International Telecommunication Union

QUESTION 22/1

Final Report

ITU-D STUDY GROUP 1 4th STUDY PERIOD (2006-2010)

QUESTION 22/1:

Securing information and communication networks: best practices for developing a culture of cybersecurity

THE STUDY GROUPS OF ITU-D

In accordance with Resolution 2 (Doha, 2006), WTDC-06 maintained two study groups and determined the Questions to be studied by them. The working procedures to be followed by the study groups are defined in Resolution 1 (Doha, 2006) adopted by WTDC-06. For the period 2006-2010, Study Group 1 was entrusted with the study of nine Questions in the field of telecommunication development strategies and policies. Study Group 2 was entrusted with the study of ten Questions in the field of development and management of telecommunication services and networks and ICT applications.

For further information

Please contact:

Mr Souheil MARINE/Ms Christine SUND
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 5323/ 5203
Fax: +41 22 730 5484
E-mail: souheil.marine@itu.int
christine.sund@itu.int

Placing orders for ITU publications

Please note that orders cannot be taken over the telephone. They should be sent by fax or e-mail.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Fax: +41 22 730 5194
E-mail: sales@itu.int

The Electronic Bookshop of ITU: www.itu.int/publications

International Telecommunication Union

QUESTION 22-1

Final Report

ITU-D STUDY GROUP 1 4th STUDY PERIOD (2006-2010)

QUESTION 22-1:

Securing information and communication networks: best practices for developing a culture of cybersecurity

DISCLAIMER

This report has been prepared by many experts from different administrations and companies. The mention of specific companies or products does not imply any endorsement or recommendation by ITU.

TABLE OF CONTENTS

Page

QUESTION 22-1

Introduction

This Report provides national administrations with an overview of the building blocks needed for addressing cybersecurity at the national level and for organizing their approach to national cybersecurity[1]. Because existing national capabilities vary and threats are constantly evolving, the report does not provide a prescriptive recipe for securing cyberspace. Instead, this framework describes a flexible approach that can be applied to help a national administration review and improve its existing institutions, policies, and relationships dealing with cybersecurity. Although this Report focuses on cybersecurity, we note that protection of the physical network is an equally important priority. We also note that best practices in cybersecurity must protect and respect the provisions for privacy and freedom of expression, as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.[2]

Key elements of this Report are:

- 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.

Each of these elements should be part of a comprehensive national approach to cybersecurity. Their order of appearance does not indicate any preference for one element over another. There could be others based on national circumstances.

For the purposes of this rReport, ***cybersecurity***, as defined by ITU-T Recommendation X.1205, is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

It is important to understand the relationship among cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), critical information infrastructure protection (CIIP), and non-critical infrastructure. This relationship is illustrated in Figure 1.

While definitions may vary slightly, ***critical infrastructures*** (CI) are generally considered as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those matters. CI are composed of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data) (see Figure 1). What constitutes "critical" may vary from country to country, but typically might include elements of the information and communications (including telecommunications) technology (ICT), energy, banking, transportation, public health, agriculture and food, water, chemical, shipping, and essential government services sectors. Countries at all stages of development need to plan for and develop policies to protect what

---

[1] Interested readers are invited to look at the output of ISO 27001 to 27003.

[2] See WSIS, Tunis Agenda for the Information Society, Paragraph 42.

