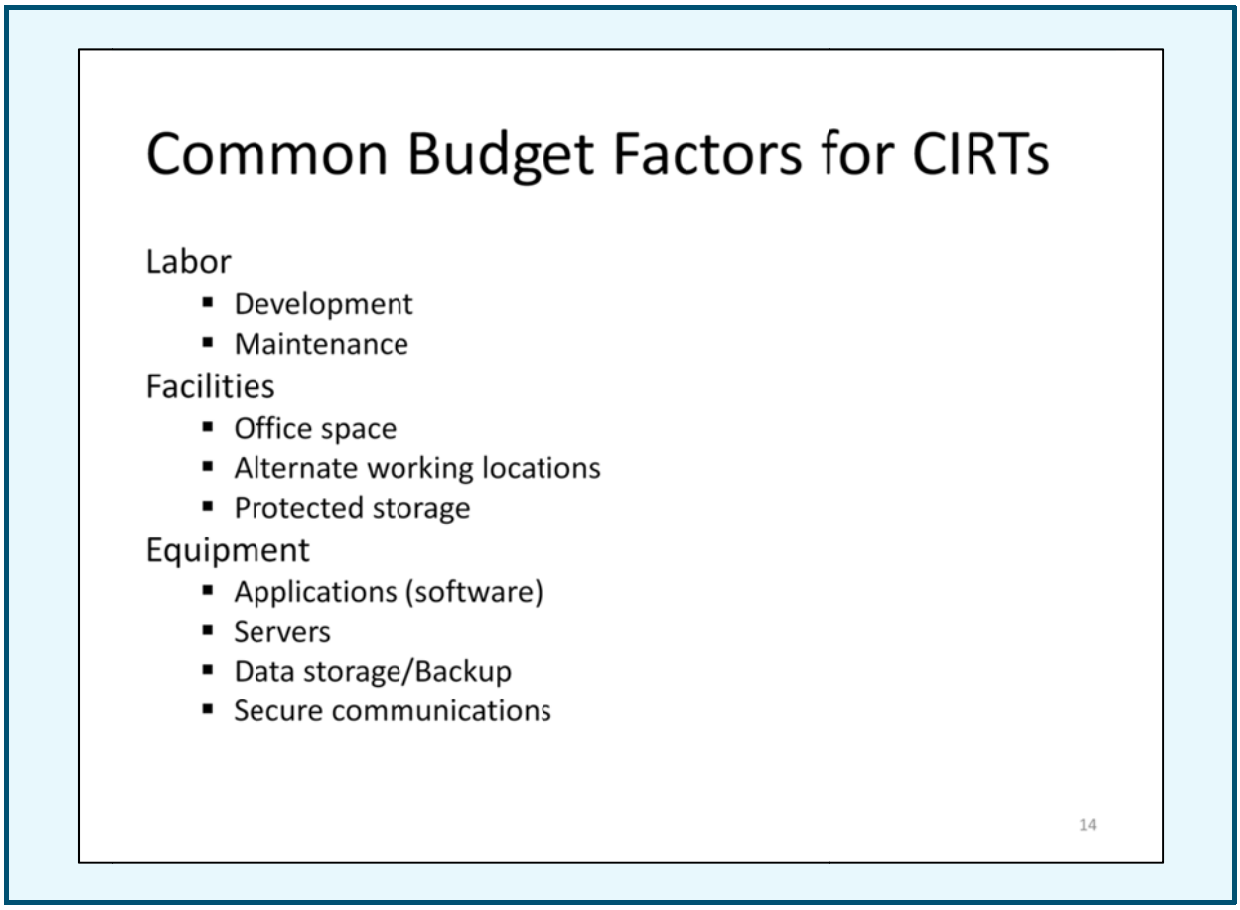
For new organizations, the following list of structural considerations is meant as guidance:

– What level of government directs the National CIRT?

– Who funds the National CIRT and who approves the budget?

– What structure would best allow the National CIRT to alleviate potential stakeholder concerns with regard to sharing information? Do the nation's privacy laws have any implications?

– If multiple National CIRTs are instituted, how should they share information?



Budgeting is an allocation of funds to activities in order to achieve a business objective or goal. Through the process of budgeting for a CIRT, funds will be allocated to specific activities, gaps will be identified, and hopefully, actual costs are tracked for future planning.

The majority of services offered by a CIRT are staff intensive, thus the largest percentage of budget would be allocated to them. An exception would be monitoring. At the national level, network monitoring would have a high cost on equipment.

"If you want to build a computer security incident response team (CIRT) with capable incident handlers, you need people with a certain set of skills and technical expertise, with abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with your constituency and other external contacts. They must also be competent problem solvers, must easily adapt to change, and must be effective in their daily activities. It is not often easy to find such qualified staff, so sometimes CIRTs nurture and train internal staff members to advance into these incident handling roles. "

"The composition of CIRT staff varies from team to team and depends on a number of factors, such as

– mission and goals of the CIRT
– nature and range of services offered
– available staff expertise
– constituency size and technology base
– anticipated incident load
– severity or complexity of incident reports
– funding "

CERT®

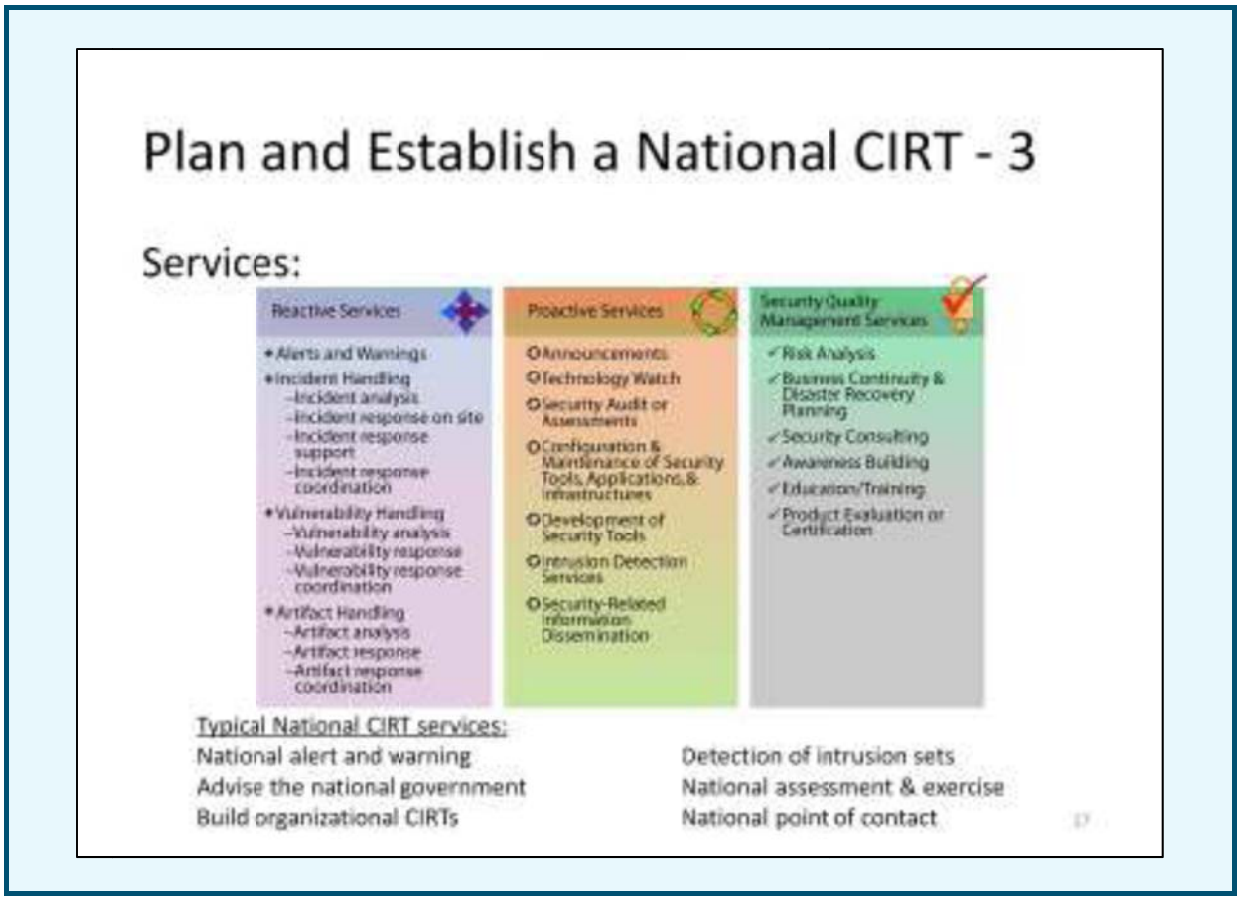
Determine the Authority of the National CIRT

The National CIRT champion or sponsor should determine if the National CIRT will have the authority to proscribe or mandate certain actions. This authority could involve mandating the reporting of security incidents, or the adoption of certain security measures, or both. In addition, the authority of a National CIRT may differ based on whether it is addressing private citizens and industry, or government departments. It may be appropriate for the National CIRT or the sponsoring organization to maintain authority over various government departments, but to have no authority over private citizens.

These decisions will be made consistently with the nation's law and culture. However, frequently National CIRTs are more effective when they act in an advisory role only. Major national stakeholders are often more willing and – depending on the legal environment – more able to fully share information and discuss security vulnerabilities in a collaborative venue where the National CIRT is not a regulatory or proscriptive body.

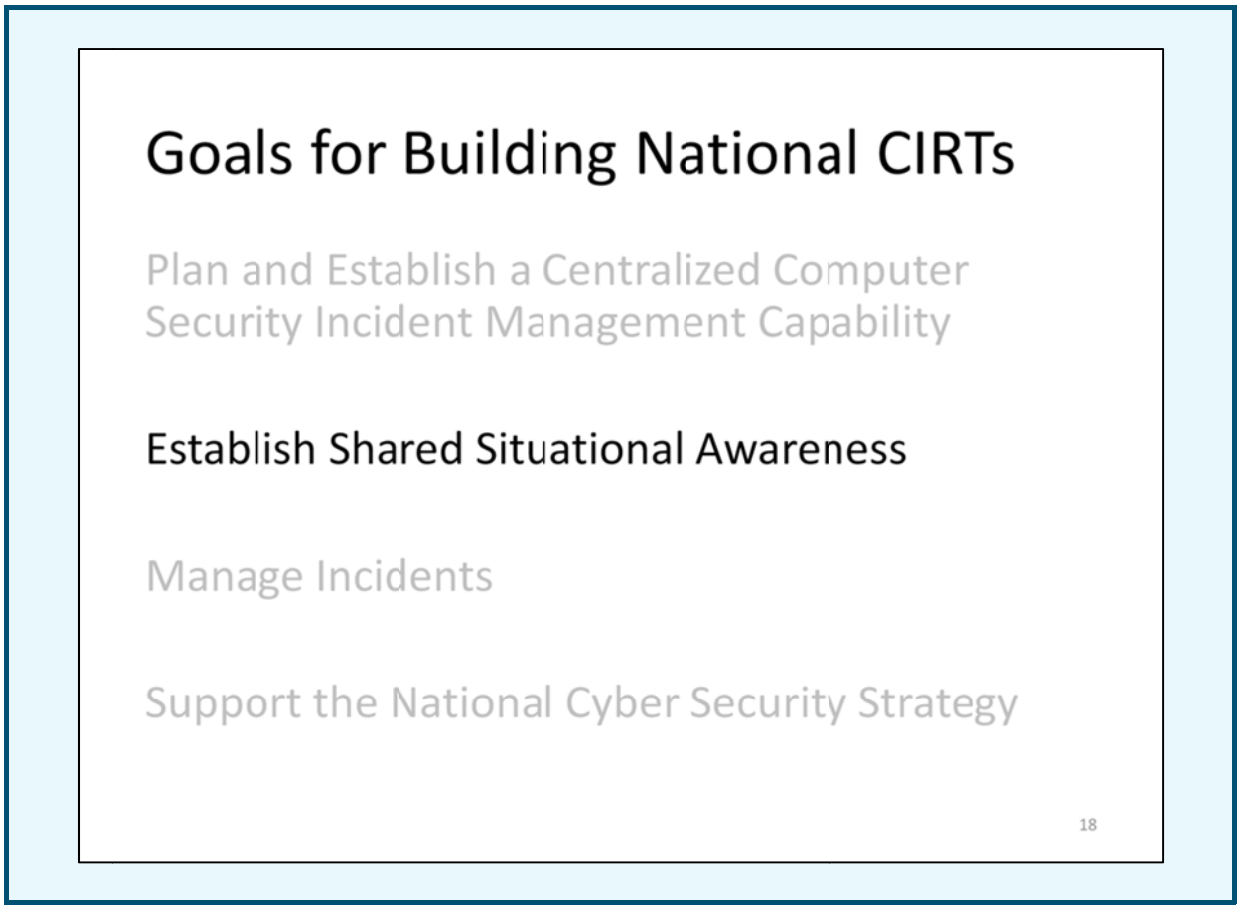
Identify constituency

A basic consideration for standing up any CIRT organization is deciding upon the constituency. Whom – specifically which organizations and individuals – will the National CIRT serve? For an organization just standing up, the leaders behind the effort should consider how cyber incident management is being done currently. With whom is the constituency communicating now and from whom are they receiving services? Are there any other response organizations that the new National CIRT will need to coordinate with? Does all of the constituency know that the National CIRT will be providing services to them? What do they need?



The National CIRT sponsor organization must determine which of these activities are realistic given the constraints involved. Typically the most significant constraint is human capital (staffing). Since the National CIRT serves as the national leader in cybersecurity incident management and analysis, the guiding principle for choosing particular services should be the ability to do it well. It may be that the best way for a particular National CIRT to fulfill its role is through close coordination with other National CIRTs that have a greater technical capability or who may already have trusted communication channels.

From https://www.cert.org/CIRTs/services.html



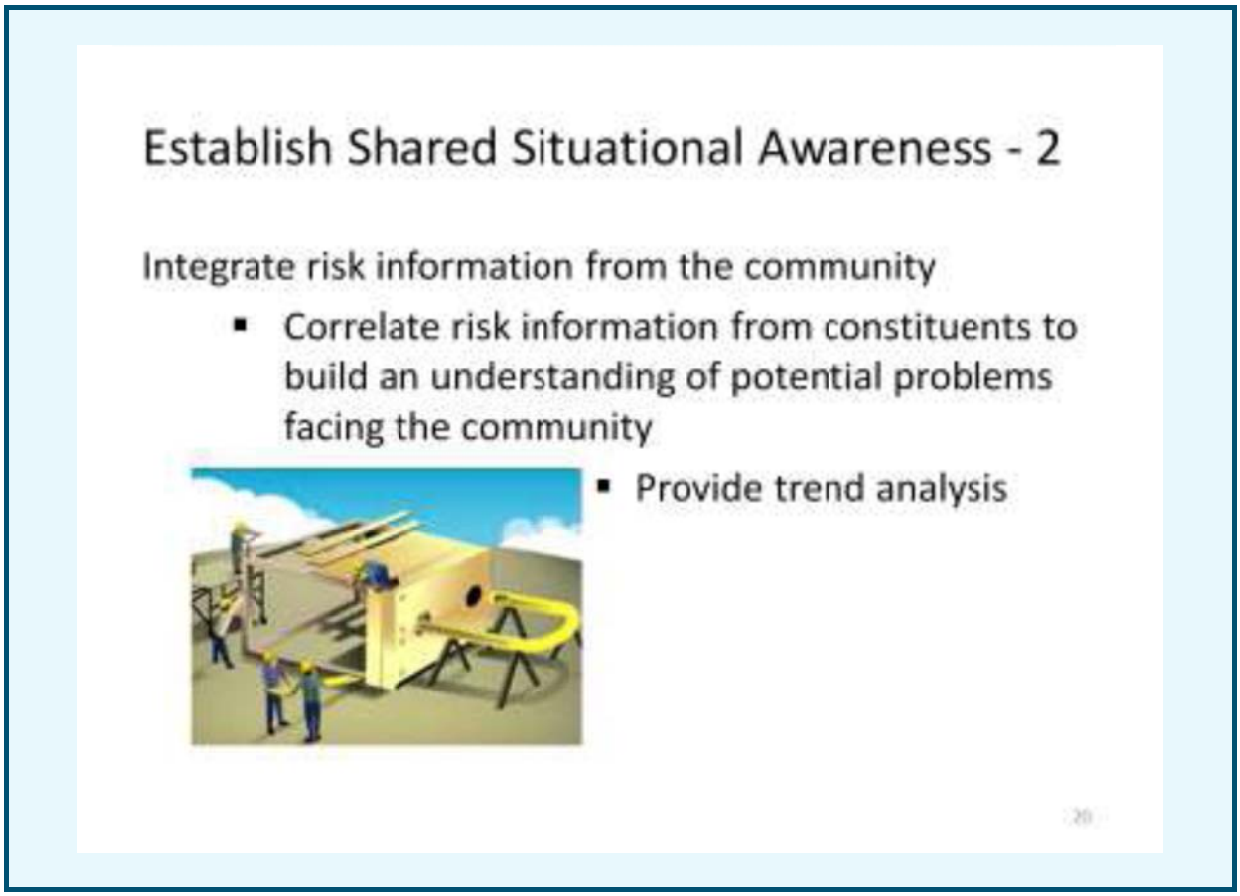
The essential function of a National CIRT is the ability to manage cybersecurity threats and incidents that are of importance to national stakeholders. Excellence in incident management helps the National CIRT to build relationships with stakeholders and achieve other strategic objectives, such as supporting the national cybersecurity strategy. The first step in managing incidents is establishing an understanding or awareness of who the National CIRT's major constituents are, what types of systems they employ (Information and Communications Technology), and what types of incidents they are experiencing. This general understanding of the environment is typically referred to as shared situational awareness.

Building and maintaining trust relationships is a very important operational imperative for a National CIRT. The most basic prerequisite is that the National CIRT must ensure the confidentiality of stakeholder information. A basic best practice to protecting confidential information is to never release information about an incident or event – even if the specific victim or organization information has been anonymized – without the permission of the victim organization.

Regardless of the specific security measures and policies, the National CIRT should proactively address stakeholder concerns in this area and be as transparent as possible about the security steps taken.

One of the most important factors in establishing a national capability is to facilitate reliable and effective information sharing. A key role for a National CIRT is to obtain incident information from the community and to disseminate timely and relevant response information back to the community. The information generally includes the following:

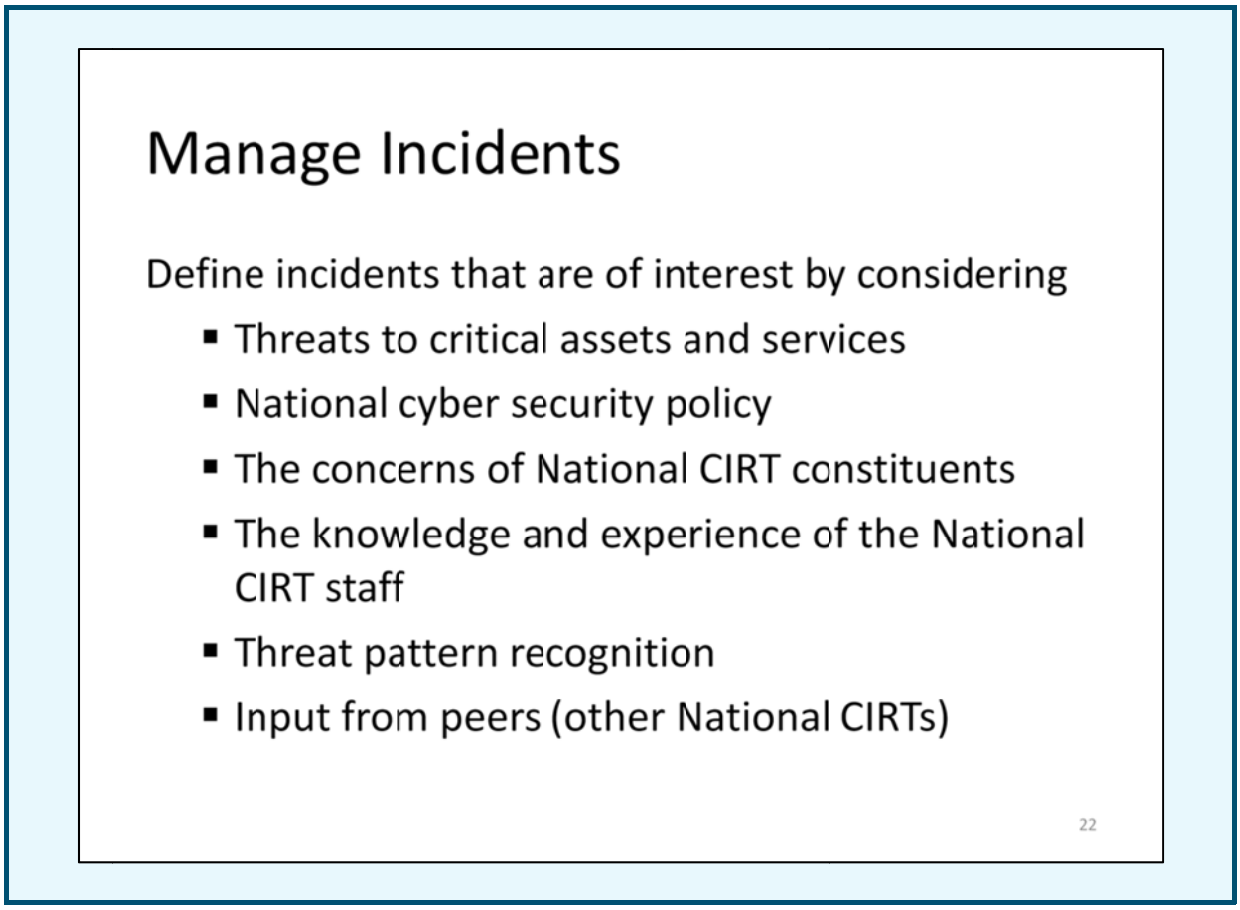
– incoming information about security incidents, collected through a variety of means
– security bulletins, awareness information on cyber threats and vulnerabilities
– general, specific, and urgent cyber warnings and alerts (technical and non-technical)
– best practices to prevent cybersecurity problems, events, and incidents
– general National CIRT information (e.g., organizational chart, sponsorship, services provided by the National CIRT, contact number/email address, etc.)
– resources and reference materials (e.g., security tools, partner organizations).