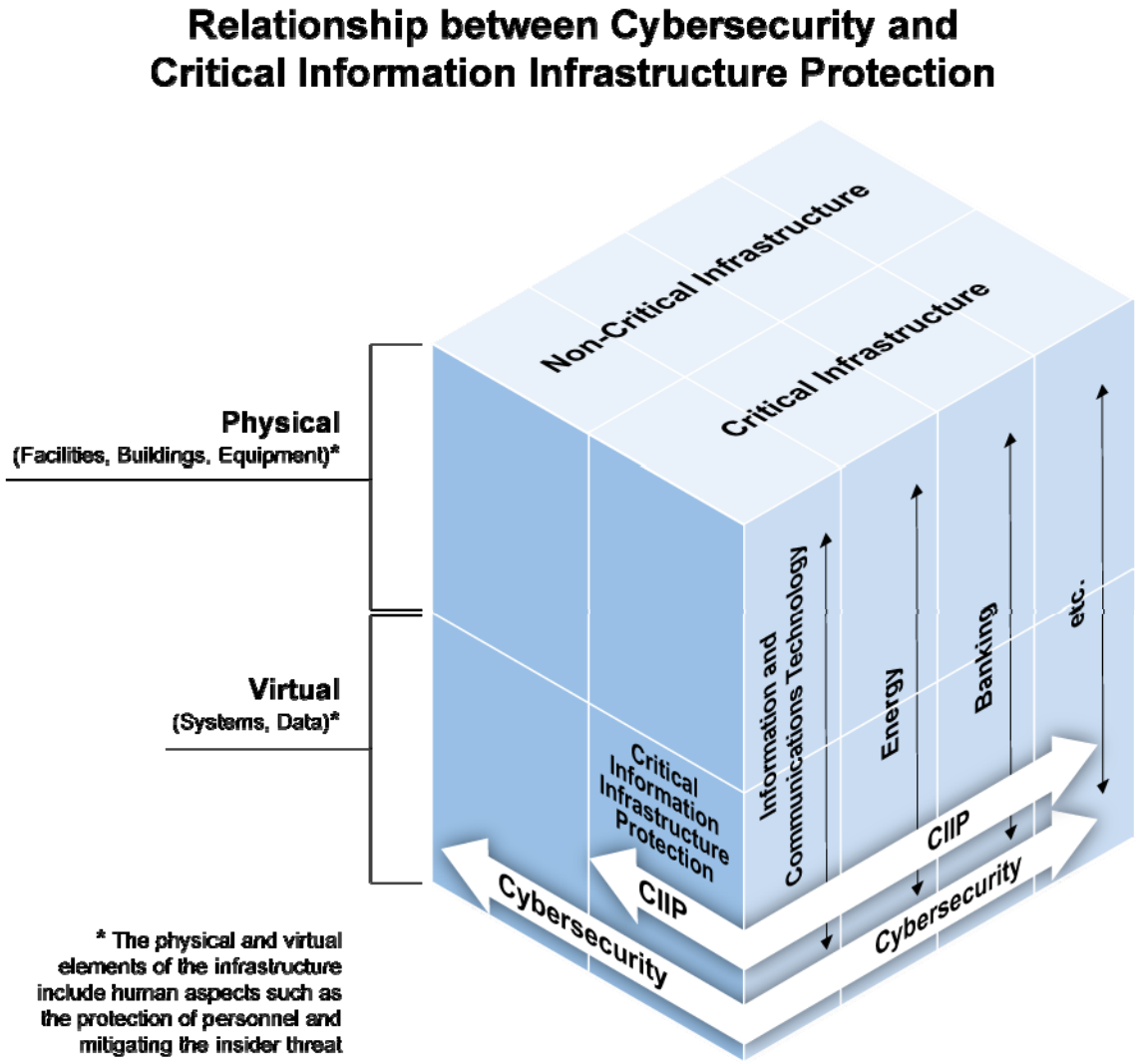
they determine to be their CI (in other words, Critical Infrastructure Protection, including both physical and virtual protection) in order to provide reasonable assurance of resilience and security to support national missions and economic stability.

Each of these economic sectors has its own physical assets, such as bank buildings, power plants, trains, hospitals and government offices. However, these critical sectors of a nation's economy all depend upon information and communication technologies. Across the board, these sectors and their physical assets today depend upon the reliable functioning of this ***critical information infrastructure*** (CII) to deliver their services and to conduct business. Consequently, significant disruption to the CII could have an immediate and debilitating impact that reaches far beyond the ICT sector and affects the ability of a nation to perform its essential missions in multiple sectors. A ***critical information infrastructure protection*** (CIIP) program protects the virtual component of the CII.

As indicated in Figure 1, CIIP is a subset of both CIP and of cybersecurity. Cybersecurity protects against all forms of cyber incidents by strengthening the safety of the critical information infrastructure on which the critical sectors depend and securing the networks and services which serve the day-to-day needs of users. Cyber incidents may affect the critical and non-critical information infrastructures alike and may take many forms of malicious activity such as use of botnets to conduct denial of service attacks and distribute spam and malware (e.g. viruses and worms) which affect the ability of the networks to operate. In addition, cyber incidents may include illicit activities such as phishing and pharming, as well as identity theft. The cyber threat continues to increase as the tools and methodologies used become more and more widely available, and the technical capability and sophistication of cyber criminals expand. Countries at all stages of development have experienced these cyber incidents.

A national approach to cybersecurity includes raising awareness about existing cyber risks, creating national structures to address cybersecurity, and establishing the necessary relationships that may be utilized to address events that occur. Assessing risk, implementing mitigation measures, and managing consequences are also part of a national cybersecurity program. A good national cybersecurity program will help protect a nation's economy from disruption by contributing to continuity planning across sectors, protecting the information that is stored in information systems, preserving public confidence, maintaining national security, and ensuring public health and safety.

Figure 1: The Conceptual Relationship Between Critical Information Infrastructure Protection and Cybersecurity



Enhancing cybersecurity could not be limited to national strategy only although it is very important, it should be complemented by regional and international strategies as called for by the relevant outcome of WSIS in its two phases 2003-2005 and the follow-up on Action Line C5 based on Nos. 35 and 36 of the Geneva Declaration of Principles and No. 39 of the Tunis Agenda, and the implementation of the outcomes of the World Summit on the Information Society by the relevant Resolutions, actions and initiatives adopted by the ITU such as:

a) Goal 4 of the PP Resolution 71 (Rev Antalya 2006) "Strategic Plan for the Union for 2008-2011";

b) PP Resolution 130 (Rev. Antalya 2006) "Strengthening the role of ITU in building confidence and security in the use of information an d communication technologies";

c) The relevant parts of the Doha Action Plan of WTDC-06, including Programme 3 on e-strategies and ICT applications that identify cybersecurity as a priority for the BDT, with defined activities and in particular the adoption of Resolution 45 (Doha, 2006) entitled "Mechanisms for enhancing cooperation on cybersecurity, including combating spam" Resolution 45 instructed the director of the BDT to organize meetings to discuss ways to enhance cybersecurity including, *inter alia*, a

memorandum of understanding to enhance cybersecurity and combat spam amongst interested member states, and to report the results of these meetings to the 2006 Plenipotentiary Conference.The BDT's report to PP 2006 can be found at http://www.itu.int/md/S06-PP-C-0024/en.[3]

d) The extensive work of ITU-T Lead Study Group No. 17 on cybersecurity and the complementary activities by Study Group 13;

e) The recent Resolution No 58 adopted by WTSA (Johannesburg, 2008) entitled "encourage the creation of national computer incident response teams (CIRTs) particularly for developing countries" which recognized the work carried out by this Question 22.1 in the ITU-D Sector;

f) 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 experts on the seven main strategy goals embedded within this initiative, with concentration on relevant Recommendations for the following five working areas:

- Legal measures
- Technical and procedural measures
- Organizational structure
- Capacity building
- International cooperation

Among these work areas, "Legal measures" focused on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner. "Technical and procedural measures" focused on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards. "Organizational structures" focused on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems. "Capacity building" focused on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Finally "International cooperation" focused on international cooperation, dialogue and coordination in dealing with cyberthreats.[4, 5]

g) The recent draft Opinion 4 adopted by the 2009 World Telecommunication Policy Forum (WTPF) on "Collaborative Strategies for Creating Confidence and Security in the Use of ICTs"[6], noting in particular the sections on *invites the ITU*, and *invites the Member States*.

h) The activities of Programme 3 (e-applications) in the BDT through direct assistance to Member States of developing countries, through projects and capacity-building/ITU National Cybersecurity/ CIIP Self-Assessment tool and the ITU Botnet Mitigation Toolkit and the toolkit to build national CIRTs.

i) The Child Online Protection (COP) Initiative was launched in November 2008 as an international collaborative network for action to promote the online protection of children and young people worldwide by providing guidance on safe online behaviour in conjunction with other UN agencies and partners. The key objectives of the COP Initiative are to: 1) Identify the key risks and vulnerabilities to children and young people in cyberspace; 2) Create awareness of the risks and issues through multiple channels; 3) Develop practical tools to help governments, organizations and educators to minimize risk; and, 4) Share knowledge and experience while facilitating international strategic partnerships to define and implement concrete initiatives.

---

[3] The Arab States after their experience of the past four years are more convinced that an MoU to enhance cybersecurity and combat spam among Member States is the best solution to meet global and/or regional needs.

[4] Experts from the Arab States supported all the Recommendations of the HLEG chairman's report.

[5] The details of the HLEG chairman's report can be found at: http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf

[6] The full WTPF draft Opinion 4 can be found at: http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf

j) The collaboration that has been established by ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT), within the framework of the ITU Global Cybersecurity Agenda, aimed at bringing key stakeholders and partners from governments, private sector companies and academia together to provide ITU Member States with the expertise, facilities and resources to effectively address cyber-threats. Key objectives of the ITU–IMPACT collaboration are to: 1) Develop a global framework for watch, warning and incident response; 2) Establish appropriate national and regional organizational structures and policies, such as National Computer Incident Response Teams (CIRT); 3) Facilitate human and institutional capacity building across sectors; and, 4) Facilitate global multi-stakeholder international cooperation.

PART I

Developing and Obtaining Agreement on a National Cybersecurity Strategy

Developing and implementing a national cybersecurity plan 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 (government authorities, the private sector, and citizens) in the process.

For reasons of national security and economic well-being, governments need to enable, promote, and ensure the protection of their critical information infrastructures. Today, information infrastructures cross nations' industrial sectors and national borders. The ubiquity of the critical information infrastructures creates tremendous opportunity and economic advantages.

With these benefits also come costly interdependencies and risks. A study commissioned by the ITU Telecommunication Development Bureau (BDT) summarized these costs as follows[7]:

> The costs and revenues of all stakeholders across the value network of information services, such as software vendors, network operators, Internet Service Providers (ISPs), and users, are affected by malware and spam. These impacts may include, but are not limited to, the costs of preventative measures, the costs of remediation, the direct costs of bandwidth and equipment, and the opportunity costs of congestion. This is further complicated by the fact that spam and malware also create new revenue streams, both legitimate and illegitimate. They enable legitimate business models (e.g., anti-virus and anti-spam products, infrastructure, and bandwidth) as well as criminal business models (renting out of botnets, commissions on spam-induced sales, pump and dump stock schemes, etc.). Consequently, they create mixed, sometimes conflicting incentives for stakeholders, which complicate coherent responses to the problem.