National CIRTs benefit from open, shared information from private industry, academia, and government. When organizations conduct thorough risk assessments and share the results with the National CIRT, situational awareness increases. Risk information from the community can help the National CIRT understand the effect that security vulnerabilities and system problems might have on important assets and infrastructure, helping the National CIRT to focus and refine its incident management process.

In its operational role of responding to incidents, a National CIRT is a key contributor to situational awareness. By analyzing trends in the incidents being managed, the National CIRT learns about the status of cybersecurity within the community it serves. The National CIRT uses this knowledge and its own perspective on problems to produce a credible, realistic picture of national situational awareness. This helps the National CIRT to identify proactive defense strategies, as well as needed improvements in practices and behaviors within the community.

A National CIRT, acting as a trusted, national cybersecurity focal point, is uniquely situated to manage incidents of national concern. To accomplish this, many National CIRTs establish certain active capabilities, such as incident response and containment, and service reconstitution. It is important to remember that in many cases the National CIRT will not handle all of the incident handling and analysis itself. A National CIRT may act to facilitate and coordinate analysis and response, either because of limited resources or because knowledge about the specific problem may reside elsewhere, for instance at another National CIRT or at a technology vendor.



Determining where the National CIRT should focus its attention is an iterative, evolving process. It is not unusual for a National CIRT to be inundated with requests for assistance shortly after its creation. This places the National CIRT in the position of having to balance the scarcity of time and resources with a desire to serve the constituency. To address this potential problem the National CIRT should decide which events and interests it will focus its attention on, and then communicate these "incident criteria" to its stakeholders and constituents.

A sample list of "incident criteria" could be:

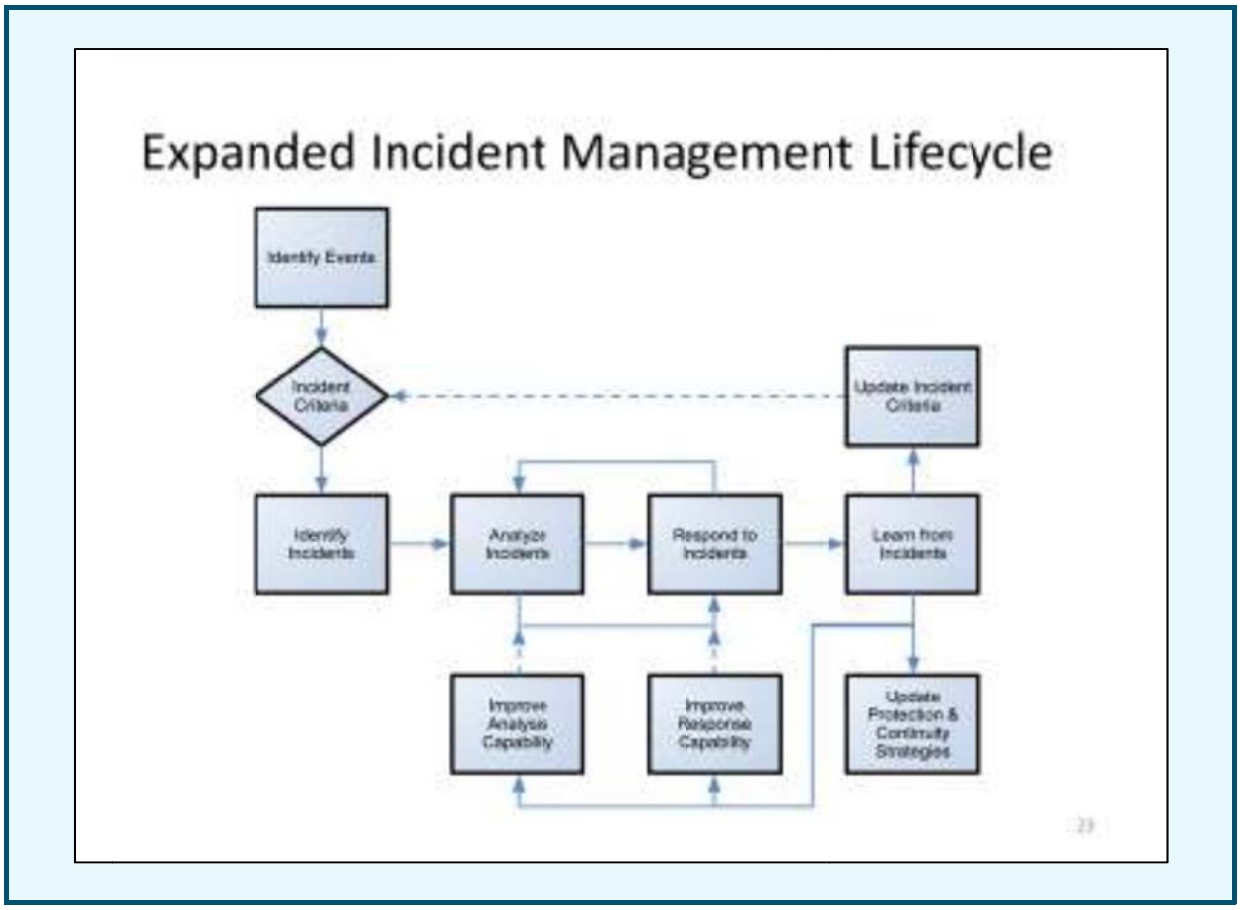
– Information systems and incidents that affect those critical infrastructure sectors identified in the National Cybersecurity Policy, if there is one;

– Incidents and threats that may affect systems in one or more sectors of critical infrastructure;

– Types of incidents or activity that may be of unique concern to national authorities because they may directly affect national security, result in revealing sensitive information, or even cause embarrassment to the nation;

– Incidents that substantially affect a majority of computer users in the general public;

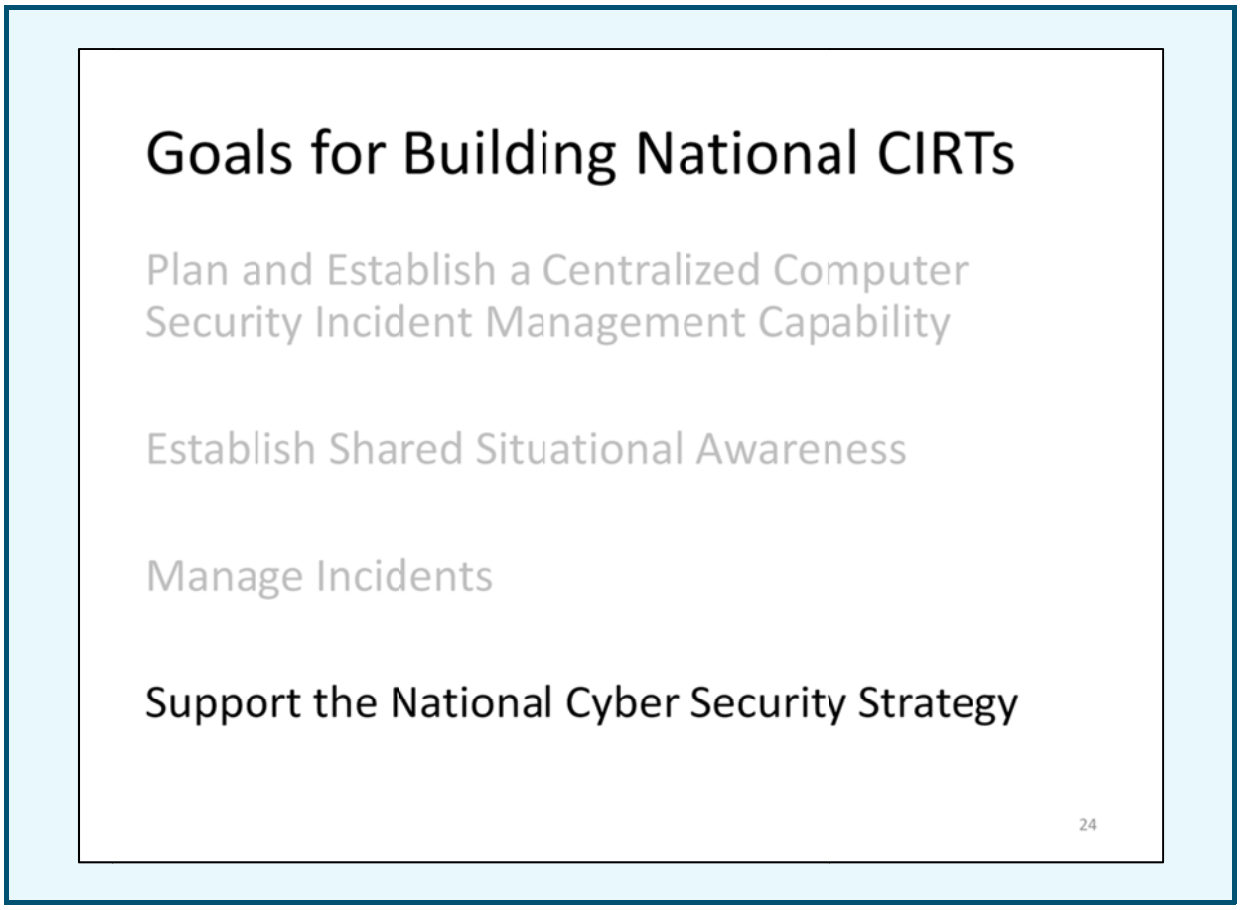
– Incidents that are part of greater or evolving threats.



For the National CIRT to efficiently and fairly handle reports, it should establish a clear, consistent workflow. Typical steps are documented here in the expanded incident management lifecycle.

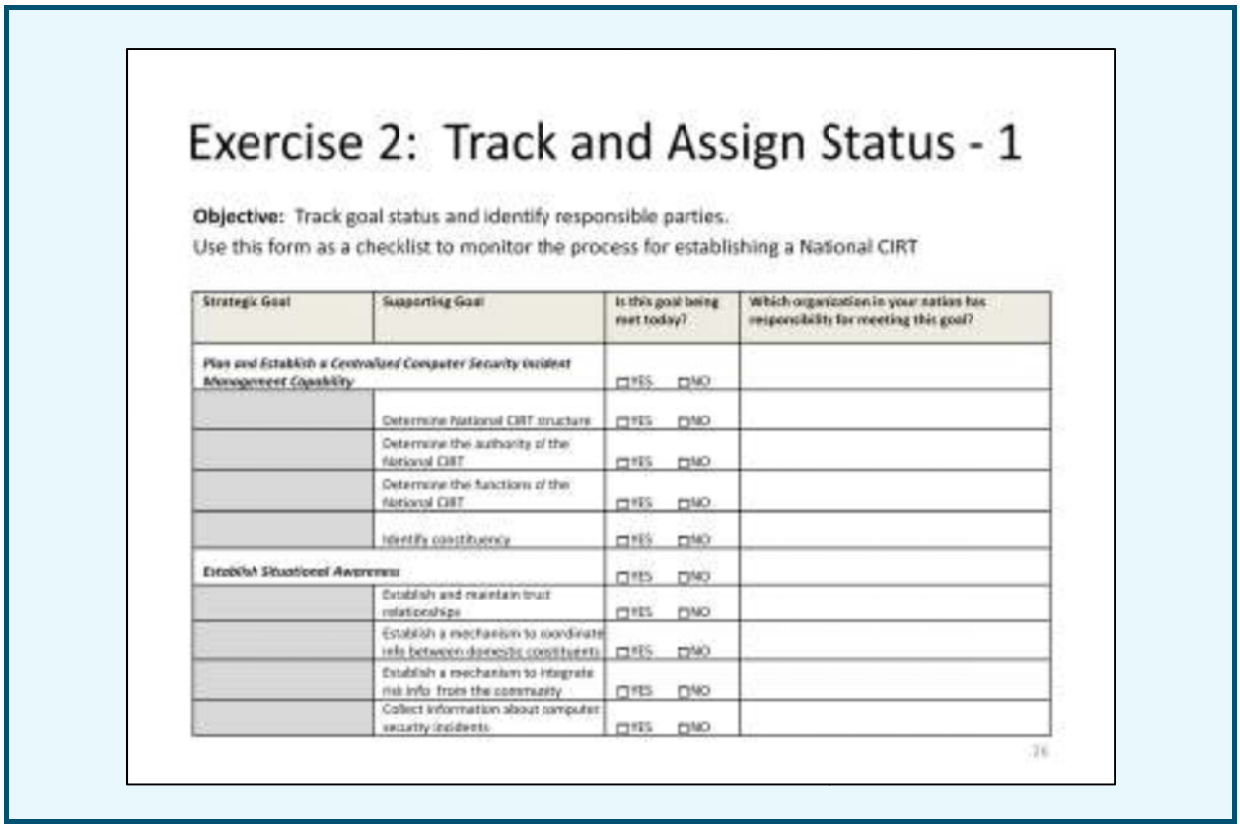
It is common to create and maintain standard operating procedures at each step in the workflow. Typical steps would include:

- Detect incidents
- Collect and document incident evidence
- Analyze and triage events
- Respond to and recover from incidents
- Learn from incidents



While organizations of all sizes will continue to perform internal cyber incident management, National CIRTs alone have the primary responsibility of addressing national level concerns. Translating National CIRT experiences in a way that is useful to policymakers, stakeholders, and the community of security practitioners enhances national cybersecurity. Translating experiences implies considering ways in which the National CIRT's work and the experiences of the community may have broader implications for national laws and policies. This translation can produce lessons learned, best practices, and improve problem avoidance and risk mitigation nationally, as well as influence national regulations, guidance, initiatives, and directives.

A National CIRT is uniquely situated to serve as a trusted, national focal point. By taking advantage of this position, a National CIRT can coordinate with all owners and operators of Information and Communication Technologies (ICT)(private and/or public) to gain a uniquely comprehensive perspective of the national cybersecurity landscape. This allows the National CIRT to support the national cybersecurity strategy, manage incidents of national concern, and support government operations most effectively. A National CIRT typically builds national cybersecurity capacity by publishing best practices and providing services, guidance, training, education, and awareness for the building of other organizational CIRTs.

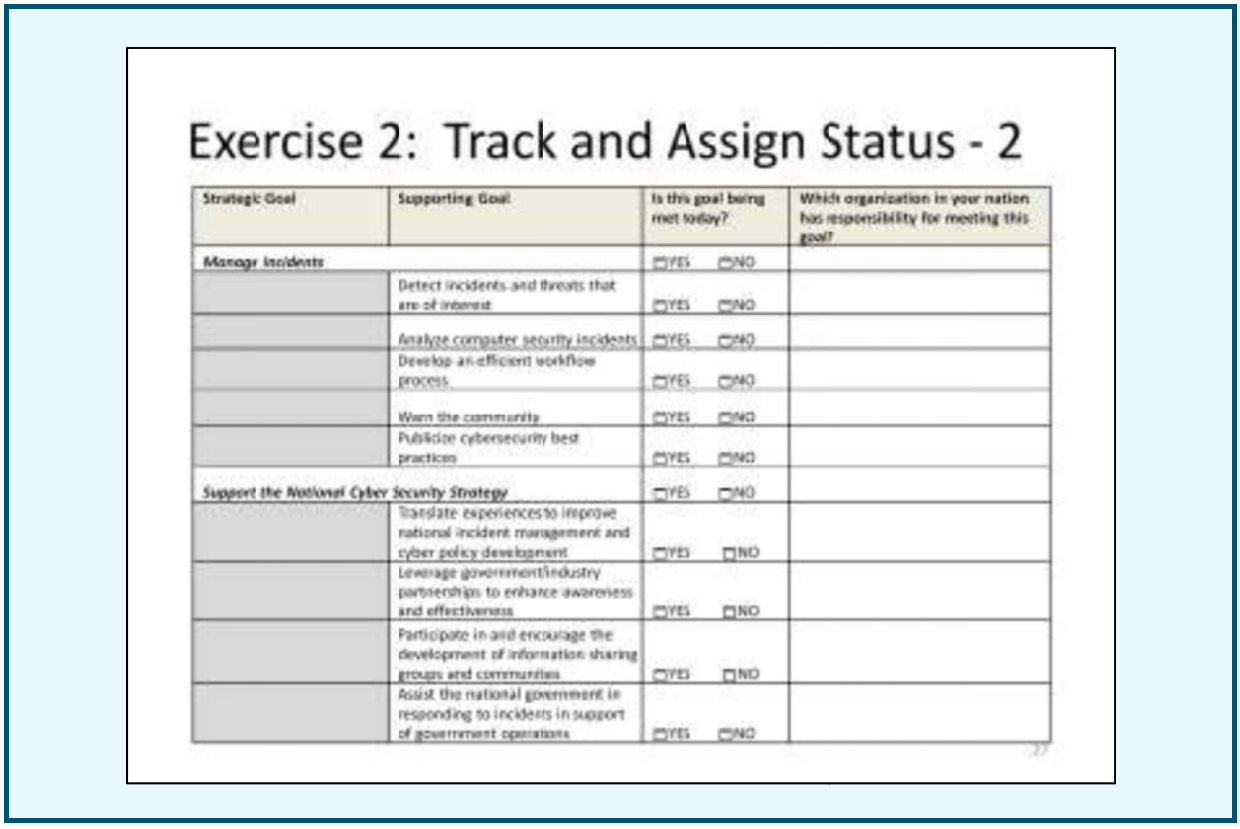


Exercise 2: Track and Assign Status - 1

Objective: Track goal status and identify responsible parties.
Use this form as a checklist to monitor the process for establishing a National CIRT

Strategic Goal	Supporting Goal	Is this goal being met today?	Which organization in your nation has responsibility for meeting this goal?
Plan and Establish a Centralized Computer Security Incident Management Capability		☐YES ☐NO	
	Determine National CIRT structure	☐YES ☐NO	
	Determine the authority of the National CIRT	☐YES ☐NO	
	Determine the functions of the National CIRT	☐YES ☐NO	
	Identify constituency	☐YES ☐NO	
Establish Situational Awareness		☐YES ☐NO	
	Establish and maintain trust relationships	☐YES ☐NO	
	Establish a mechanism to coordinate info between domestic constituents	☐YES ☐NO	
	Establish a mechanism to integrate risk info from the community	☐YES ☐NO	
	Collect information about computer security incidents	☐YES ☐NO	

This exercise involves a basic checklist to track the status of action items to develop a National CIRT.



Exercise 2: Track and Assign Status - 2

Strategic Goal	Supporting Goal	Is this goal being met today?	Which organization in your nation has responsibility for meeting this goal?
Manage Incidents		☐YES ☐NO	
	Detect incidents and threats that are of interest	☐YES ☐NO	
	Analyze computer security incidents	☐YES ☐NO	
	Develop an efficient workflow process	☐YES ☐NO	
	Warn the community	☐YES ☐NO	
	Publicize cybersecurity best practices	☐YES ☐NO	
Support the National Cyber Security Strategy		☐YES ☐NO	
	Translate experiences to improve national incident management and cyber policy development	☐YES ☐NO	
	Leverage government/industry partnerships to enhance awareness and effectiveness	☐YES ☐NO	
	Participate in and encourage the development of information sharing groups and communities	☐YES ☐NO	
	Assist the national government in responding to incidents in support of government operations	☐YES ☐NO	

Summary – Building a National CIRT

It is important to understand the context of national cyber security. The national context relates to the coordination of incident management and development of the national community's understanding of cyber security issues.

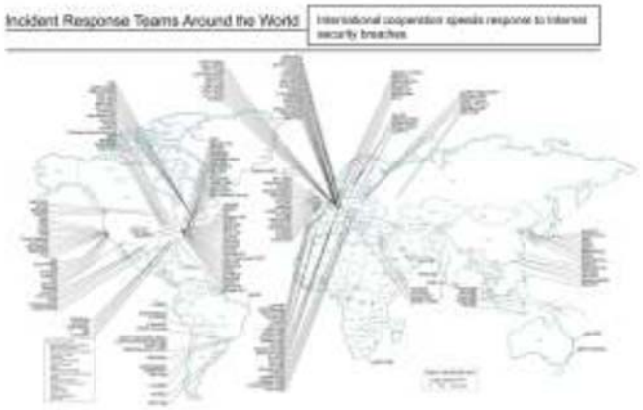
National CIRTs have a unique position and the roles they can take, likewise, provide unique information of great importance to the nation they serve.

The goals for building national CIRTs are intended to help interested parties create the right size and kind of organization to fit their unique needs.

28

NATIONAL CIRT MANAGEMENT

Incident Response Teams Around the World



29

Challenges Facing National CIRTs

National CIRTs are products of their environment.

- Political factors
- Structural factors
- Funding
- Internet penetration and use in the country
- Staffing and human resources

The overarching theme: It is very hard to generalize about National CIRTs. As discussed in the first section of this material, many of the key decisions made to stand up and operate a National CIRT depend on factors that are often unique to each situation.

No "one size fits all" Solutions

How might National CIRT activities vary?

- Between a CIRT with a $300,000 annual budget and $3 million?
- In an organization housed under the national police, or a self-standing telecommunications ministry?
- Between a CIRT that serves primarily the government and one serving privately owned critical infrastructure?
- Where most of the information held by the National CIRT is accessible to the public under a freedom of information law?
- Where only 20% of the population uses computers but 85% have smart phones?
- In a country with a long civil service tradition, or in a country with recent instability and distrust of the central government?
- In a country with a well-formed national cyber security strategy, or without?