For many years most nations have treated the national public switched telephone network (PSTN) as a critical infrastructure and have protected it accordingly. In many countries, commercial firms own significant portions of this PSTN infrastructure and have cooperated with the government and each other in this effort. However, the rapid rise of digitally-based ICTs in interconnected wired and wireless communication networks has dramatically changed the nature and requirements for network security and may have made traditional PSTN-based security policies and procedures insufficient to meet new requirements for such security.

The changes brought about by ICTs require a much greater emphasis on cooperation by governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks. While governments often continue to have the lead role in establishing public policy related to network security, it is critical to ensure that other relevant stakeholders, including infrastructure operators and vendors, are integrated into the overall planning and policy process. By working together, government and the private sector can effectively leverage their respective expertise and manage CII risks. This integration fosters increased trust and ensures that policies and technologies are developed and applied in the appropriate and most effective manner. At the international level, protecting critical information infrastructures and enhancing cybersecurity requires cooperation and coordination among nation states and with international partners.

I.A Overview of the Goals under this Part

I.A.1 Create awareness at a national policy level about cybersecurity issues and the need for national action and international cooperation.

I.A.2 Develop a national strategy to enhance cybersecurity to reduce the risks and effects of both cyber and physical disruptions.

---

[7] See the Draft Study "Financial Aspects of Network Security: Malware and Spam", ITU-D 1/144 (6 May 2008).

I.A.3 Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.

I.B Specific Steps to Achieve these Goals

The foregoing goals are common to all countries; however, the specific steps taken to implement these goals will vary according to each country's unique needs and circumstances. In many countries, the national government will undertake these steps.

I.B.1 Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy-level discussions.

1) For a nation seeking to enhance cybersecurity and secure its critical information infrastructure, a first step is to establish cybersecurity as national policy. In general a national cybersecurity policy statement (1) recognizes the importance of CII to the nation, (2) identifies the risks it faces (usually an all-hazards approach[8]), (3) establishes the cybersecurity policy goal, and (4) broadly identifies how it will be implemented, including through collaboration with relevant stakeholders.

   Once an overall cybersecurity policy is clearly defined, it can be amplified by a national strategy that delineates roles and responsibilities, identifies priorities, and establishes timeframes and metrics for implementation. Additionally, the policy and strategy may also place the national efforts in the context of other international cybersecurity activities. In order to achieve an overall cybersecurity policy, it may be necessary to raise awareness of the issues among key decision makers. The decision makers need to understand that it may take a long period to achieve the agreed upon cybersecurity goals.

2) A national cybersecurity framework should not be comprised of immutable policies. Instead, the framework and policies should be flexible and able to respond to the dynamic risk environment. The framework should establish policy goals. By establishing clear policy goals, government agencies and non-government entities can work together to achieve the stated goals in the most efficient and effective manner.

3) This national policy should be developed cooperatively through consultation with representatives of all relevant participant groups including government agencies, the private sector, academia, and relevant associations. This policy should be promulgated at the national level, preferably by the head of government.

I.B.2 Identify a lead person and institution for the overall national effort; determine where within the government a Computer Security Incident Response Team[9] with national responsibility[10] should be established; and identify lead institutions for each aspect of the national strategy.

1) The launch of a cybersecurity initiative requires the identification of someone in the initial phase to lead the national cybersecurity effort, a person in government at the policy level who understands the issues of cybersecurity and who can direct and coordinate the efforts of governmental institutions and can effectively interact with the private sector. Ideally this person should have political stature and access to the head of government. This high-level authority is necessary to ensure the coordination among entities that need to interact. In time, this coordination effort will provide an institutional foundation on which the country's cyber security technical leaders and organizations can build.

---

[8] An all-hazards or multi-hazards approach to risk management includes consideration of all potential natural and technological hazards; this includes natural and manmade (accidental or intentional) emergencies and disasters.

[9] A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and assist their constituents to recover from breaches (A Step-by-Step Approach on How to Set Up a CSIRT is at:http://www.enisa.europa.eu/act/cert). CSIRTS are also sometimes called Computer Emergency Response Teams or Computer Emergency Readiness Teams (CERTs), CSIRTS and CERTS perform the same function. The term 'computer' in CSIRT is used inclusively in this report to encompass, for example, routers, servers, IP-mobile devices, and related applications.

[10] For the purposes of this Report, a nationally designated CSIRT will be referred to as an "CIRT".

2) Once the nation has launched a cybersecurity initiative, the person or institution that launched the effort may no longer need to play such a role.

3) Other institutions responsible for developing and implementing different parts of a national security strategy must be identified.