31

One Tool That May Be Used

Critical Success Factors (CSFs) help identify

- Key activities where we must succeed
- The things that must go right
- The "vital few" areas

32

Introduction to Critical Success Factors - 1

First defined by John Rockhart of the Massachusetts Institute for Technology (MIT) Sloan School of Management.

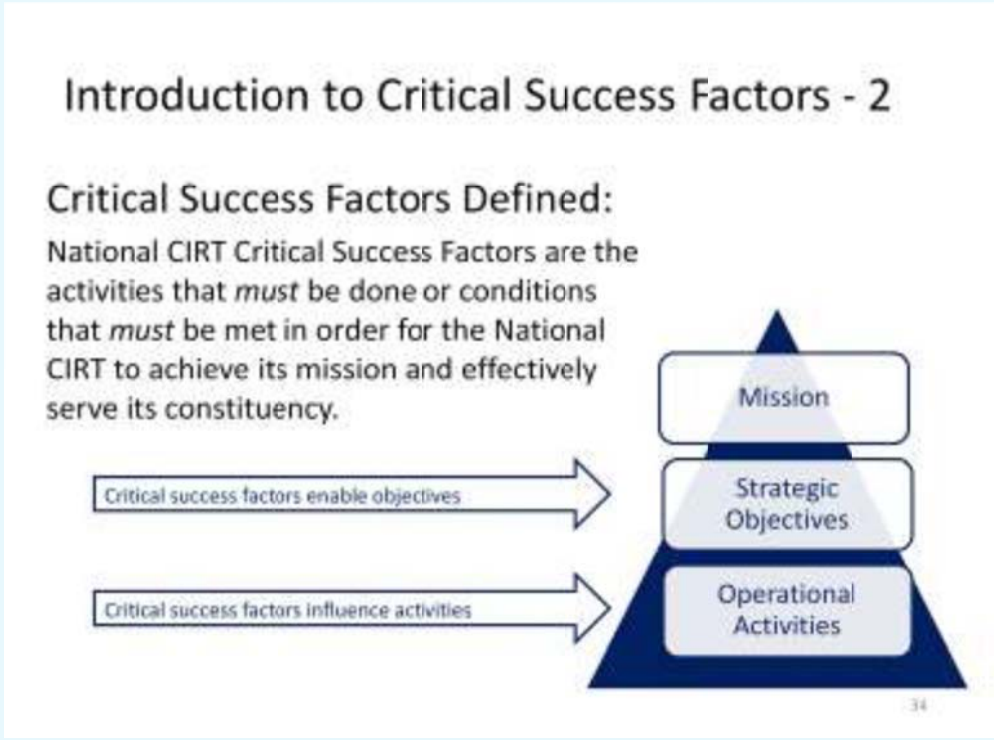
- "A Primer on Critical Success Factors" published by the Center for Information Systems Research in June 1981.
- Rockhart advocated using CSFs as a way for senior executives to better manage information systems
  - What information do executives require?
  - What services are critically important?
  - Where should my risk management focus be?
  - What types of activity should I measure?

33

The use of critical success factors started with the work of John Rockhart of the Massachusetts Institute for Technology (MIT) Sloan School of Management. This work originally involved helping organizations to identify information needs for senior executives.

It has also been applied to the question of helping senior IT managers (CIOs and CISOs, for example) to plan the use of information technology so that it supports business drivers across large organizations. Rockhart advocated using CSFs as a way for senior executives to better manage information systems.

"Critical success factors (CSFs) define key areas of performance that are essential for the organization to accomplish its mission. Managers implicitly know and consider these key areas when they set goals and as they direct operational activities and tasks that are important to achieving goals. However, when these key areas of performance are made explicit, they provide a common point of reference for the entire organization. Thus, any activity or initiative that the organization undertakes must ensure consistently high performance in these key areas; otherwise, the organization may not be able to achieve its goals and consequently may fail to accomplish its mission."



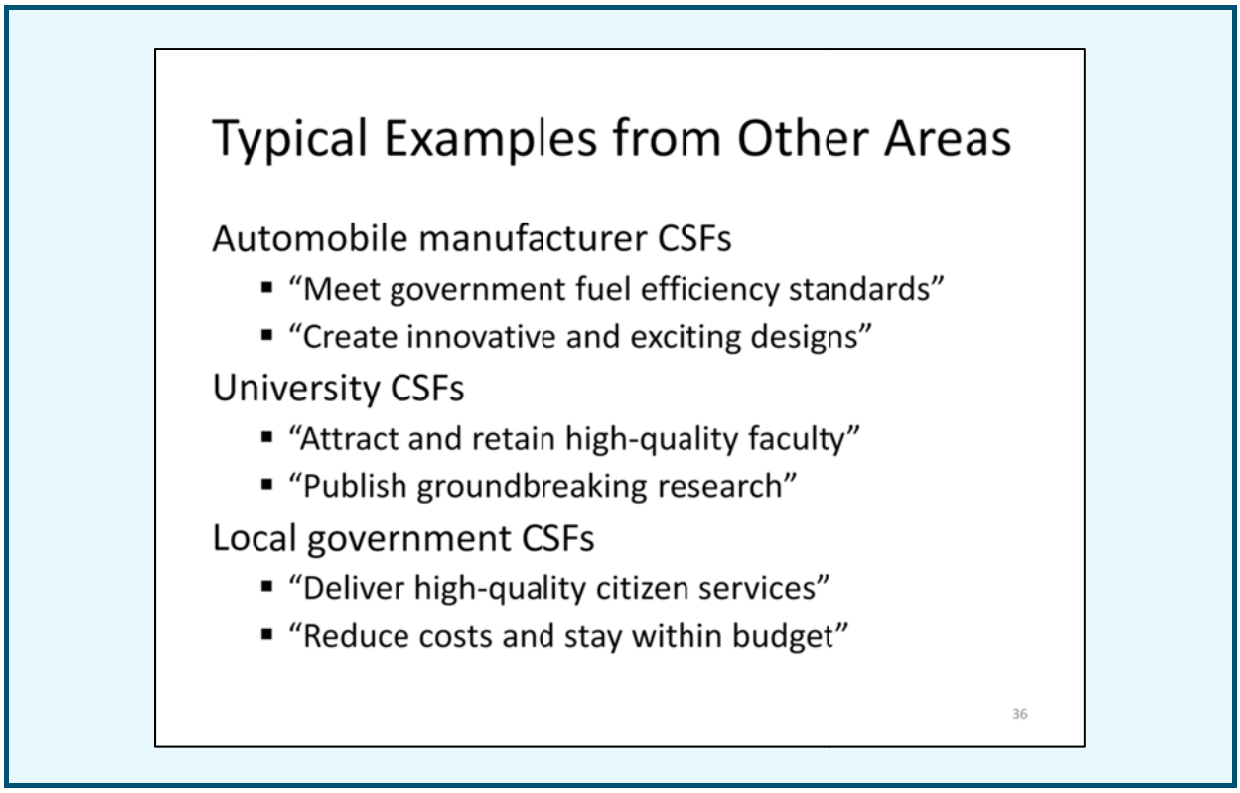
Critical success factors have been defined in different ways in the literature, including:

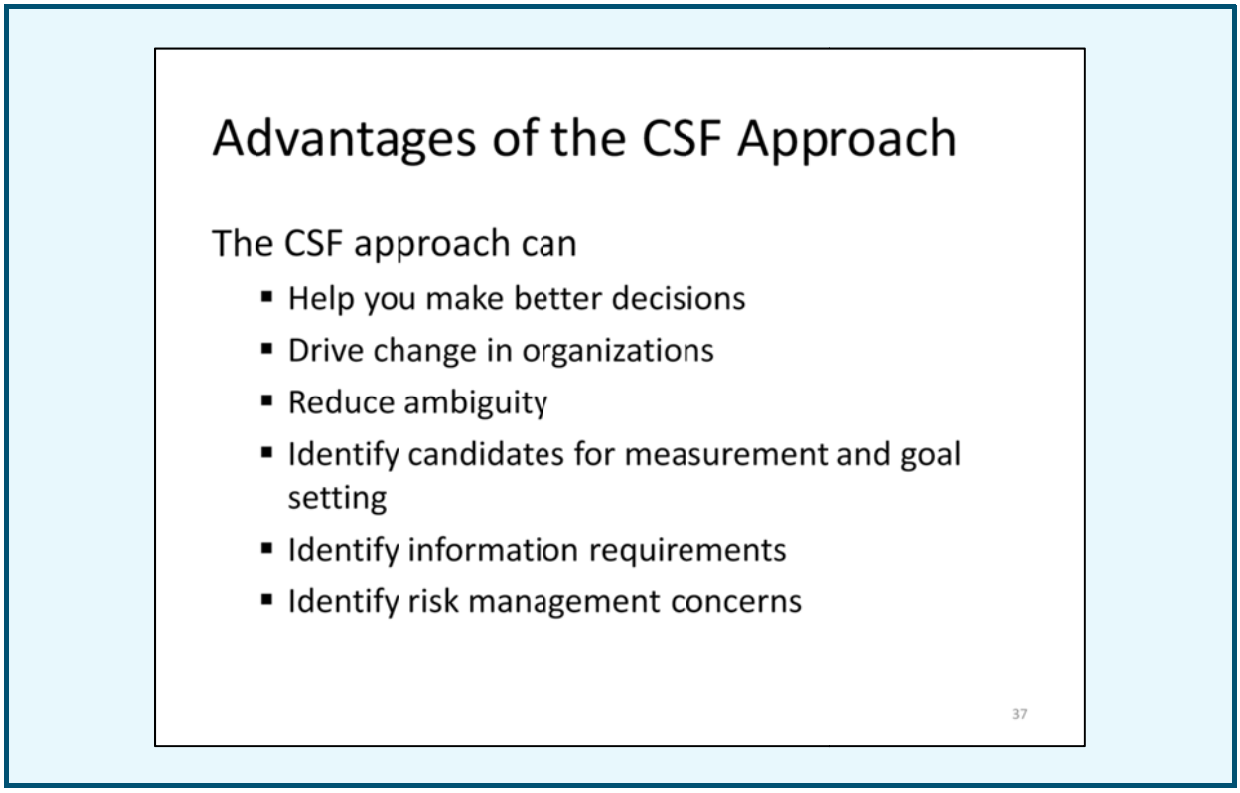
- Key activities in which favorable results are necessary to reach goals
- Key areas where things must go right for the business to flourish
- "factors" that are "critical" to the "success" of the organization
- A relatively small number of truly important areas.

These definitions share similarities. CFSs are the things that an organization must do or attributes the organization must have to achieve its mission. They have been described as things that "must be achieved in addition to the organization's goals and objectives.

Indeed, CSFs can be attributes or conditions such as “be a trusted partner”, “passion”, “shared ownership”, or “clear authority and responsibility”. In this sense, CSFs are not simply deconstructed or more granular versions of strategic goals.

It is important to understand the relationship and differences between CSFs and strategic goals, as they might initially seem to be interchangeable. Strategic goals are the higher level objectives that describe what the National CIRT must do to accomplish its mission (for example, “Protect the availability and confidentiality of information in government networks.”) These are typically fairly general statements that further describe and explain the mission of the organization. They provide little guidance to National CIRT managers about how to accomplish the strategic goal in the context of their unique operating environment. CSFs, on the other hand, help the manager or executive identify and understand the several important things that must be accomplished to meet the strategic goals and mission. These can then be operationalized into actionable activities. CSFs can, in turn, be used to generate performance goals that help the manager understand how well the organization is meeting its requirements.





These notes highlight a few of the items here.

Reducing ambiguity CSFs can help managers build agreement across their staff on the organization's purpose and activities. The process of identifying and implementing CSFs can help to foster

communication throughout teams by involving them in the discussion, helping the National CIRT have more confidence in the decisions made by management.

Identifying Candidates for Measurement and Goal Setting As stated above, a key aspect of managing any organization is measuring performance. However, measuring organizational performance involves costs and complicated questions. Gathering and analyzing information data can consume staff hours and require technology investment. What is to be measured? How often? Many organizations find measuring the right things difficult – or they measure only those activities that are simple to measure. Sometimes this uncertainty results in no or sub-optimal measurement of the organization's activity. Evaluating CSFs can provide clarity and direction on this question, ensuring that measurement and metrics help to produce optimal results.

Identifying Information Requirements Closely aligned with goal setting, CSFs can help managers identify what types of information they really need in order to understand the operations and health of their National CIRTs. Sometimes an objective, thorough evaluation of CSFs can identify information requirements that are not obvious. For example, the success of a National CIRT often hinges on how willing major constituents are to communicate incident and other information to the organization. An objective, formal examination of CSFs may indicate that whether the National CIRT is perceived as trustworthy or a technology leader in its community. Examining CSFs can lead the National CIRT manager to watch indicators and information that he or she may not have considered.

Identifying Risk Management Concerns CSFs can help identify the vital assets and services that support the organizational mission. This function can help a National CIRT identify which systems and assets should be subject to a risk management processes. This is common use of CSFs in many industries.

Advantages of a CSF Approach

	Without considering CSFs	Conclusion with a CSF analysis
Processes	"We have a basic process to respond to incidents."	"We realize we are missing important information in our process that we need to achieve success. We need to modify our process."
Ambiguity	"We know we want to do network monitoring of certain assets, because monitoring is very important."	"We will do netflow analysis only on public facing sites - rather than full packet capture - because we've identified respect for privacy and regulatory compliance as a critical success factor."
Skill sets	"We know we generally need technical skills, but I am unsure about specific job descriptions."	"I have a better idea of which skills I need my staff to have because I can compare the existing skills we have to our critical success factors to identify gaps."
Measurement	"We have posted 100 general advisories on our web page this month."	"We have measured information about phishing directed at our national banks and provided this information to the banks because supporting key sectors of the economy like banking is a critical success factor."

38

Sources of CSFs

- National cyber security strategy
- Constituency
- Peer community
- Governing organizations
- Laws
- Political or structural considerations
- Resource constraints

39

Critical Success Factors

Identifying Critical Success Factors (CSFs) for an Organization

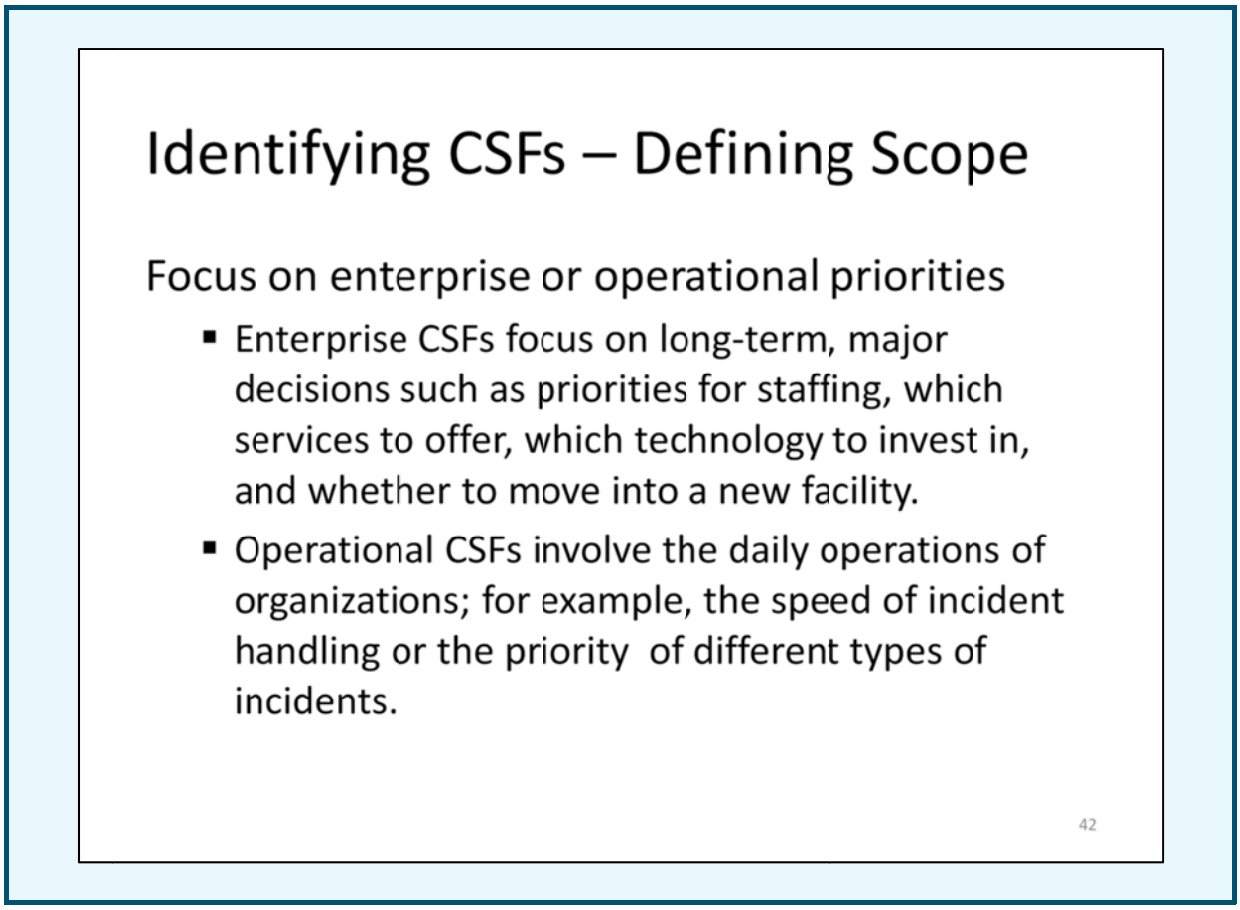
Using Critical Success Factors in National CIRT Management

40

Detailed materials are available about the process of identifying and refining CSFs. This section serves as a primer on this topic, describing a process for identifying CSFs in the context of National CIRTs. The intent is to give National CIRT managers an understanding of the formal process that drives development of CSFs.

Deriving CSFs is accomplished through activities that take the form of workshops and working sessions. The personnel that facilitate this work are selected by management based on various traits, such as their ability to think objectively about the organization, their leadership ability, their understanding of the organization, and their communication ability, among others. There are four phases to the identification and refinement of CSFs for National CIRTs. These are

– Defining Scope
– Collecting Data
– Analyzing data
– Deriving CSFs.



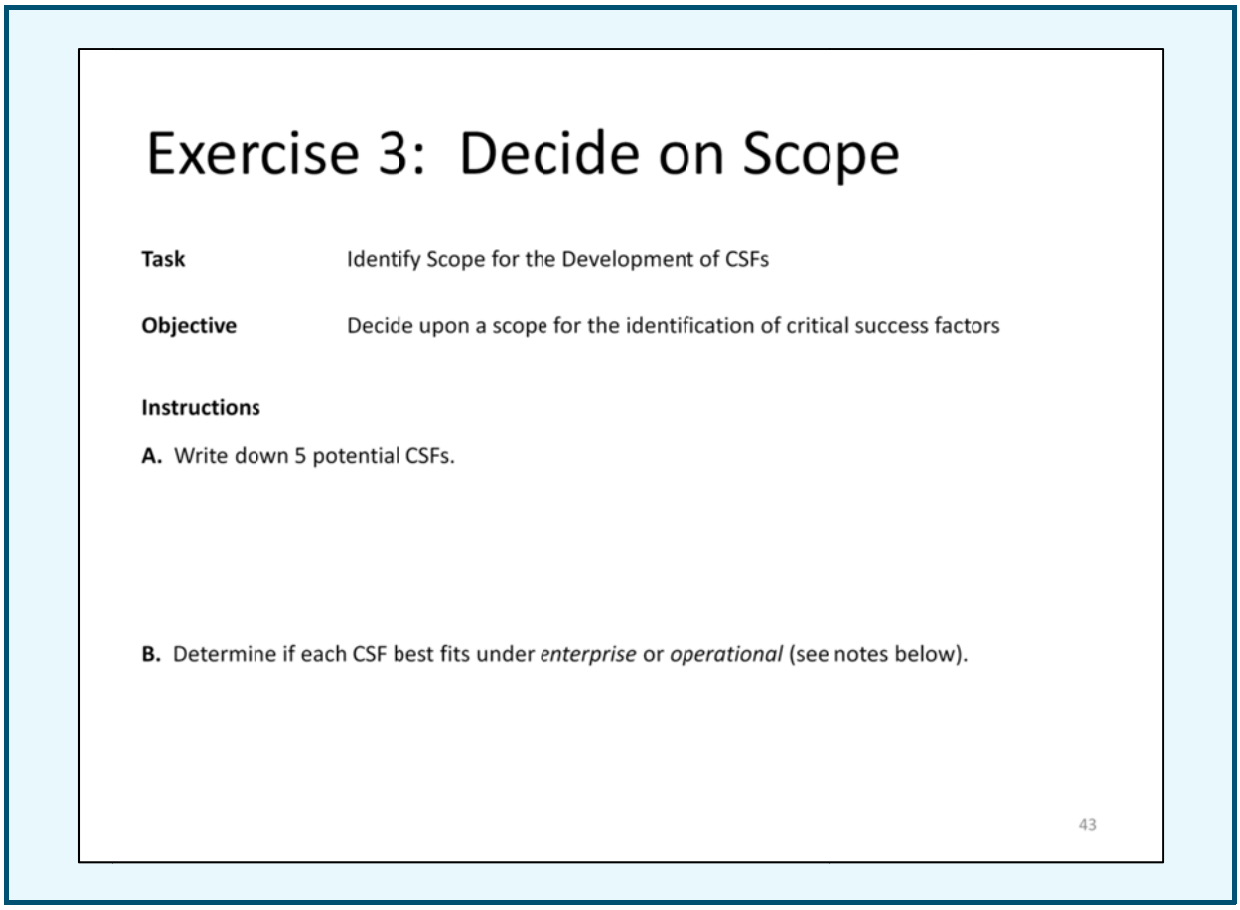
Defining Scope

Defining scope ordinarily involves an analysis of whether the task of collecting CSFs is focused on enterprise priorities for the organization or on operational activities.

Enterprise CSFs focus on long-term, major decisions such as priorities for staffing, which services to offer, which technology to invest in, or whether or not to move into a new facility. By contrast, operational CSFs involve the daily operations of organizations. For a National CIRT, operational CSFs may involve the speed of incident handling or the priority for handing different types of incidents.

Many organizations, especially large firms with many subsidiary divisions and departments, start their CSF process at the enterprise level, for the sake of simplicity.

However, for smaller organizations or organizations with a flat organizational structure – where there are few organizational layers between managers and workers – collecting both enterprise and operational CSFs at the same time can be effective. Many of the small teams that comprise National CIRTs share these characteristics and can feasibly derive CSFs in one exercise, with no distinction between enterprise and operational CSFs.

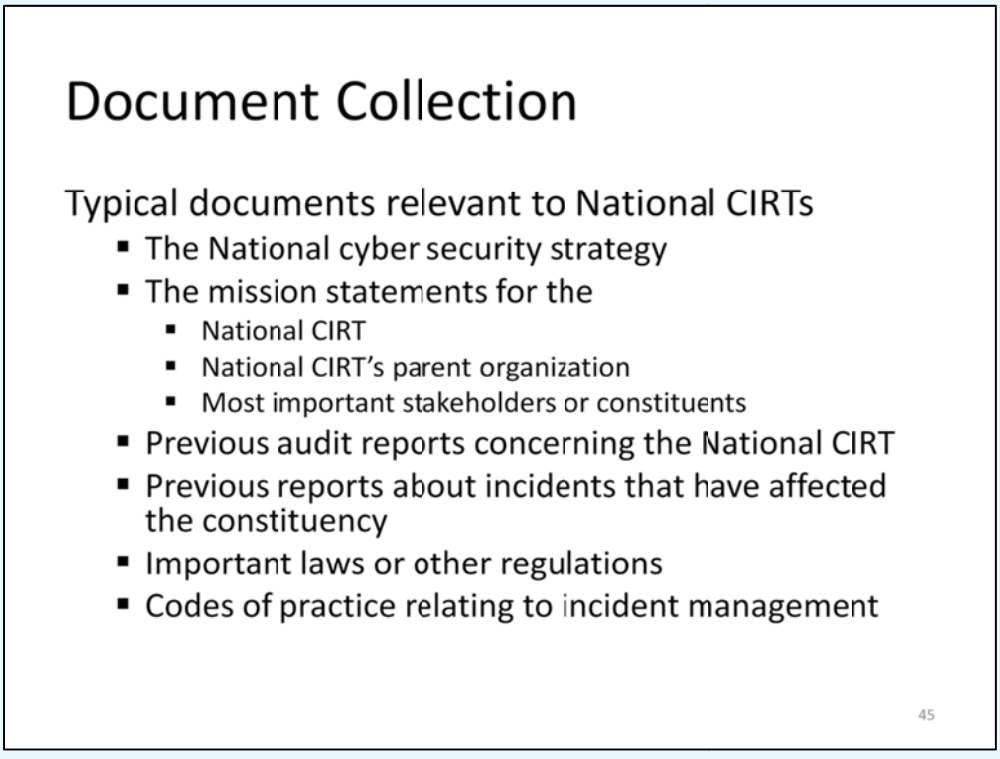


Defining scope usually involves deciding whether the task of collecting CSFs focuses on enterprise priorities for the organization or on operational activities.

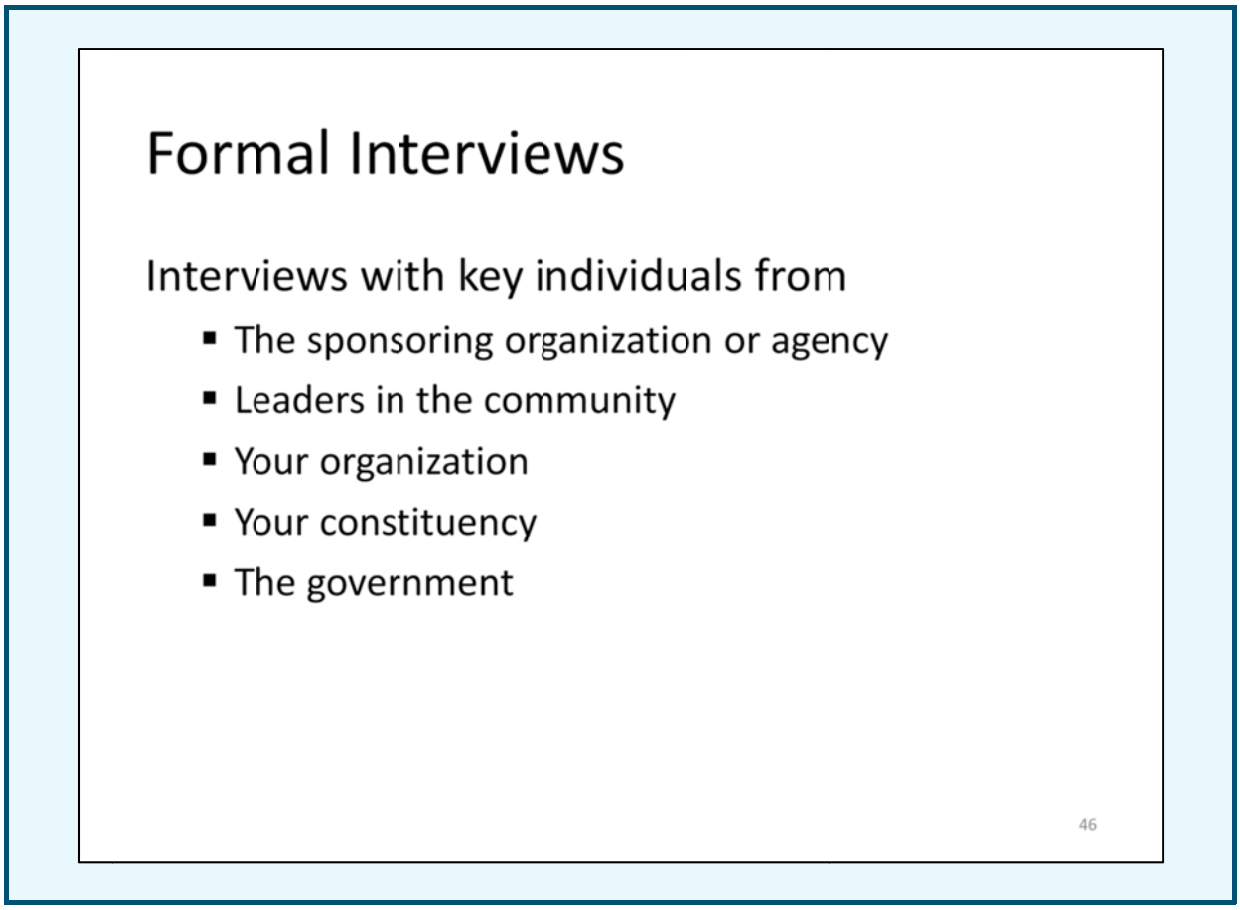
Enterprise CSFs focus on long-term, major decisions, such as priorities for staffing, which services to offer, which technology to invest in, or whether or not to move into a new facility.

By contrast, operational CSFs involve the daily operations of organizations. Operational CSFs may involve the speed of incident handling or in what priority different types of incidents should be handled.

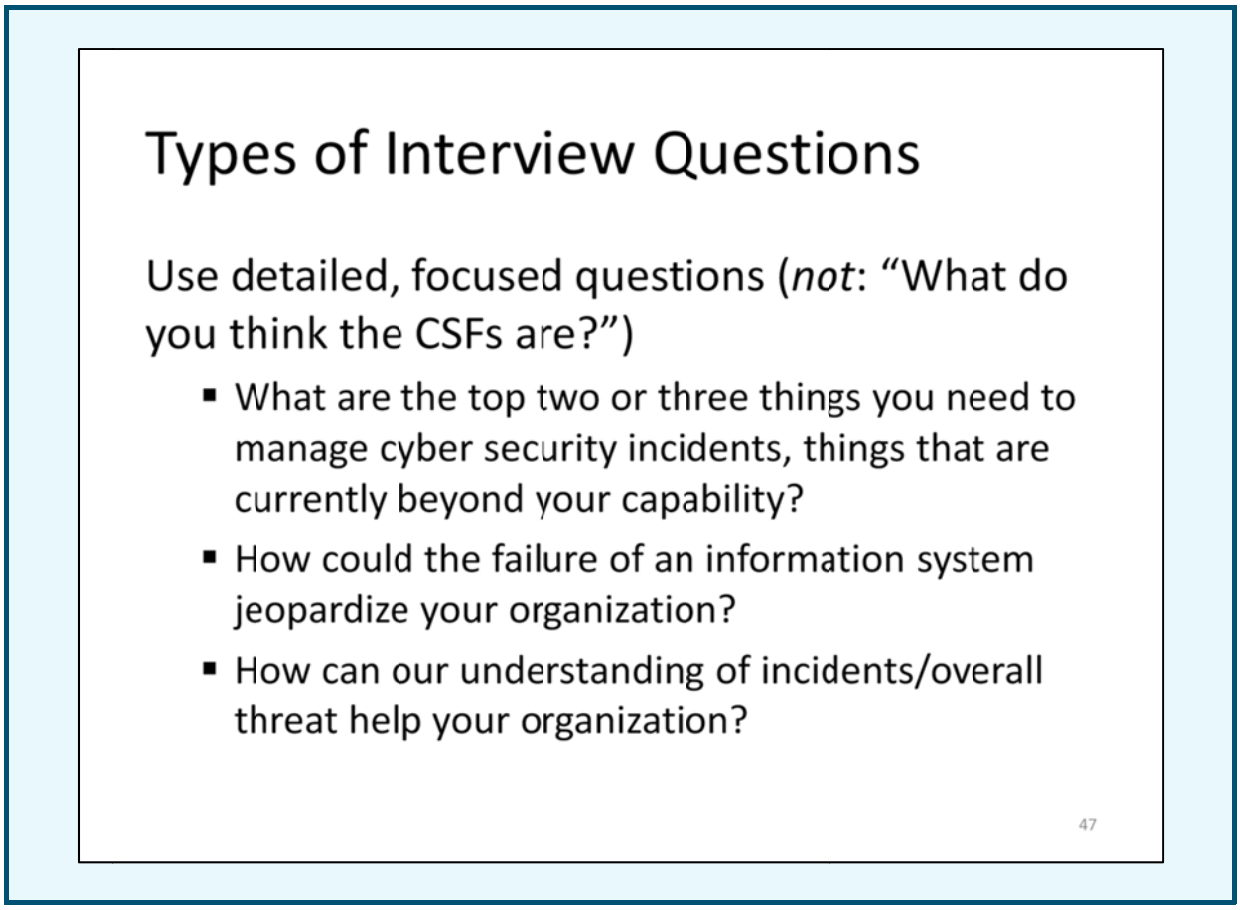
Collecting data to develop CSFs is done in two primary ways, document collection and interviews of key personnel.



Document collection normally involves gathering important documents that provide information about the essential factors that affect the National CIRT's mission. These types of documents are typical.



Of the two collection methods, interviewing is typically the more productive method. Interviewing managers, employees, constituents, and other stakeholders provides the opportunity to reach agreement and understand what is truly important for the operation of the organization. Also the interactive process of an interview allows for participants to guide the process and expose areas of concern and other nuances in a way that reviewing documents usually does not.



For CSF interviews to be productive, the right people must participate in the event, and forethought should be put into the interview questions. For instance, while simply asking a constituent "What are your Critical Success Factors?" might yield useful information, probing or open-ended questions can be more beneficial.

Exercise 4: Data Collection

Task

Identify documents and interview subjects for the collection of data to identify CSFs for your organization.

Objective

Understand data collection for a CSF process. *Collecting data to develop CSFs is dore in two primary ways*: document collection and interviews of key personnel.

Potential sources of critical success factors for National CIRTs include

- The organization's constituency
- Governing or sponsoring organizations
- Peer organizations
- Laws and regulations
- The political environment

Instructions

A. Considering the possible sources of CSFs listed above, record ten possible documents to be analyzed for critical success factors.

B. Considering the possible sources of CSFs listed above, record ten possible interviewees for the identification of critical success factors. Identify specific individuals and their organizations.

48

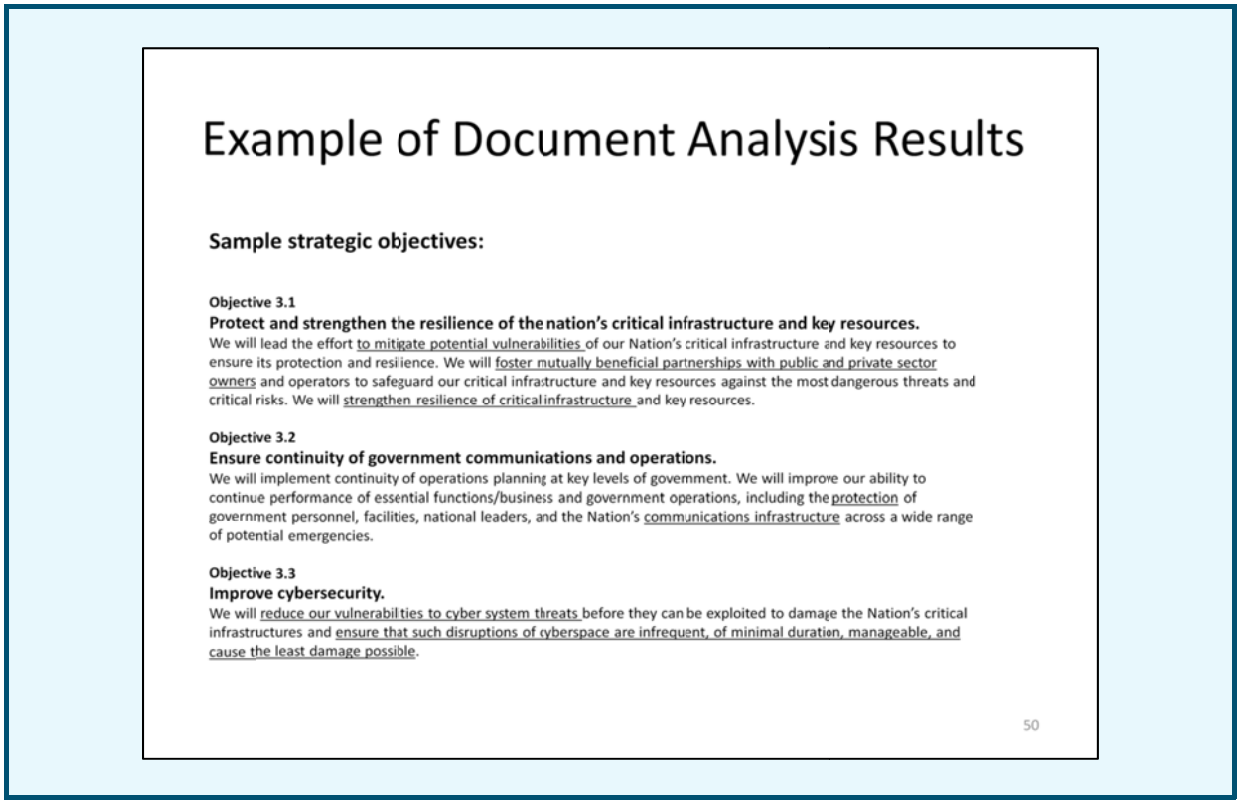
Analyzing Data

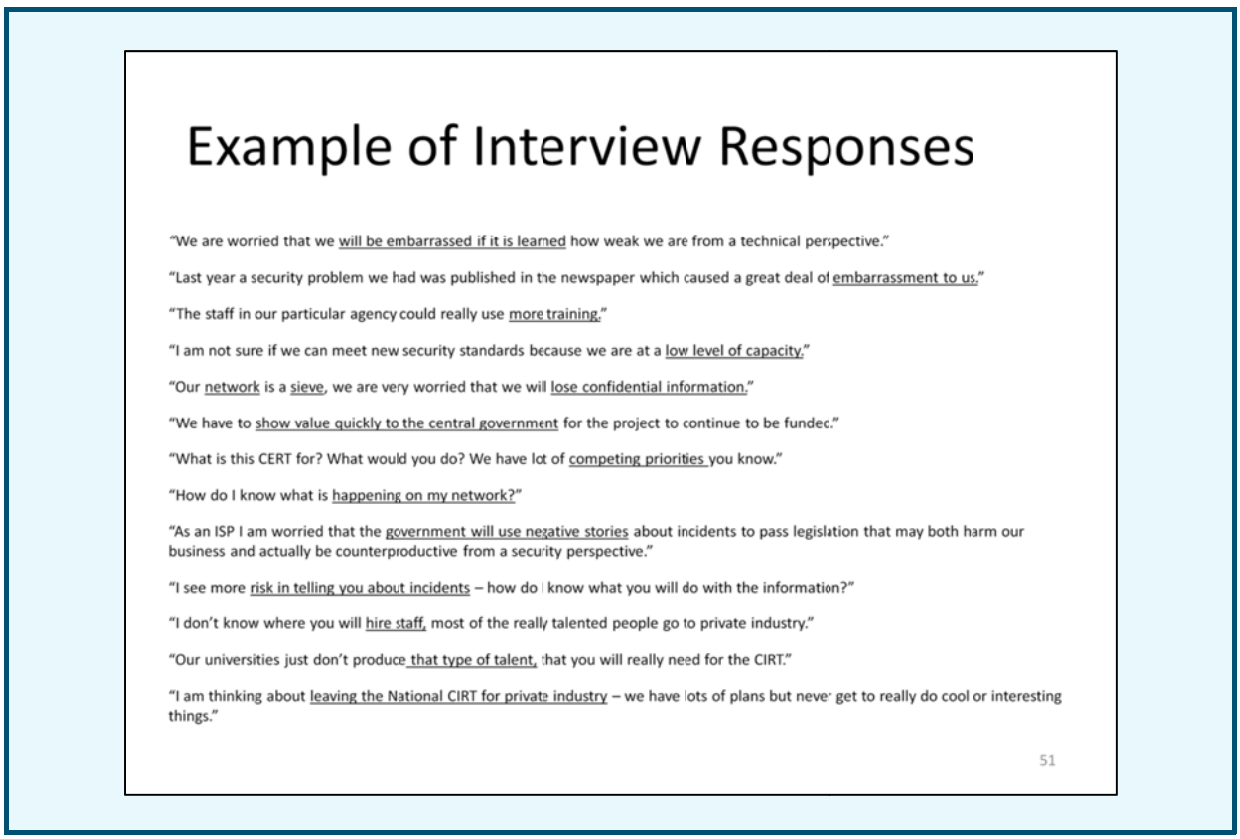
Documents and interview responses are examined to identify similar ***themes***.

Themes are ideas, statements, or activities that seem to recur throughout the documents or responses.

49

After data is collected, it must be **analyzed**. During the analysis phase, documents and interview responses are examined to identify similar themes. Themes are ideas or activities that seem to recur throughout the documents or responses.





Deriving Themes and CSFs

Activities and Statements	Themes
Mitigate potential vulnerabilities	Limiting vulnerabilities and potential disruption to critical infrastructure
Minimal, manageable disruption	
Strengthen critical infrastructure	Partnering with private owners of critical infrastructure
Partnerships with industry	
"We will be embarrassed if it is learned . . ."	Maintaining confidentiality is important Some constituents may see risk not only in the incident or disruption, but also in notifying a central authority
". . . If we lose confidential information . . ."	
"risk in telling you about incidents"	
"what type of talent"	Finding and keeping the right talent will be an issue
"staff leaving CIRT for private industry"	
"competing priorities"	We will need to provide measurable, specific results to merit investment and expansion
"limited capacity"	

52

Deriving themes involves grouping similar statements from documents and interview responses into like categories.

Deriving CSFs

Themes identified during analysis are refined to develop concise, unique critical success factors.