I.B.3 Identify the appropriate experts and policymakers within government authorities, and private sector, and their roles.

1) Effective national action requires the inculcation of a "culture of cybersecurity" among all participants. All individuals and institutions within government and outside of government that develop, own, provide, manage, service, and use information systems and networks must understand the role they need to play and the actions that need to be taken. Senior policymakers and leaders of the private sector must establish goals and priorities within their institutions. Senior technical experts must provide guidelines and frameworks for action.

I.B.4 Identify cooperative arrangements for and among all participants.

1) National government should foster both formal and informal collaborative arrangements that permit and encourage communication and information-sharing between the private sector and government. Cybersecurity will be implemented at the technical or operational level by a wide array of institutions, both governmental and non-governmental. These efforts must also be coordinated and include mechanisms for information sharing.

I.B.5 Establish mechanisms for cooperation among government and private sector entities at the national level.

1) Policy development and the elaboration and implementation of the national plan must be undertaken through open and transparent processes. These efforts must take into account the views and interest of all participants.

I.B.6 Identify international counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts, taking into consideration the results of the Project implementing Resolution 45 of WTDC-06.

1) The effort to improve national cybersecurity will be helped by participating in regional or international forums that can provide education and training, often in the form of conferences and workshops. Such forums raise awareness of the issues, provide expert presentations and permit countries to share their ideas, experiences and perspectives. Participation and/or membership in regional as well as international organizations working toward similar goals can also assist in this effort. This is one of the aims of the Resolution 45 project.

2) Participation in available programs and activities of multilateral organizations that seek to improve and enhance global cybersecurity is another way to foster international collaboration. Examples of multilateral organizations include the International Telecommunication Union (WSIS Action Line C5), Organization for Economic Cooperation and Development (OECD), Organization of American States (OAS), and Asia-Pacific Economic Cooperation (APEC), etc. In addition, there are other conferences where governments can share information on cybersecurity issues, such as the Meridian Conference.

3) In addition, participation in efforts led by the private sector, such as the Anti-Phishing Working Group and other similar international endeavours, also should be considered.

I.B.7 Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.

1) Only by understanding risks can government and infrastructure owners and operators (including the vendors who support them) begin a public-private-peoples collaboration to identify and prioritize key functions and elements for protection. Once identified, the critical information infrastructure functions can be prioritized or ranked as to which is most important and in what context. It is important to remember that the notion of "criticality" is situation-dependent, and what could be critical in one instance may not be critical in the next. As nations identify and prioritize critical

functions, they need to remember that criticality will change with technology, infrastructure, and process enhancements.

2) Achieving the protection of CII and cyberspace is very challenging. Protecting CII and cyberspace and the critical functions comprised therein involves the continuous application of a series of risk management practices (i.e., assessing threat, vulnerability, and consequence, identifying controls and mitigations, implementing controls, and measuring effectiveness) that enable operators to manage risks and ensure resilience across their essential missions. Individually, information infrastructure providers generally have sophisticated risk management methodologies and practices in place because of the real-time nature of the services they deliver. However, the interconnectivity, interdependence, and technical complexity of the information infrastructure limit the ability to easily assess overall risk or readiness. As a result, there is a significant benefit to leveraging public-private collaborations to assess the shared dependencies and infrastructure risks (natural disaster, technological failure, terrorist attack, etc.).

I.B.8 Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities.

1) The national cybersecurity strategy should include a national assessment survey, which could be used for self-evaluation of progress being made or as part of training or supported assessment effort. By utilizing a common self-assessment tool, countries can identify strengths and potential gaps in their national framework and establish a process for aligning them with their desired goals. (A self-assessment tool, the ITU National Cybersecurity/CIIP Self-Assessment Tool has been developed by BDT to accompany this best practices document.)

I.B.9 Identify training requirements and how to achieve them.

1) As a result of comparing the recommended best practices contained in this report with its current cybersecurity practices (i.e., conducting a gap analysis), a country may find there are aspects of its cybersecurity program that need improvement. The solution may be technical (for example, new equipment or software), legal (e.g., drafting new laws or regulations to address inappropriate cyber conduct), or organizational. A gap analysis is also likely to reveal where additional human capacity building (training) is needed.

PART II

Establishing Collaboration Between National Government and the Private Sector

Protecting critical information infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government at all levels and the private sector, which owns and operates much of the infrastructure. Of course, governments must have the final say on any national decisions that are made. It is important to recognize that although the world's information security systems have largely become an interoperable and interconnected whole, the structure of this network can vary greatly from country to country. Therefore, an effective and sustainable system of security will be enhanced by collaboration among owners and operators of these systems.

Both the government and the private sector have an enduring interest in assuring the resilience of the infrastructure. Accordingly, a public-private partnership is fundamental to enhancing cyber security because no one entity alone can protect the entire infrastructure. As much of the cyber infrastructure in many countries is owned and/or operated by the private sector, it is recommended that government and the private sector, each within its respective role, work together in a meaningful way. Successful public-private collaboration requires three important elements: (1) a clear value proposition; (2) clearly delineated roles and responsibilities; and (3) trust.

Value proposition

The success of the partnership depends on articulating the mutual benefits to government and private sector partners. The benefits to governments are that infrastructure vendors and operators provide capabilities that typically fall outside government's core competencies, such as:

- Ownership and management of the majority of the critical infrastructure in many sectors, in many countries;
- Understanding of assets, networks, systems, facilities, functions, and other capabilities;
- Incident response expertise and experience;
- Ability to innovate and provide products, services, and technologies to quickly focus on requirements; and
- Design, deployment, operation, administration and maintenance of the global Internet.

In assessing the value proposition for the private sector, there is a clear benefit to working with government to enhance CIIP and cybersecurity. Governments can bring value to the collaborative relationship in a number of ways, which include:

- Providing owners and operators with timely, analytical, accurate, aggregated, and useful information on critical infrastructure threats;
- Engaging the private sector at the outset in the development of CIP initiatives and policies;
- Articulating to corporate leaders, through the use of public platforms and direct communications, both the business and national security benefits of investing in security measures that exceed their specific business strategies;
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices and, as needed, to update and enhance their security operations and practices beyond what their parochial business interests demand;
- Working with the private sector to develop and clearly prioritize key missions and enable their protection an/or restoration;
- Providing support for research needed to enhance future CI protection efforts;

- Identifying the resources to engage in cross-sector interdependency studies, through exercises, symposiums, training sessions, and computer modelling, that result in guided decision support for business continuity planning; and
- Enabling time-sensitive information sharing as well as restoration and recovery support to priority infrastructure facilities and services during an incident.

Roles and Responsibilities

Together, government and the private sector can develop a common understanding of their respective roles and responsibilities related to cybersecurity. The government can provide coordination and leadership of protection efforts. For example, continuity of government requires ensuring the security and availability of governments' cyber and physical infrastructure necessary to support its essential missions and services. In addition, the government can play a key coordinating role during a catastrophic event or it can help in instances when the private sector lacks sufficient resources to respond to an incident. The government can promote and encourage voluntary private sector efforts to improve security, including establishing the policies and protocol needed to share timely analytical and useable information about threats, and providing incentives for the private sector to enhance security beyond what their corporate interests demand. Finally, the government can sponsor and fund studies and research and development to improve security processes and tools.

Trust

A fundamental element of successful collaboration between government and the private sector is trust. Trust is necessary for establishing, developing, and maintaining sharing relationships between government and the private sector. Robust collaboration and information exchange between the private sector and government enhances situational awareness, facilitates cooperation on strategic issues, helps manage cyber risk and supports response and recovery activities. Through improved information sharing and analysis, both the government and the private sector will be better equipped to identify threats and vulnerabilities, and to exchange mitigating and preventive tactics and resources.

Listed below are general goals which governments should consider as they collaborate with the private sector.

II.A Overview of the Goals under this Part

II.A.1 Develop public-private collaborative relationships that work to effectively manage cyber risk and to protect cyberspace.

II.A.2 Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.

II.B Specific Steps to Achieve these Goals

II.B.1 Include the private sector perspectives in the earliest stages of development and implementation of security policy and related efforts.

1) In numerous countries, most critical infrastructures, and the cyber elements on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private sector innovation. Therefore, governments alone cannot sufficiently secure cyberspace. Awareness of the private sector perspectives and inclusion of the primary owners and operators of critical infrastructure are invaluable for government cybersecurity efforts to develop and implement cyber security policy and frameworks for risk management. Governments can be informed by the private sector through participating in government-the private sector working groups, soliciting comments from the private sector for cyber security 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.

2) Governments and the private sector should collaboratively adopt a risk management approach that enables government and the private sector to identify cyber infrastructure, analyze threats, assess vulnerabilities, evaluate consequences, and identify mitigations.

3) Governments and the private sector should collaboratively pursue research and development (R&D) activities that seek to manage cyber risk. Visibility into R&D priorities and initiatives being undertaken by the private sector and government can ensure that resources are allocated and used efficiently, that R&D initiatives are developed on a timely basis, and ultimately, that products and services are in the pipeline in time to enhance national cyber security.

II.B.2 Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government.

1) The formation of these groups, such as business associations, in various critical infrastructure sectors can help to address common cybersecurity needs. These groups may focus on strategic and/or operational issues and management of security concerns relative to the private sector as a whole. These issues may include risk management, awareness, policy development and implementation, and a multitude of others. Such private sector groups provide an institutionalized process for engagement with government and can serve as a forum for sensitive dialogue on cyber security matters.

2) In some countries, groups have been established by several critical infrastructure sectors to bring sector representatives together to share information on security threats, vulnerabilities, and impacts. Often, these groups also provide real-time alerts and warning to members to facilitate efforts to mitigate, respond to, and recover from actual incidents impacting the critical infrastructures.