Sample CSFs

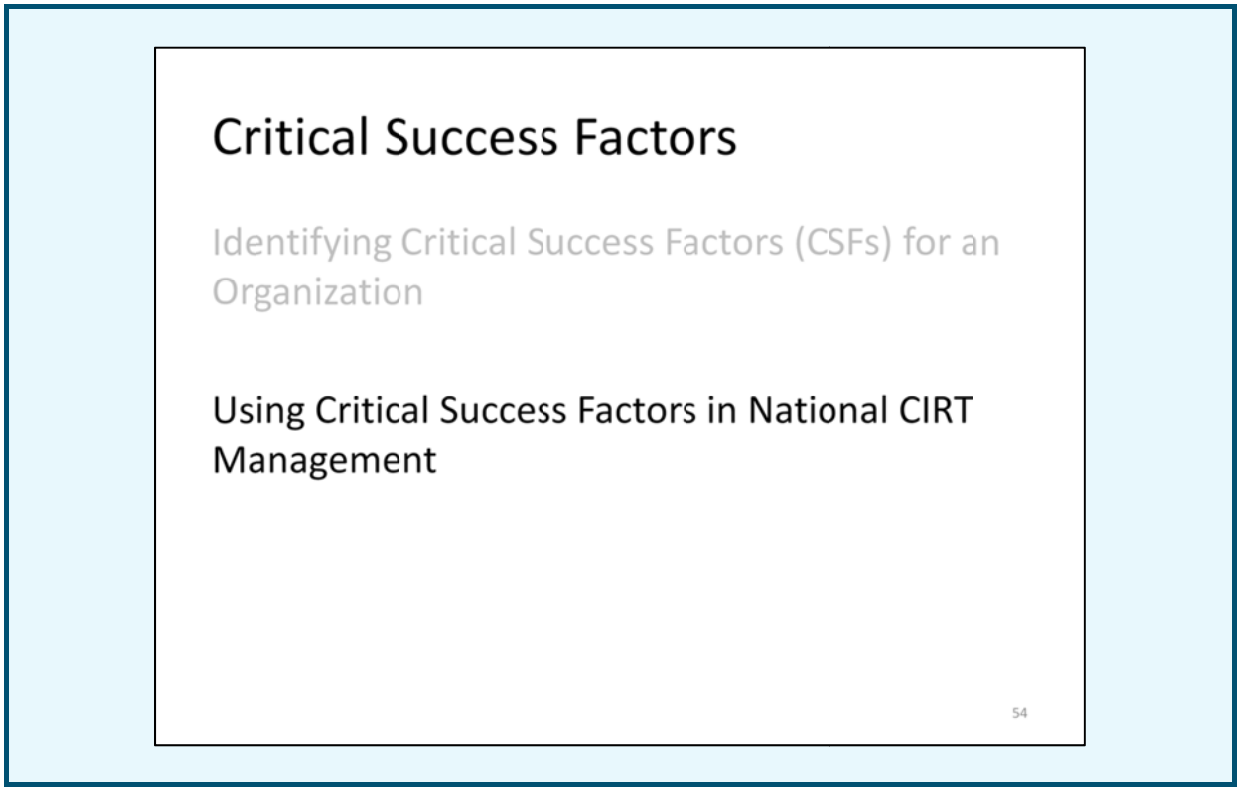
- Unauthorized traffic in government networks must be detected
- Incident information provided by constituents must be protected
- Vulnerabilities in critical infrastructure must be mitigated
- The CIRT must provide measurable results to the central government
- The CIRT must attract and retain quality staff

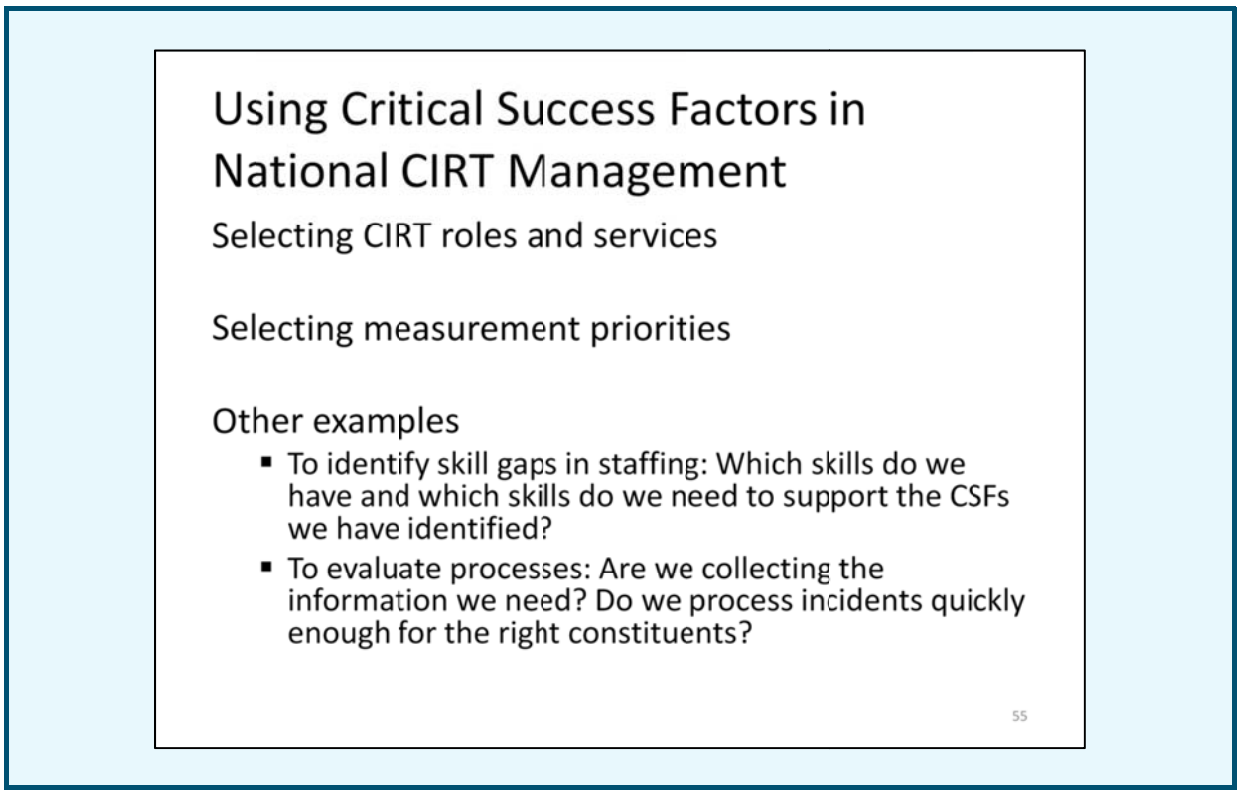
53

Deriving CSFs involves taking the themes identified during analysis and further refining them to develop concise, unique CSFs that describe the critical areas where the National CIRT must perform in order to

satisfy its mission. Refinement of the themes involves grouping them together by their similar characteristics and expressing what the theme means to the organization as concisely as possible. This process is repeated to eliminate candidate CSFs that are unclear or duplicative.

Once CSFs are identified, they must be implemented to be useful. The following section gives two examples of how CSFs can be used to support National CIRT management.





National CIRTs can use CSFs in ways similar to many IT-centric organizations. For instance, CSFs can be used to help manage security and resilience by helping managers understand what services and assets are truly important and need to be secured. They can also help managers determine the relative priority of securing various assets. Closely related to this question, CSFs can be used to help determine the scope for risk assessments. Risk assessment can be a labor- and time-intensive process. Consequently, having a formal process to identify important services, and their related assets, is essential for making risk assessment fruitful. Finally, CSFs can be used to help managers identify the resilience requirements (confidentiality, integrity, and availability) that support information assets.

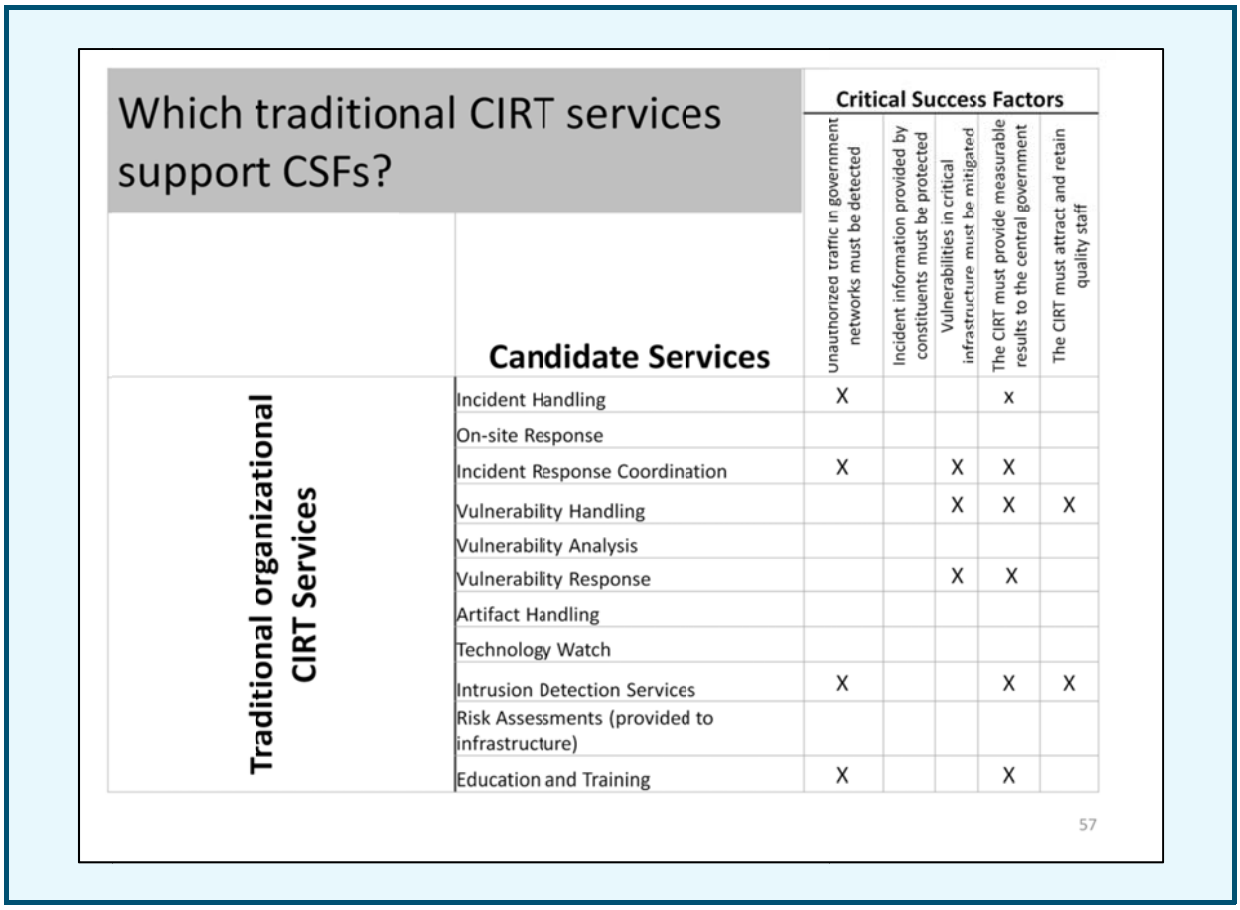
Selecting roles and services; Which National CIRT roles support CSFs?

	Candidate Services	Critical Success Factors: Unauthorized traffic in government networks must be detected	Incident information provided by constituents must be protected	Vulnerabilities in critical infrastructure must be mitigated	The CIRT must provide measurable results to the central government	The CIRT must attract and retain quality staff
Typical National CIRT Services	Detection of Intrusion Sets					
	Advise the National Government on Cybersecurity Matters					X
	Assess National Readiness and Crisis Management Capability			X		
	National Alert and Warning			X	X	
	Organizational CIRT Capacity Building	X		X	X	
	Trusted Point of Contact and Coordinator			X	X	
	Build Cybersecurity Culture					

56

Affinity analysis is usually performed by constructing a comparison matrix that allows CSFs to be compared and correlated with various criteria. In the example on this slide, it is Candidate Services.

The purpose of constructing a comparison matrix is to identify the relationship between some criteria and the CSFs. For instance, in this simple example, CSFs are compared to Candidate Services in a hypothetical National CIRT to determine which Candidate Services support which critical success factors.



Which traditional CIRT services support CSFs?

	Candidate Services	Critical Success Factors: unauthorized traffic in government networks must be detected	Incident information provided by constituents must be protected	Vulnerabilities in critical infrastructure must be mitigated	The CIRT must provide measurable results to the central government	The CIRT must attract and retain quality staff
Traditional organizational CIRT Services	Incident Handling	X			x	
	On-site Response					
	Incident Response Coordination	X		X	X	
	Vulnerability Handling			X	X	X
	Vulnerability Analysis					
	Vulnerability Response			X	X	
	Artifact Handling					
	Technology Watch					
	Intrusion Detection Services	X			X	X
	Risk Assessments (provided to infrastructure)					
	Education and Training	X			X	

57

As is often the case with an analysis using CSFs, the formal process does not yield results that are entirely unexpected. For example, based on historic and anecdotal information, it is often the case that acting as a trusted coordinator is a basic service that broadly supports a variety of functions. However, a formal analytical process helps to foster agreement among managers, stakeholders, and major constituents.

Identifying Measurement Priorities

Critical Success Factors	Candidate Information Requirement
Unauthorized traffic must be detected in government networks	Number of incidents year to date involving beaconing to a compromised or malicious host
	False positive rate for event detection rules
	Percentage of government access points being monitored
	Frequency of updating event detection criteria
Incident information provided by constituents must be protected	Information security audits conducted and status of recommendations
	Number of exceptions to policy requiring prior authorization of incident reporter before release of information
Vulnerabilities in critical infrastructure must be mitigated	Number of incidents voluntarily reported by private industrial constituents
	Number and trending of private industry inquiries to the National CIRT about emerging security threats
	Number of discrete vulnerabilities collected and reported to infrastructure organizations per month
The CIRT must attract and retain quality staff	Disparity in wage between CIRT staff and private industry workforce
	Staff turnover rate
	Results of employee satisfaction surveys

58

Another area in which CSFs can be helpful is identifying measurement priorities for National CIRT managers. Executives in any organization are often faced with a broad variety of information in the form of reports about activity in their organizations. However, in many cases this information is either irrelevant or not helpful to managers trying to determine the health of their organization and whether or not it is accomplishing its mission.

Reports may often be primarily intended for other parts of the organization or to facilitate general business functions. In a for-profit business, these may take the form of accounts receivable reports or sales reports about a particular item. In some organizations, there is little effort aimed at providing leadership with timely, tailored information about the health of the organization. Sometimes it is assumed the operational and working environment changes so rapidly that formalized reporting about the organization's health is not practical, or that it's preferable for managers to determine the state of their organization simply by talking to their staff and customers.

While leaders are usually very interested in knowing the health of their organization, there are costs to measuring intangible aspects of organizational performance. These usually take the form of labor hours and opportunity cost. Therefore, the information requirements for organizational leaders should be identified carefully. CSFs provide a useful way to identify these requirements.

Exercise 5: Apply CSFs - 1

Task

Given a set of CSFs, apply them to make decisions about CIRT services and measurement priorities

Objective: Decide what is needed to support a given CSF.

The purpose of identifying CSFs is to help National CIRT managers understand their operations and environment, and make better decisions. National CIRTs can use CSFs in ways similar to many IT-centric organizations. For instance, CSFs have been used to help managers prioritize services and assets based on importance and need for security. CSFs are ideal for driving and directing activities like risk management in large organizations, for example.

Instructions:

You are given the followirg CSFs:

- Contracts with the private vendors of the national government network infrastructure must be managed to ensure security.
- Government websites must be protected from damaging DDOS attacks launched by hacker groups.
- The National CIRT must provide tips and advice to help the public understand the internet's benefits and risks.
- The National CIRT must build relations with similar institutions in other countries
- The National CIRT must be seen as an impartial asset for all of the government.

59

Exercise 5: Apply CSFs - 2

Part 1: Define Services

Review slides 7, 8, 14, 17, 18 for the CIRT services and roles of a National CIRT. Also, this embedded CIRT Services .pdf from http://www.cert.org/csirts/services.html includes more detailed information.

After reviewing possible CIRT services, complete the charts on the next two pages by answering the following question for each service or role listed:

A. Does the service or role directly support the achievement of the critical success factor listed?

B. If it does, signify this by placing an X at the intersection of the service and the Critical Success Factor.

C. After completing the chart, list three services that would support the CSFs given.

A .pdf version of http://www.cert.org/CIRTs/services.html is embedded in this slide.

Exercise 5: Apply CSFs - 3

		Critical Success Factors				
	Candidate Services	Contracts with the private vendors of the national government network infrastructure must be managed to ensure security.	Government websites must be protected from damaging DDOS attacks launched by hacker groups.	The National CIRT must provide tips and advice to help the public understand the internet's benefits and risks	The National CIRT must build good relations with similar institutions in other countries	The National CIRT must be seen as an impartial asset for the government.
Traditional organizational CIRT Services	Incident Handling					
	On-site Response					
	Incident Response Coordination					
	Vulnerability Handling					
	Vulnerability Analysis					
	Vulnerability Response					
	Artifact Handlirg					
	Technology Watch					
	Intrusion Detection Services					
	Risk Assessmerts (provided to infrastructure)					
	Education and Training					

61

Exercise 5: Apply CSFs - 4

		Critical Success Factors				
	Candidate Services	Contracts with the private vendors of the national government network infrastructure must be managed to ensure security.	Government websites must be protected from damaging DDOS attacks launched by hacker groups.	The National CIRT must provide tips and advice to help the public understand the internet's benefits and risks	The National CIRT must build good relations with similar institutions in other countries	The National CIRT must be seen as an impartial asset for the government.
Typical National CIRT Roles	Detection of Intrusion Sets					
	Advise the National Government on Cybersecurity Matters					
	Assess National Readiness and Crisis Management Capability					
	National Alert and Warning					
	Organizational CIRT Capacity Building					
	Trusted Point of Contact and Coordinator					
	Build Cybersecurity Culture					

62

Exercise 5: Apply CSFs - 5

Part II: Define Measurement Priorities

Given the Critical Success Factors identified above, devise a potential measurement to support each of the CSFs. The measurements you identify must:

1) Be understandable for staff collecting or obtaining the measurement as well as to the consumer of the information.

2) Describe in quantitative terms the degree to which the CSF is being achieved (numbers or percentages).

For example:

CSF: *Contracts with the private vendors of the national government network infrastructure must be managed to ensure security.*

Measure: % of proposed contracts reviewed over the last quarter for security controls (or other required security language).

Exercise 5: Apply CSFs - 6

Critical Success Factors	Candidate Information Requirement
Contracts with the private vendors of the national government network infrastructure must be managed to ensure security.	
Government websites must be protected from damaging DDOS attacks launched by hacker groups.	
The National CIRT must provide tips and advice to help the public understand the internet's benefits and risks	
The National CIRT must build good relations with similar institutions in other countries	
The National CIRT must be seen as an impartial asset for all of the government.	

64

Summary – National CIRT Management

Identifying critical success factors for a National CIRT can help management

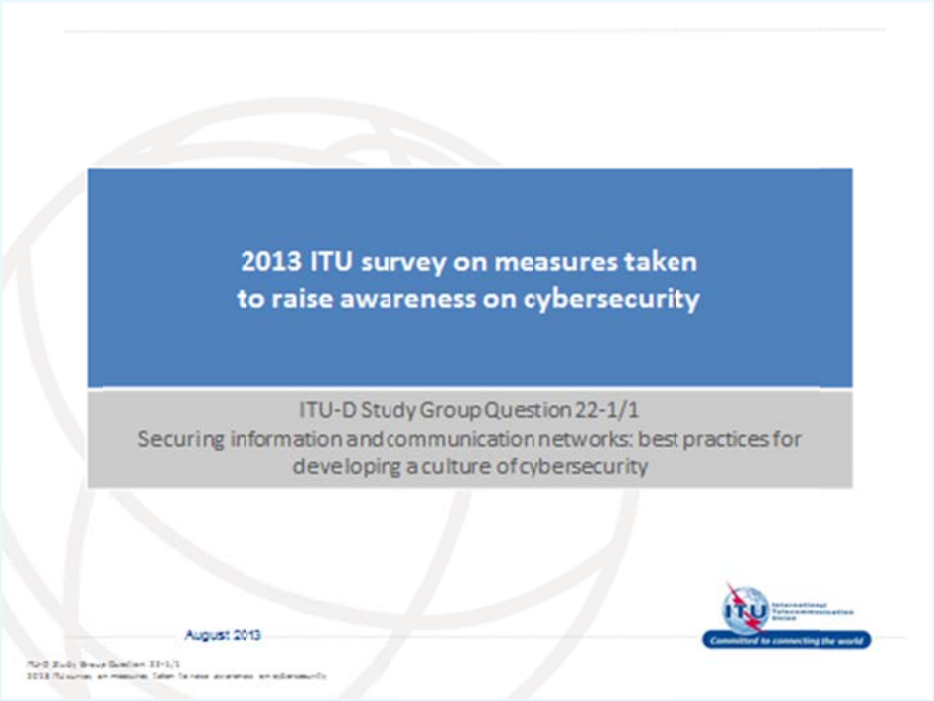
- Form the mission statement, strategic objectives, operational activities, and services
- Identify measurement and reporting priorities
- Gain support from stakeholders and staff

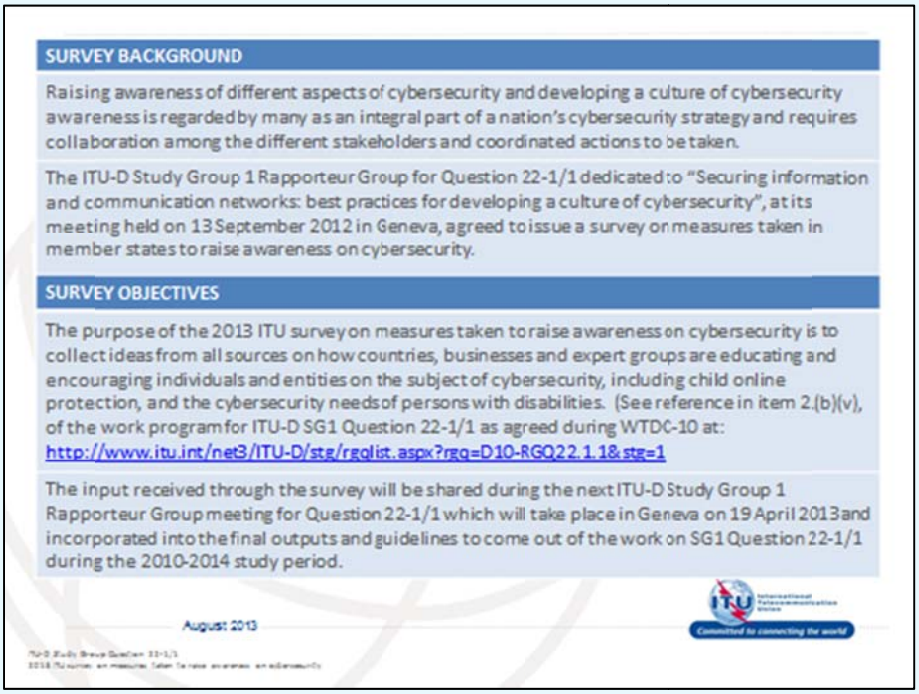
Identifying CSFs takes serious effort and time.