3) These groups should consider adopting practices that enable collaboration and information exchange among members (i.e., government and private sector) in a trusted forum. Some of these practices may include providing the following: anonymity for members; access to cross sector and government information; access to sensitive threat, vulnerability, and analytical products; and subject matter expertise on emergency response coordination, operational practices, and exercises. While considering these practices to enable collaboration, it is important to incorporate means for the protection or proprietary and business-sensitive information.

II.B.3 Bring private sector groups and government together in trusted forums to address common cybersecurity challenges.

1) Several conditions are necessary to build trust and promote successful collaboration between government and the private sector. A written agreement that guides the collaboration and exchange between government and the private sector is recommended. Participants need a shared vision and purpose. Strong individual or organizational leadership sets priorities, allocates resources, and makes commitments necessary to sustain public-private collaboration. Rules of engagement are also needed to guide individual and organizational behaviour within the collaborative relationship.

2) Participants must see tangible and measurable outcomes. Creating a value proposition for the collaboration for individuals and organizations and clearly articulating that value is key to the development and maintenance of [public-private] collaborative relationships.

II.B.4 Encourage cooperation among groups from interdependent industries.

1) Incidents involving one kind of infrastructure can have cascading effects and result in incidents in other kinds of infrastructures. For example, power outages may disrupt telephone and Internet services. Moreover, although people may plan for emergencies in their own sector, they must also consider the impact that incidents may have on other sectors. Sharing information across infrastructures can help efforts to respond to incidents that cut across multiple sectors and are nationally significant.

II.B.5 Establish cooperative arrangements between government and the private sector for incident management.

1) Rapid identification, information exchange, and remediation can often diminish the damage caused by cyber incidents. At the national level, [public-private] collaboration is needed to conduct analyses, issue warnings, and coordinate response efforts.

2) Governments and industry should collaboratively develop a framework for strategic, operational, and awareness coordination for improving incident management. This framework should contain a formal construct for sharing information that includes focal points for policy-related issues and operational information exchange. The framework should also include policies and procedures for sharing and reporting incidents, protecting and disseminating sensitive (government and the private sector) proprietary information, and mechanisms for communicating and disseminating information. Private sector information often contains company proprietary information that if released to the public could result in lost market share, adverse publicity, or other negative consequences. Similarly, government information may be classified or sensitive and not for release to the public. Policy and technical measures to safeguard information while balancing the public's right to know should be put in place. Governments can continue to build trust by enhancing information sharing policies and private sector relationships through continual evaluation of policies. Cyber exercises can also test communications between government and the private sector and coordination related to cyber incident response and recovery efforts by exercising mechanisms deployed in times of real crisis.

PART III

Deterring Cybercrime

Cybersecurity can be greatly improved through, among other means, the establishment and modernization of supporting, criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.

III.A Overview of the Goal under this Part

III.A.1 Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime.

Every country needs laws that address cybercrime per se, the procedures for electronic investigations, and assistance to other countries. These laws may or may not be in a single place in a country's code. For simplicity's sake, this document assumes that each country will have one primary cybercrime statute plus a collection of related procedural and mutual assistance legal texts. Of course, countries should use whatever structure they determine is best suited to their national circumstance.

III.B Specific Steps to Achieving this Goal

III.B.1 Assess the current legal authorities for adequacy. A country should review its existing criminal code, including relevant procedures, to determine if it is adequate to address current (and future) problems. Suggested steps:

1) To develop, as appropriate, the necessary relevant legislation, noting in particular regional initiatives. Such law should address among other issues, damaging or destroying computer data; procedural mechanisms supporting investigations and including the ability to trace the source of e-mail messages, etc.; and including possible international legal cooperation (for example, procuring evidence, etc.)

2) A country should consider whether its laws rely on outdated technological expectations. For example, a law may discuss the tracing of voice transmissions only. Such a law may need to be changed to cover transmissions of data as well.

3) A country's cybercrime law should be evaluated by all relevant government authorities and legislative bodies that might have an interest in it, even if they have nothing to do with criminal justice, so that no useful idea is missed. An information technology official might notice, for example, that the cybercrime law is inadequate to reach a new technology that is coming into increasing use but is not yet widely known to legal drafters in that country.

4) In addition it is recommended that a country's existing criminal law should similarly be evaluated by some or all of the following: the local private sector, any local affiliate of the international private sector, local non-governmental organizations, academics, and recognized experts or groups of citizens.

5) A country may seek advice on such issues from other countries.

III.B.2 Draft and adopt substantive, procedural and mutual assistance laws and policies to address cybercrime.

1) Recommend that countries participate actively in developing, as appropriate, the necessary legislation, noting in particular regional initiatives, including but not limited to, the Council of Europe Convention on Cybercrime. Recommend that countries engage in regional and international collaboration in order to combat cybercrime and strengthen cybersecurity, and to develop mechanisms for enhancing cooperation in cybersecurity, including combating spam, malware, botnets, etc.