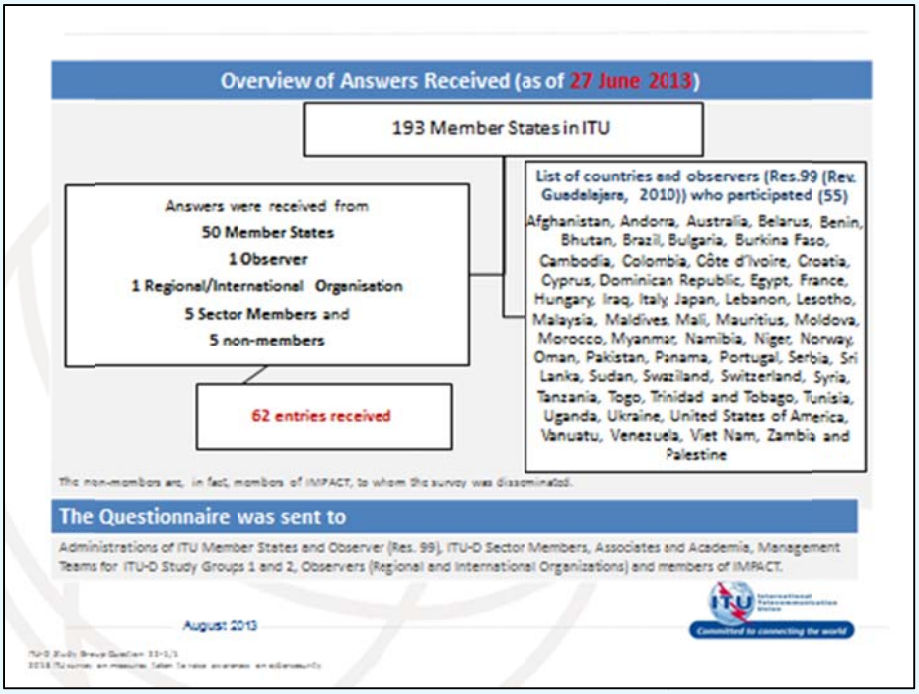
- Teams should commit to using the results.

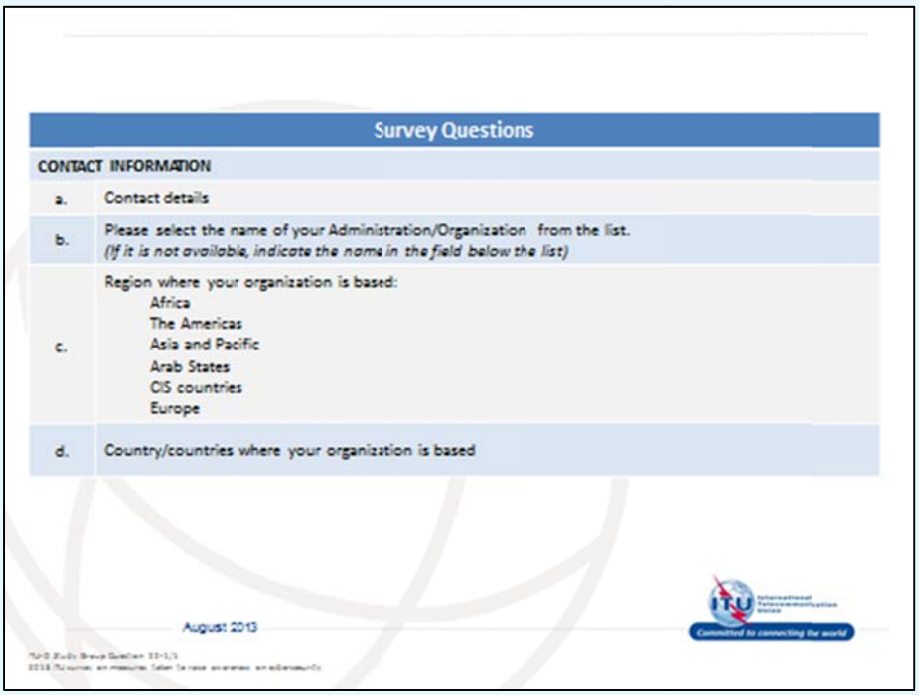
65

Annex F: Best practices for Cybersecurity – Survey on Measures Taken to Raise Awareness on Cybersecurity






Overview of Answers Received (as of 27 June 2013)
193 Member States in ITU
Answers were received from
50 Member States
1 Observer
1 Regional/International Organisation
5 Sector Members and
5 non-members
62 entries received
List of countries and observers (Res.99 (Rev. Guadalajara, 2010)) who participated (55)
Afghanistan, Andorra, Australia, Belarus, Benin, Bhutan, Brazil, Bulgaria, Burkina Faso, Cambodia, Colombia, Côte d'Ivoire, Croatia, Cyprus, Dominican Republic, Egypt, France, Hungary, Iraq, Italy, Japan, Lebanon, Lesotho, Malaysia, Maldives, Mali, Mauritius, Moldova, Morocco, Myanmar, Namibia, Niger, Norway, Oman, Pakistan, Panama, Portugal, Serbia, Sri Lanka, Sudan, Swaziland, Switzerland, Syria, Tanzania, Togo, Trinidad and Tobago, Tunisia, Uganda, Ukraine, United States of America, Vanuatu, Venezuela, Viet Nam, Zambia and Palestine
The non-members are, in fact, members of IMPACT, to whom the survey was disseminated.
The Questionnaire was sent to
Administrations of ITU Member States and Observer (Res. 99), ITU-D Sector Members, Associates and Academia, Management Teams for ITU-D Study Groups 1 and 2, Observers (Regional and International Organizations) and members of IMPACT.
August 2013


Survey Questions
CONTACT INFORMATION
a. Contact details
b. Please select the name of your Administration/Organization from the list.
(If it is not available, indicate the name in the field below the list)
c. Region where your organization is based:
Africa
The Americas
Asia and Pacific
Arab States
CIS countries
Europe
d. Country/countries where your organization is based
August 2013

Survey Questions (Cont'd)	
SURVEY	
1	In your opinion, how important is raising awareness on cybersecurity as a basic step to achieving security in cyberspace? Not important Somewhat important Important Very important
2	Has your country already adopted a general framework/strategy for cybersecurity? If not, move directly to survey question 5. Yes No
	If yes, please provide links/references:
3	If you answered 'yes' to the previous question, has any part of this policy/framework/strategy been directed to raising the awareness of the general public? Yes No
	If yes, please provide links/references:
4	If you answered 'yes' to the previous question, at which stage of the general framework/strategy for cybersecurity should the raising of awareness start?

August 2013

Survey Questions (Cont'd)	
5	If your country has not yet adopted a general framework/strategy for cybersecurity, has it been discussing/developing/formulating one? (If "No" is selected, please move directly to question 9) Yes No
	If yes, please provide links/references:
6	Do these discussions/formulations include raising cybersecurity awareness? Yes No
	If yes, please provide links/references:
7	At which stage of the general framework/strategy for cybersecurity should awareness raising start according to these discussions/formulations?
8	Who are the parties concerned with raising public awareness on cybersecurity, in accordance with the legislations/policies/practices adopted in your country?
9	Are there other parties not identified by the legislations/policies/practices that are concerned with raising public awareness on cybersecurity? Yes No
	If yes, please specify:

August 2013

Survey Questions (Cont'd)	
10	Was any specific research or survey conducted concerning cybersecurity in your country and/or region? Yes No
	If yes, please provide links/references:
11	Which groups are targeted by cybersecurity awareness campaigns in your country? Children Youth Students Elderly people Persons with disabilities Private institutions Government agencies Others
	If "others" was selected, please specify:
12	Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 for the highly targeted to the less targeted? *(1 to indicate highly targeted and 6 to indicate less targeted)* Children Youth Students Elderly people Persons with disabilities Private institutions Government agencies Others

Survey Questions (Cont'd)	
13	Has your country designed, or is in the process of designing, a dedicated plan in the general cybersecurity framework/strategy for persons with disabilities? Yes No
	If yes, please provide links/references:
14	What are the cybersecurity issues that are addressed by existing awareness campaigns? Internet safety Privacy Fraud Phishing Malware Child Online Protection Other, such as cyber-bullying and harassment, identity theft, spam, firewalls, passwords, shopping and business

August 2013

Survey Questions (Cont'd)	
15	What is the degree of importance of each issue? Please arrange in order of the most important to the less important and give reasons for such order? Internet safety Privacy Fraud Phishing Malware Child Online Protection Other, such as cyber-bullying and harassment, identity theft, spam, firewalls, passwords, shopping and business
16	What are the mechanisms used to raise awareness among the targeted groups stated in question 11?
	Please provide links/references:
17	Are there unconventional channels used for cybersecurity awareness? If yes, what are they?
	Please provide links/references:
18	Are there certain technologies related to providing cybersecurity, such as anti-virus or anti-spam software, available to the persons with disabilities? Yes No
	Please provide links/references:

August 2013

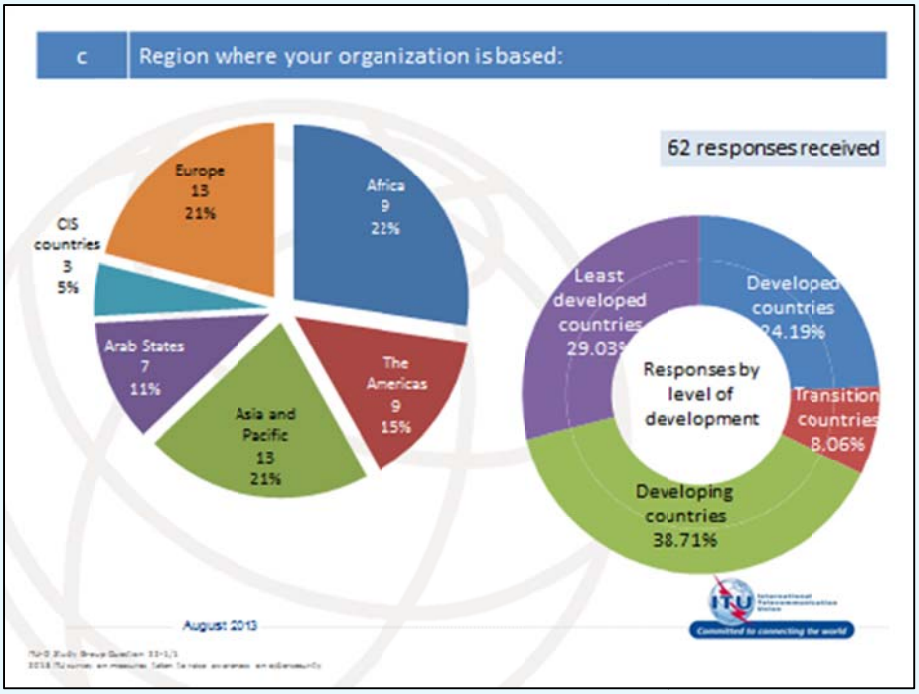
Committed to connecting the world

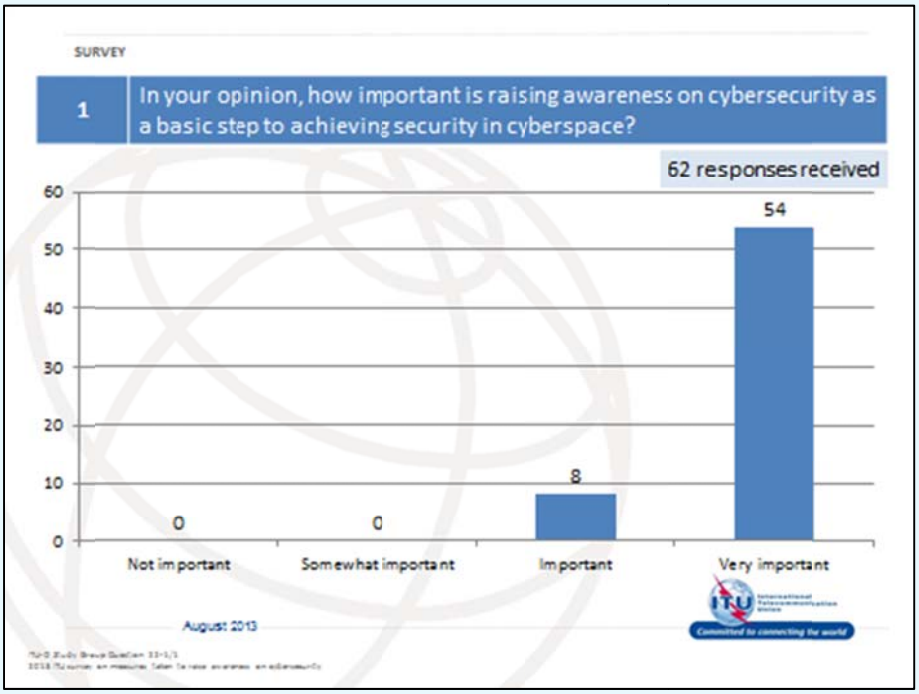
Survey Questions (Cont'd)	
19	Is the public encouraged to use the different technologies for cybersecurity such as anti-virus or anti-spam software? Yes No
	If yes, please specify:
20	If the answer is 'yes' to the previous question, are these different types of technologies made available to the public and how? Yes No
	If yes, please specify:

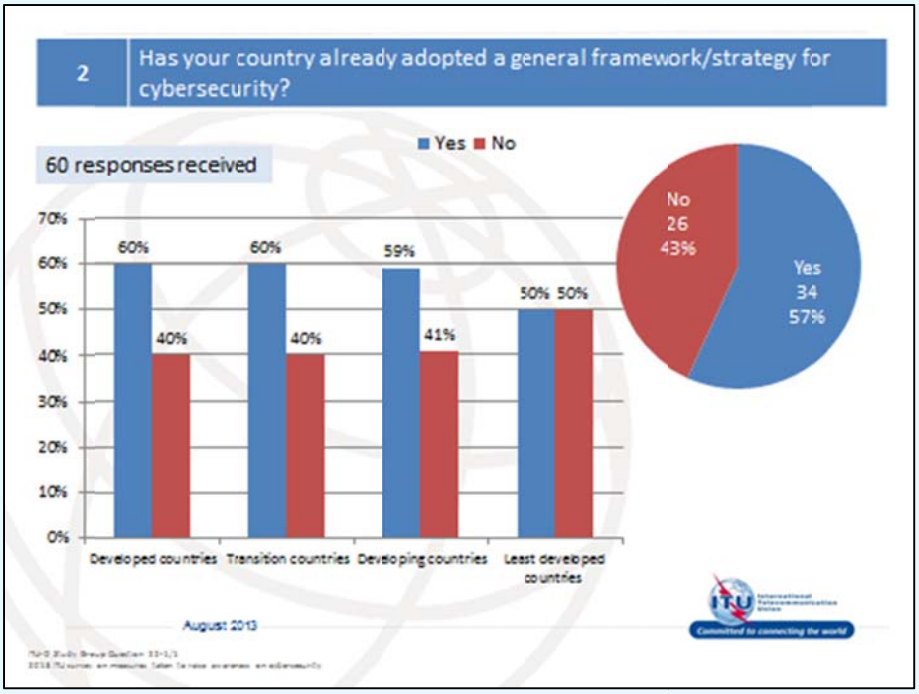
August 2013

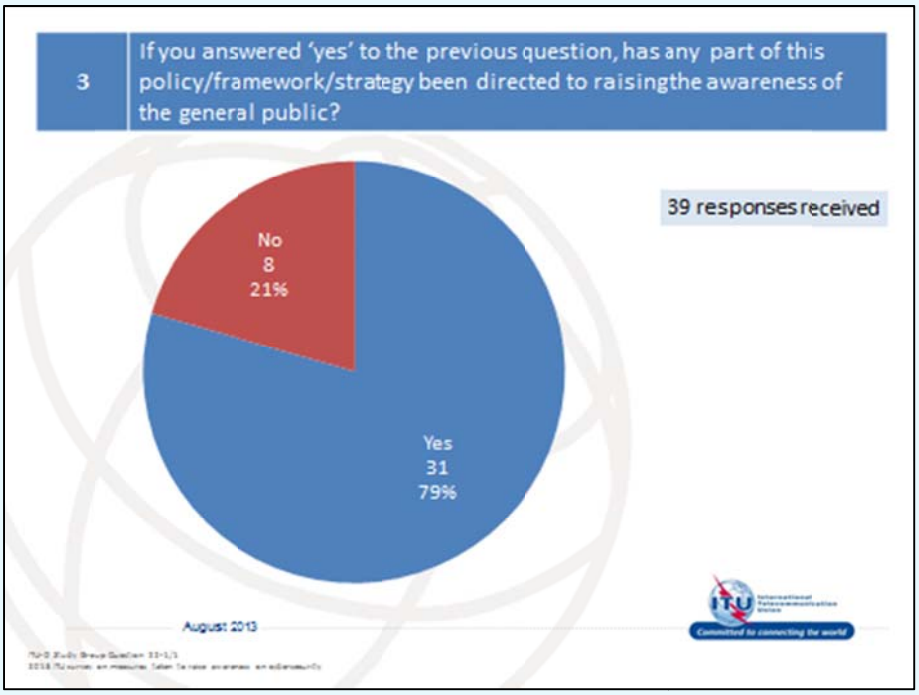
ITU

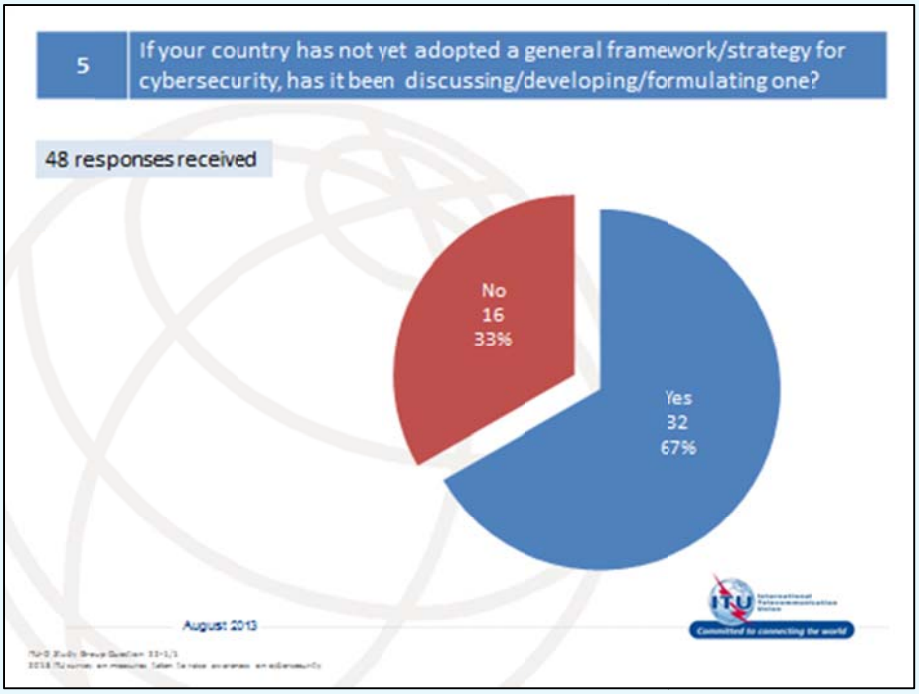
Committed to connecting the world

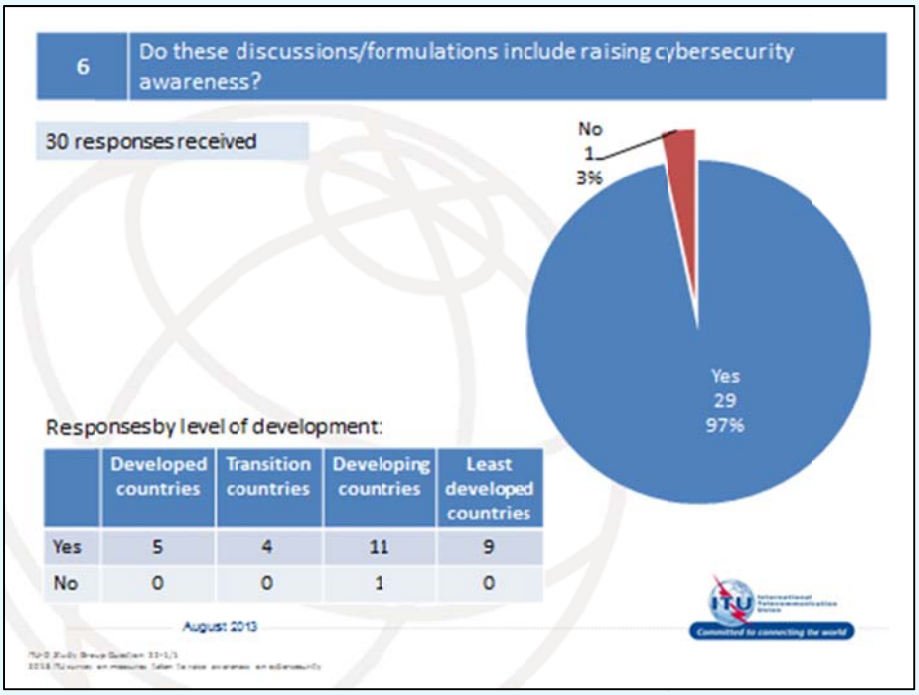

c
Region where your organization is based:
62 responses received
Europe
13
21%
Africa
9
21%
CIS countries
3
5%
Arab States
7
11%
The Americas
9
15%
Asia and Pacific
13
21%
Least developed countries
29.03%
Developed countries
Responses by level of development
Transition countries
8.06%
Developing countries
38.71%
August 2013


SURVEY
1
In your opinion, how important is raising awareness on cybersecurity as a basic step to achieving security in cyberspace?
62 responses received
60
50
40
30
20
10
0
0
0
8
54
Not important
Somewhat important
Important
Very important
August 2013


2
Has your country already adopted a general framework/strategy for cybersecurity?
60 responses received
Yes
No
70%
60%
50%
40%
30%
20%
10%
0%
60%
40%
60%
40%
59%
41%
50%
50%
Developed countries
Transition countries
Developing countries
Least developed countries
No
26
43%
Yes
34
57%
August 2013

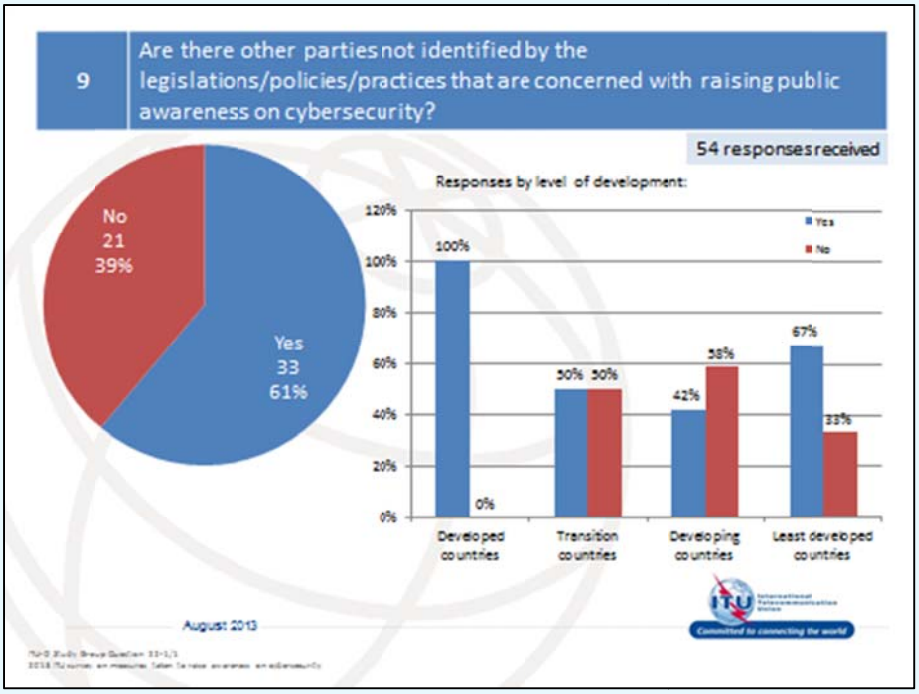

3
If you answered 'yes' to the previous question, has any part of this policy/framework/strategy been directed to raisingthe awareness of the general public?
39 responses received
No
8
21%
Yes
31
79%
August 2013

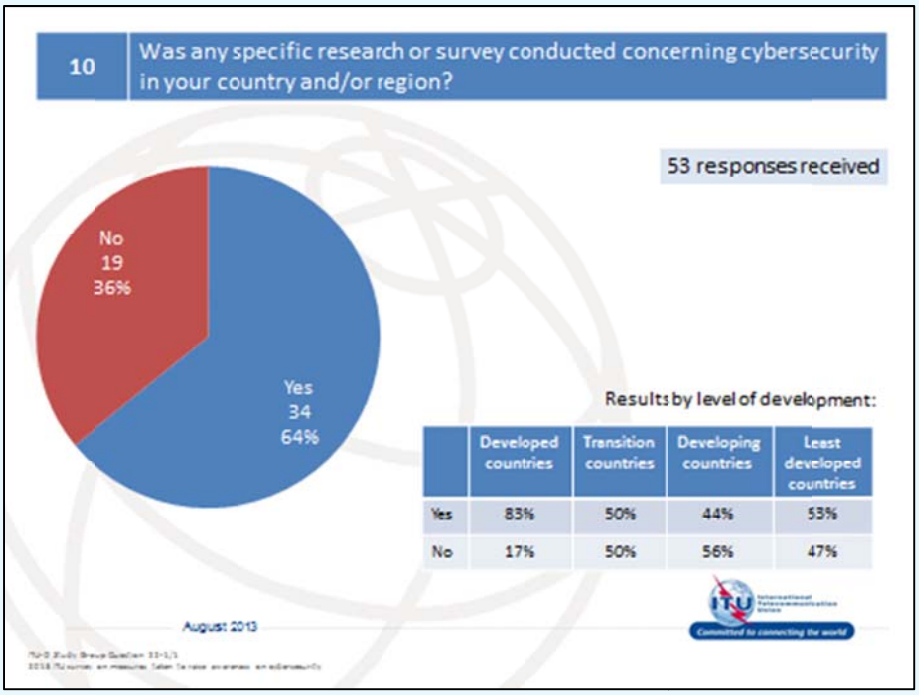




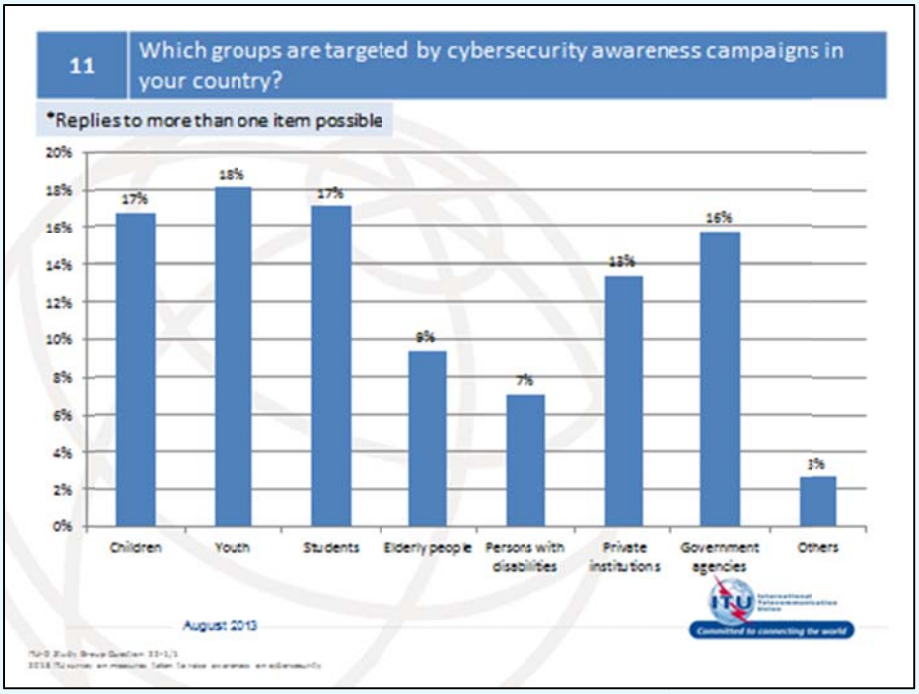
Responses by level of development:

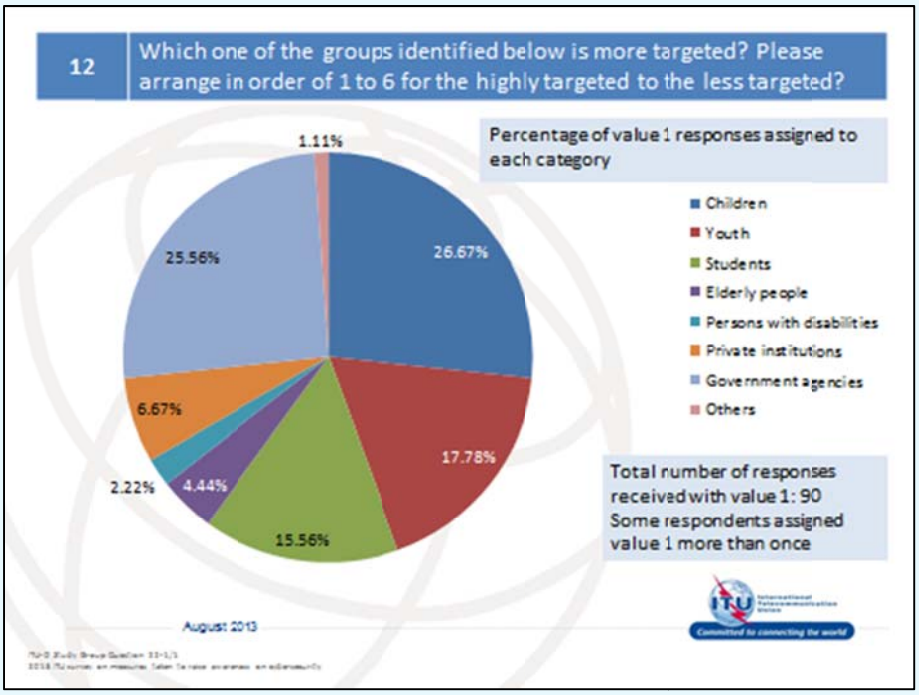
	Developed countries	Transition countries	Developing countries	Least developed countries
Yes	5	4	11	9
No	0	0	1	0

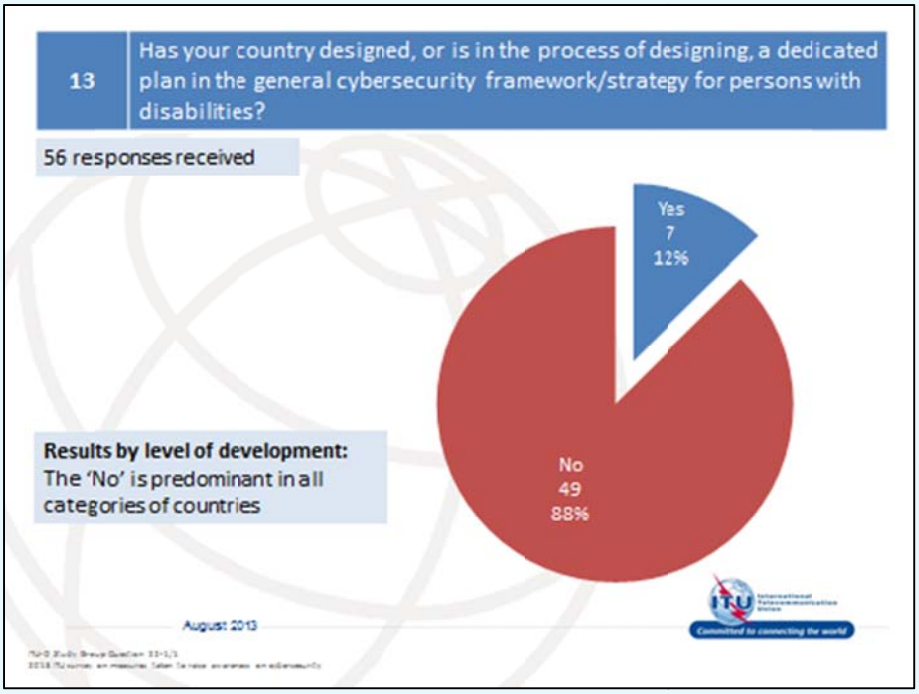


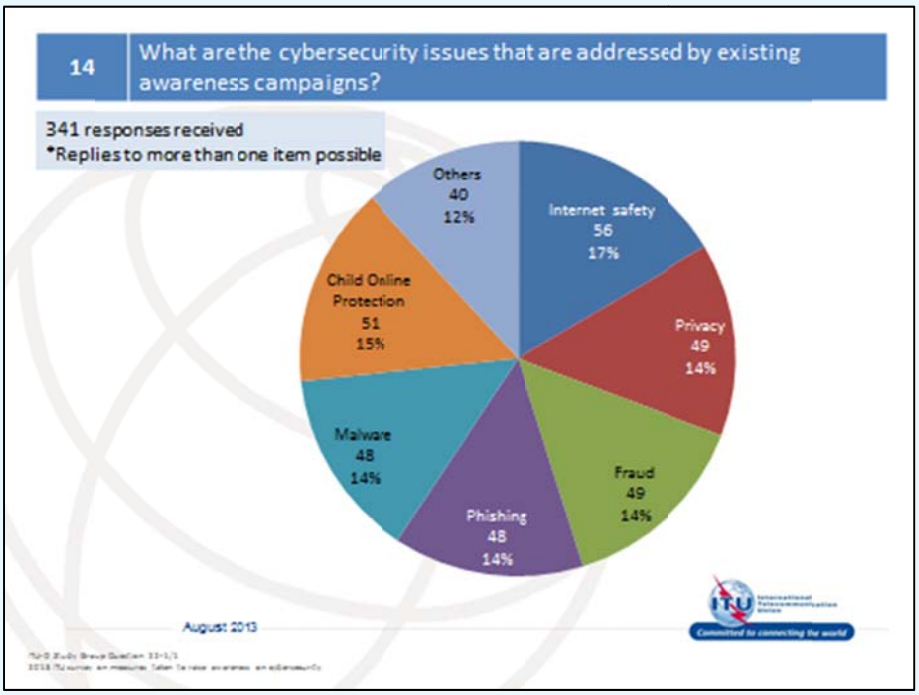


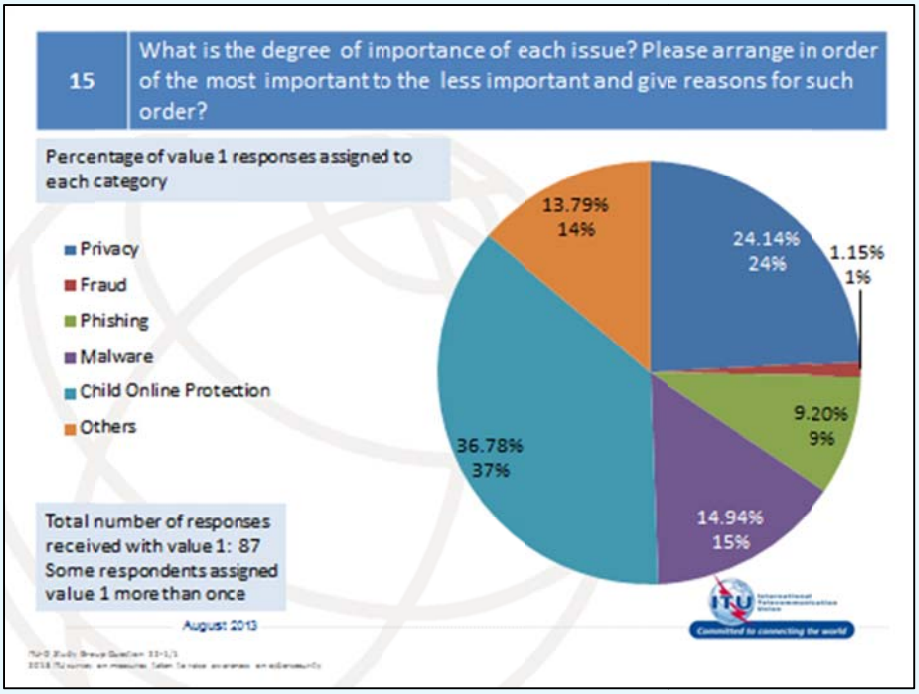
	Developed countries	Transition countries	Developing countries	Least developed countries
Yes	83%	50%	44%	53%
No	17%	50%	56%	47%

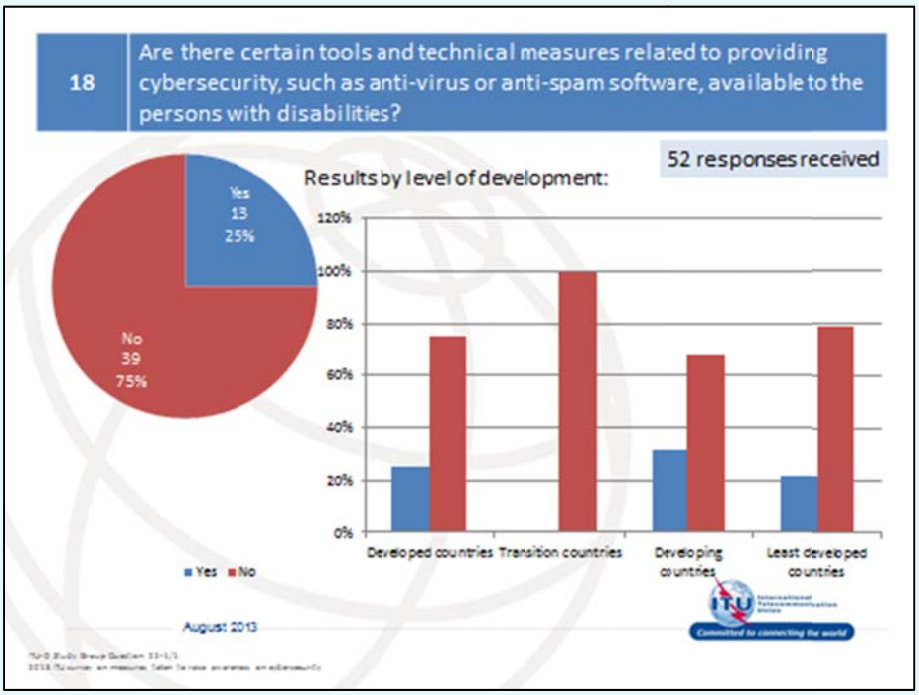

11
Which groups are targeted by cybersecurity awareness campaigns in your country?
*Replies to more than one item possible
20%
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
17%
18%
17%
9%
7%
13%
16%
3%
Children
Youth
Students
Elderly people
Persons with disabilities
Private institutions
Government agencies
Others
August 2013

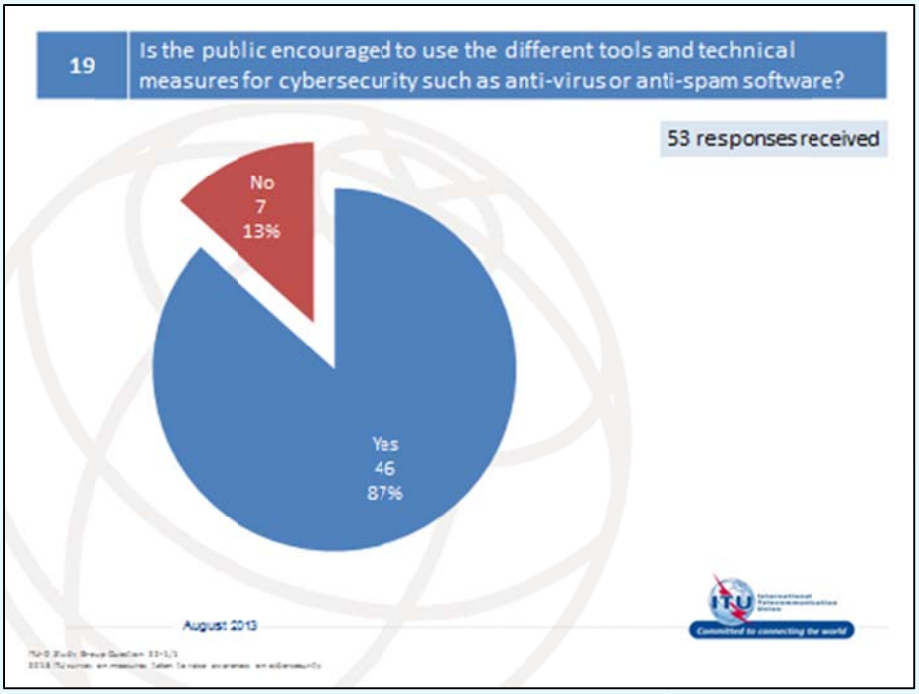

12
Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 for the highly targeted to the less targeted?
Percentage of value 1 responses assigned to each category
1.11%
26.67%
25.56%
17.78%
6.67%
2.22%
4.44%
15.56%
Children
Youth
Students
Elderly people
Persons with disabilities
Private institutions
Government agencies
Others
Total number of responses received with value 1: 90
Some respondents assigned value 1 more than once
August 2013

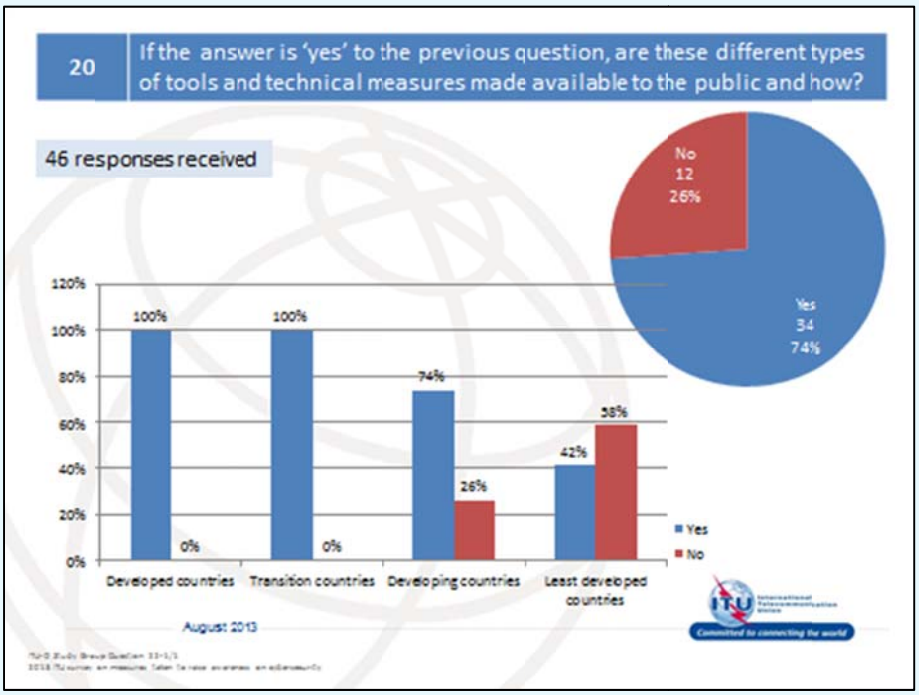

13
Has your country designed, or is in the process of designing, a dedicated plan in the general cybersecurity framework/strategy for persons with disabilities?
56 responses received
Yes
7
12%
No
49
88%
Results by level of development:
The 'No' is predominant in all categories of countries
August 2013

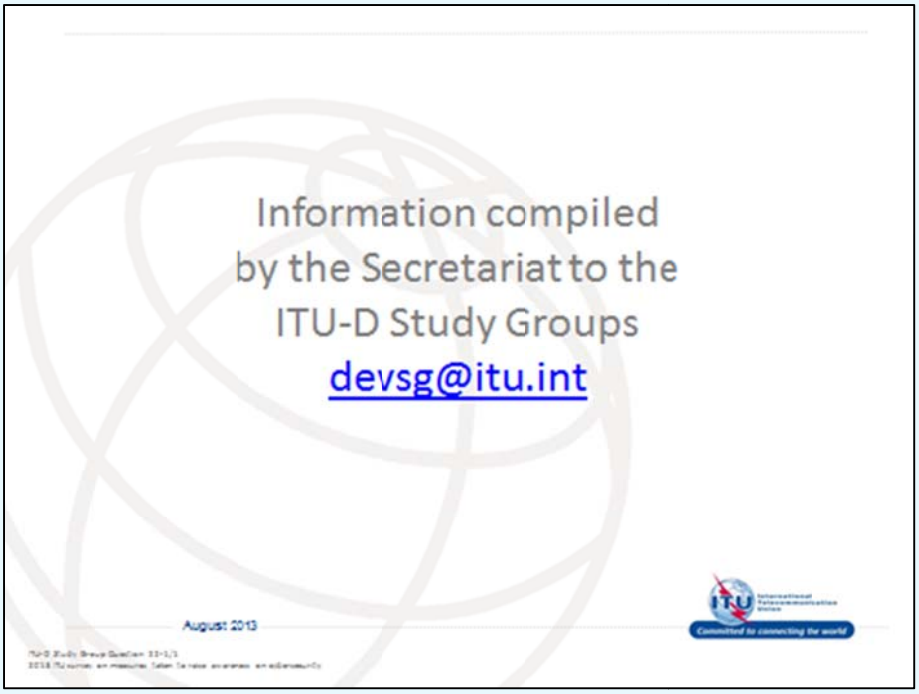

14
What are the cybersecurity issues that are addressed by existing awareness campaigns?
341 responses received
*Replies to more than one item possible
Others
40
12%
Internet safety
56
17%
Child Online Protection
51
15%
Privacy
49
14%
Malware
48
14%
Fraud
49
14%
Phishing
48
14%
August 2013


15
What is the degree of importance of each issue? Please arrange in order of the most important to the less important and give reasons for such order?
Percentage of value 1 responses assigned to each category
Privacy
Fraud
Phishing
Malware
Child Online Protection
Others
13.79%
14%
24.14%
24%
1.15%
1%
9.20%
9%
36.78%
37%
14.94%
15%
Total number of responses received with value 1: 87
Some respondents assigned value 1 more than once
August 2013

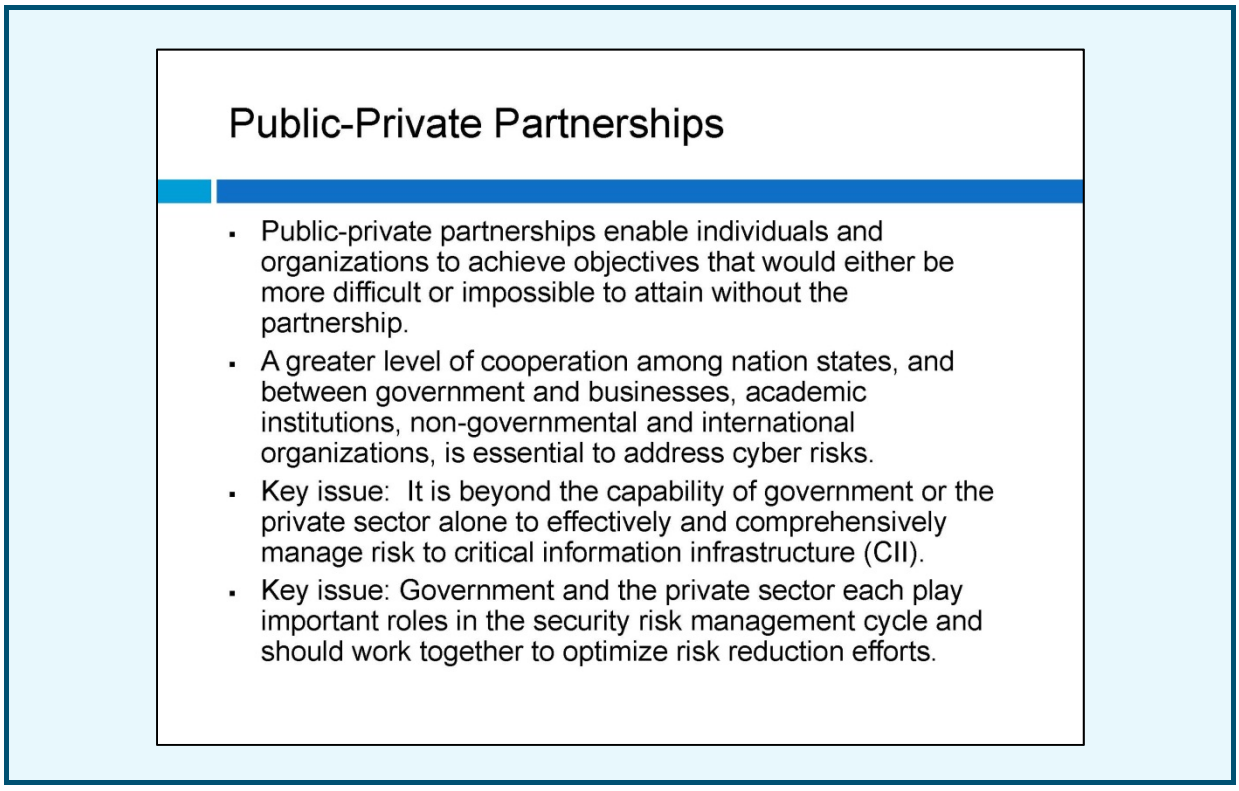

18
Are there certain tools and technical measures related to providing cybersecurity, such as anti-virus or anti-spam software, available to the persons with disabilities?
52 responses received
Yes
13
25%
No
39
75%
Results by level of development:
120%
100%
80%
60%
40%
20%
0%
Developed countries
Transition countries
Developing countries
Least developed countries
Yes
No
August 2013

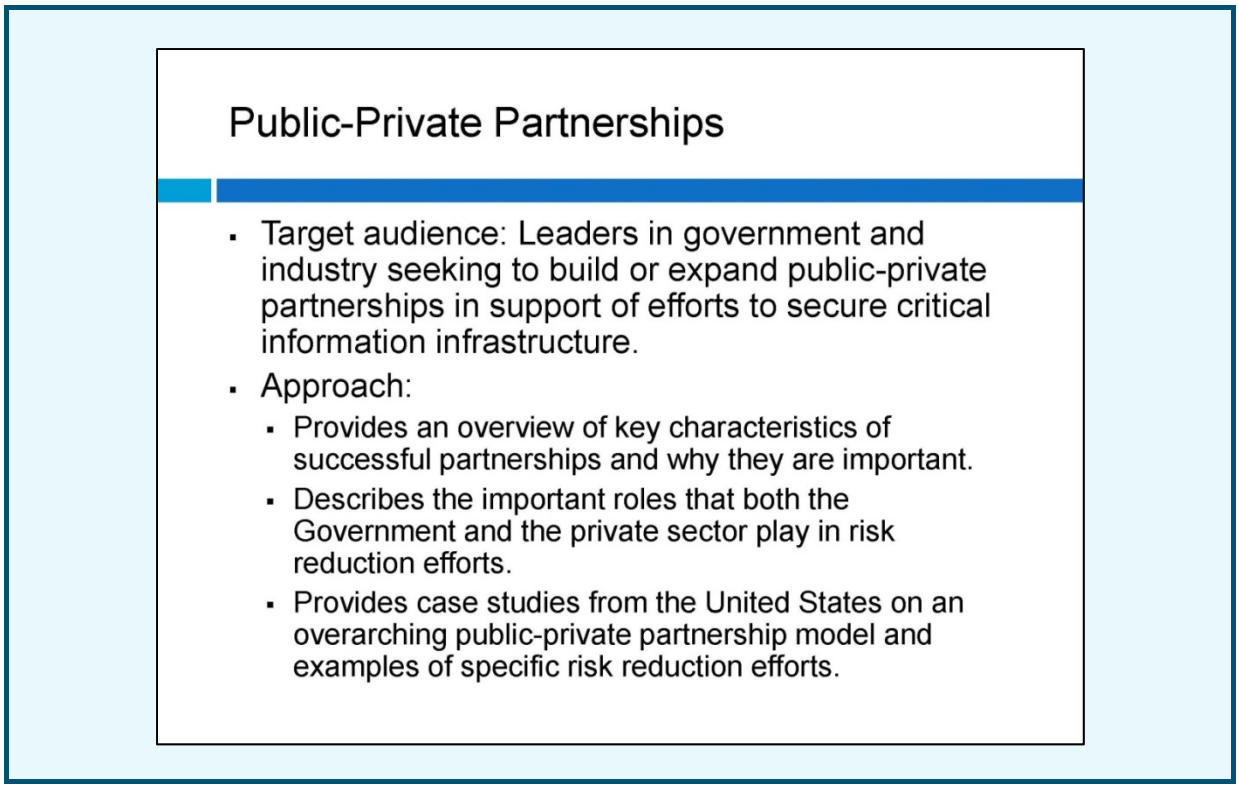

19
Is the public encouraged to use the different tools and technical measures for cybersecurity such as anti-virus or anti-spam software?
53 responses received
No
7
13%
Yes
46
87%
August 2013


20
If the answer is 'yes' to the previous question, are these different types of tools and technical measures made available to the public and how?
46 responses received
No
12
26%
Yes
34
74%
120%
100%
80%
60%
40%
20%
0%
100%
0%
100%
0%
74%
26%
42%
58%
Developed countries
Transition countries
Developing countries
Least developed countries
Yes
No
August 2013


Information compiled
by the Secretariat to the
ITU-D Study Groups
devsg@itu.int
August 2013

Annex G: Best practices for Cybersecurity – Public-Private Partnerships in Support of Cybersecurity Goals and Objectives




Public-Private Partnerships
Target audience: Leaders in government and industry seeking to build or expand public-private partnerships in support of efforts to secure critical information infrastructure.
Approach:
Provides an overview of key characteristics of successful partnerships and why they are important.
Describes the important roles that both the Government and the private sector play in risk reduction efforts.
Provides case studies from the United States on an overarching public-private partnership model and examples of specific risk reduction efforts.

Annex H: Compendium on Cybersecurity Country Case Studies

Abstract

This document presents the updated draft for Question 22-1/1 country case studies compendium, which will assemble, based on the contributions submitted, a volume of cases describing the current status of countries' cybersecurity efforts, and their cybersecurity policies, in accordance with Question 22-1/1 Work Program, 2, "d".

The contributions are classified according to the subject matter headings set forth in the Question 22-1/1 Final Report (Developing a National Strategy for Cybersecurity; Establishing National Government – Private Sector Collaboration; Deterring Cybercrime; Creating National Incident Management Capabilities; and Promoting a National Culture of Cybersecurity).

The cases assembled in this proposal reflect the contributions received in the last cycle of the Question 22-1/1 work and the ones received in this cycle (updated until May 13th, 2013). This version of the compendium is structured according to the discussion held during the last meeting of Question 22-1/1

Member States are invited to to review and to approve the Compedium, as one of Question 22-1/1 expected outputs.

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Bangladesh (People's Republic of)	Document RGQ 22/1/048; http://www.itu.int/md/D06-RGQ22.1-C-0048/en Contribution by Bangladesh.	√		√	√	
	Document 1/203 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0203/en Prevention of cyber crime in Bangladesh.			√	√	
Brazil	Document 1/245 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0245/en Brazilian legal framework to address cybercrimes.			√		
	Document RGQ 22-1/1/010; http://www.itu.int/md/D10-RGQ22.1.1-C-0010/en Project Angels on the Net: A successful Brazilian multi-partnership example.			√		√
	Document 1/93 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0093/en Tentacles Project – a New Way to Combat Cybercrimes.		√	√		
	Document RGQ 22-1/1/029; http://www.itu.int/md/D10-RGQ22.1.1-C-0029/en Brazilian Cybercrime Legislation Update.			√		

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Burkina Faso	Document 1/241 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0241/en NB: The content of this contribution is also presented in: Document RGQ 22/1/047; (http://www.itu.int/md/D06-RGQ22.1-C-0047/en) Mise en place d'un cadre réglementaire pour la cybersécurité au Burkina Faso.			√		
	Document RGQ 22-1/1/017; http://www.itu.int/md/D10-RGQ22.1.1-C-0017/en Instauration de la confiance et de la sécurité dans l'utilisation des Technologies de l'information, acquis et perspective pour le Burkina Faso.			√		
Cameroon	Document 1/240 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0240/en NB: The content of this contribution is also presented in: Document RGQ 22/1/046; (http://www.itu.int/md/D06-RGQ22.1-C-0046/en) Case study: Cameroon – Draft act on cybercrime.			√		
Congo	Document RGQ 22/1/028; http://www.itu.int/md/D06-RGQ22.1-C-0028/en Contribution de la République Démocratique du Congo.	√				

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Congo *(Cont.)*	Document 1/INF/46 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-INF-0046/en Cybersecurity in Developing Countries.	√		√		√
	Document RGQ 22-1/1/028; (http://www.itu.int/md/D06-RGQ22.1-C-0046/en Cybersecurity in Developing Countries.	√		√		√
Côte d'Ivoire	Document 1/155 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0155/en Experience of Côte d'Ivoire in regard to cybercrime.	√		√	√	√
Japan	Document 1/281 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0281/en Results of the Strategic Dialogue on a Safer Internet Environment for Children ("Tokyo Strategic Dialogue"), on June 2 and 3, 2009.		√	√		√
Korea (Republic of)	Document 1/272 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0272/en Current Status of Information Security Threats and Countermeasures of Korea.	√		√	√	√
	Documet 1/INF/033 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-INF-0033/en Smart Mobile Security Strategy of Korea and their Implications.	√				

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Korea (Republic of) *(Cont.)*	Document 1/118 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0118/en Development of Healthy Information Culture (Extracted From 2006 Digital Opportunity White Paper).			√		√
	Document 1/202 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0202/en Status of Internet Addiction and the National Policy to Cope with it.					√
	Document 1/223 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0223/en Internet addiction treatment.					√
	Document 1/270 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0270/en Korea's Efforts to Create Safe Online Environment.					√
	Document 1/271 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0271/en Practical Guidelines for Internet Addiction Prevention.					√
	Document 1/179 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0179/en Amendment of the ICT Network Act of Korea to Reinforce Personal Information Protection System on the Internet.	√				√
Lithuania	Document RGQ 22/1/007; http://www.itu.int/md/D06-RGQ22.1-C-0007/en Network and Information Security.	√	√	√	√	√

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Madagascar	Document 1/239 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0239/en NB: The content of this contribution is also presented in: Document RGQ 22/1/045; (http://www.itu.int/md/D06-RGQ22.1-C-0045/en) Contribution from Madagascar.	√	√	√		√
Mali	Document 1/150 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0150/en Compendium on cybersecurity country case studies.			√	√	
	Document 1/69 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0069/en Overview of cybercrime targeting persons with disabilities.			√		
Mongolia	Document 1/149 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0149/en Current Status of Mongolia's Cybersecurity Policies and Efforts.	√		√	√	
Niger	Document 1/23 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0023/en Contribution du Niger.			√		

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Oman (Sultanate of)	Document 1/201 (2010-2014 Study Period);http://www.itu.int/md/D10-SG01-C-0201/en Regulation of Internet Service Provision.	√				
People's Republic of China	Document 1/037 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0037/en Information Network Security Status in China.	√				
	Document 1/113 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0113/en Real-Name Registration Will Be Applicable In China Telecom Industry.			√		
	Document 1/107 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0107/en Real Name Registration Introduced in Mobile Communication.			√		
	Document 1/196 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0196/en A research on web privacy policies in China.	√		√		

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
Rwanda	Document RGQ 22/1/010; http://www.itu.int/md/D06-RGQ22.1-C-0010/en Best Computer Security Practices.			√		
	Document 1/101 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0101/en Best Computer Security Practices.	√			√	√
	Document 1/169 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0169/en National information security programme overview: Current status.	√		√	√	
Senegal	Document 1/148 (2010-2014 Study Period); http://www.itu.int/md/D10-SG01-C-0148/en The Senegalese legal framework and cybersecurity.			√		
Switzerland	Document 1/189 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0189/en Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI.			√	√	
Togo	Document RGQ 22-1/1/INF/08-F (2010-2014 Study Period); http://www.itu.int/md/D10-RGQ22.1.1-INF-0008/en Evaluation de la cybersécurité dans les institutions et entreprises togolaises.	√		√	√	

Contribution		Topics Addressed by the Contribution				
Country	**Document**	**Developing a National Strategy for Cybersecurity**	**Establishing National Government – Private Sector Collaboration**	**Deterring Cybercrime**	**Creating National Incident Management Capabilities**	**Promoting a National Culture of Cybersecurity**
United States of America	Document RGQ 22-1/1/009; http://www.itu.int/md/D10-RGQ22.1.1-C-0009/en Internet Service Provider (ISP) Network Protection Best Practices.		√			
Venezuela	Document 1/25 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0025/en Normativa Venezolana En Materia De Ciberseguridad.	√		√		
	Document 1/30 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0030/en Proyectos Desarrollados en Materia de Ciberseguridad.	√	√			
	Document 1/199 (2006-2010 Study Period); http://www.itu.int/md/D06-SG01-C-0199/en Visión de la Seguridad de la información en la República Bolivariana de Venezuela.	√		√	√	

الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المدير

Place des Nations
CH-1211 Geneva 20
Email: mailto:bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

نائب المدير ورئيس دائرة الإدارة وتنسيق العمليات (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

دائرة البنية التحتية والبيئة التمكينية والتطبيقات الإلكترونية (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

دائرة الابتكارات والشراكات (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

دائرة دعم المشاريع وإدارة المعرفة (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

إفريقيا

إثيوبيا

المكتب الإقليمي للاتحاد
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia a

E-mail: itu-addis@itu.int
Tel.: +251 11 551 49 77
Tel.: +251 11 551 48 55
Tel.: +251 11 551 83 28
Fax: +251 11 551 72 99

الكاميرون

مكتب المنطقة للاتحاد
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

E-mail: itu-yaounde@itu.int
Tel.: + 237 22 22 92 92
Tel.: + 237 22 22 92 91
Fax: + 237 22 22 92 97

السنغال

مكتب المنطقة للاتحاد
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

E-mail: itu-dakar@itu.int
Tel.: +221 33 849 77 20
Fax: +221 33 822 80 13

زيمبابوي

مكتب المنطقة للاتحاد
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

E-mail: itu-harare@itu.int
Tel.: +263 4 77 59 41
Tel.: +263 4 77 59 39
Fax: +263 4 77 12 57

الأمريكتان

البرازيل

المكتب الإقليمي للاتحاد
SAUS Quadra 06 Bloco "E"
11 andar – Ala Sul
Ed. Luis Eduardo Magalhães (AnaTel)
70070-940 – Brasilia, DF – Brasil

E-mail: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

بربادوس

مكتب المنطقة للاتحاد
United Nations House
Marine Gardens
Hastings – Christ Church
P.O. Box 1047
Bridgetown – Barbados

E-mail: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

شيلي

مكتب المنطقة للاتحاد
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

E-mail: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

هندوراس

مكتب المنطقة للاتحاد
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT 4 Piso
P.O. Box 976
Tegucigalpa – Honduras

E-mail: ituteguciglapa@itu.int
Tel.: +504 2 2 201 074
Fax: +504 2 2 201 075

الدول العربية

مصر

المكتب الإقليمي للاتحاد
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

E-mail: itucairo@itu.int
Tel.: +20 2 35 37 17 77
Fax: +20 2 35 37 18 88

آسيا – المحيط الهادئ

تايلاند

المكتب الإقليمي للاتحاد
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

E-mail: itubangkok@itu.int
Tel.: +66 2 574 8565/9
Tel.: +66 2 574 9326/7
Fax: +66 2 574 9328

إندونيسيا

مكتب المنطقة للاتحاد
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

E-mail: itujakarta@itu.int
Tel.: +62 21 381 35 72
Tel.: +62 21 380 23 22
Tel.: +62 21 380 23 24
Fax: +62 21 389 05 521

كومنولث الدول المستقلة

الاتحاد الروسي

مكتب المنطقة للاتحاد
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

E-mail: itumoskow@itu.int
Tel.: +7 495 926 60 70
Fax: +7 495 926 60 73

أوروبا

سويسرا

مكتب تنمية الاتصالات (BDT)
الاتحاد الدولي للاتصالات (ITU)
وحدة أوروبا (EUR)

Place des Nations
CH-1211 Geneva 20 – Switzerland
E-mail: eurregion@itu.int
Tel.: +41 22 730 5111

الاتحاد الدولي للاتصالات
مكتب تنمية الاتصالات
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

طبع في سويسرا
جنيف، 2014

01/2014