2) A country's draft cybercrime law should be evaluated by all government authorities and legislative bodies. Such a draft should also be publicly available for comment in order to address any possible technologies, infractions or other relevant issues, which were not originally covered.

3) Any cybercrime statute should address not merely classic cyber crimes, such as computer crimes and computer intrusions, but also protect electronic evidence on networks regarding other crimes.

4) Data protection laws written for civil and commercial life should not be extended or interpreted to impede inappropriately the flow of criminal evidence between countries.

5) Countries that decide to hire consultants to do the drafting should consider their qualifications and supervise their work throughout the process. Persons who have not been trained specifically under the law of a country may not adequately integrate all the necessary provisions, especially procedural and mutual legal assistance sections. Moreover, persons who do not have prosecutorial experience are unlikely adequately to consider the practicalities of proving a case. Some consultants are qualified to assist in drafting electronic commerce laws but not criminal laws.

6) Other countries may be consulted for suggestions beyond what is contained in the convention. For example, countries may require Internet service providers to retain some of the data transiting their systems for some period, often six months; or they may require computer incidents of a certain significance to be reported to government authorities; or they may require proper identification before a person uses a cybercafé.

7) If time permits, a country may seek comments on the draft cybercrime law (or amendments) from other countries and multilateral organizations. Such comments can be obtained privately and, as noted above, it is helpful to obtain the viewpoints of several countries based on their experience.

8) At the earliest possible stage (consistent with national procedures), a country may seek comments also from those concerned with a recognized interest in the subject matter: the local private sector, any local affiliate of the international private sector, local non-governmental organizations, academics, unaffiliated interested citizens, and others.

III.B.3 Establish or identify national cybercrime units.

1) It is important for every country, regardless of the level of development, to have at least a basic cybercrime investigation capacity. For example, the use of cell phones has expanded rapidly in developing countries, and cell phones can be used to commit fraud, to transfer money, to conspire, to transmit viruses to electronic networks, to set off explosives, etc.

2) Each country should select or train a cybercrime investigative unit that will have competence for national cybercrime investigations. Sometimes it will be obvious which law enforcement service or services this should be. Sometimes competing law enforcement agencies will disagree over the selection and senior authorities will have to make a difficult decision. Even if it appears that the country does not currently have anyone with the necessary skills, it is normally true that there is a law enforcement officer somewhere who is interested in electronic technology and is ambitious to learn more and go further with the field.

3) Cybercrime investigative units, even if they consist of only a limited number of investigators, require support. They require relatively up-to-date equipment, reasonably reliable network connections, and continuing training. Such support may come from the government of the country; from international organizations or other countries; and from private sector donations.

4) Where possible, it is advisable for units to have at least basic computer forensic capacity. Such capacity will require software tools and additional training. (If forensic capacity is considered impossible to achieve, countries should accept beforehand that crucial evidence, even in crucial cases, may be lost.) In some circumstances, forensic assistance for specific cases may be available from other countries. In addition, training in cyberforensics may be available both from other countries and from relevant organizations. For example, the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University in the United States (http://www.cert.org) offers some cyber forensics training for free or at very low prices online or by CD-ROM.

5) Once a cybercrime unit is set up, it should publicize its existence and capabilities to other law enforcement services and to prosecutors in the country. It is not useful to have a cybercrime unit in the capital if a regional law enforcement force is investigating a terrible crime that involves electronic evidence but does not know that there is a cybercrime unit that could search the target's

computer or offer other help. Unfortunately, it is very common worldwide that a country's law enforcement establishment is unaware that the country possesses a cybercrime unit.

6) Cybercrime units or potential units should foster relationships with international partners to the greatest possible extent. At initial stages, advice about setting up the unit is available from other countries and from international law enforcement organizations. At later stages, training of many types and even equipment and software are available from other countries, from international law enforcement organizations, from relevant multilateral organizations, and from the private sector. Such contacts will also be valuable for another reason: in a world that will become more and more networked, it is critical to be able to request assistance from foreign law enforcement.

7) Cybercrime units should also take up contact with every relevant and interested sector within their countries, for example domestic non-governmental organizations, computer security incident response teams, private sector entities, and academia, to ensure they know of the unit's existence and capabilities, can collaborate with it, and understand how to report possible cybercrime.

III.B.4 Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector.

1) Cooperative relationships among government authorities, other elements of the national cybersecurity infrastructure and the private sector are important for several reasons:
   a) to exchange information between these groups (for example, to advise that a new law is contemplated or a new technology is in development.
   b) to exchange opinions (for example, "If we draft a new law along those lines, would you see any privacy problems with it?" or "Is there any way you can alter that technology so that email traces can still be done if there are legitimate public safety reasons?")
   c) to exchange training, though most often training will be offered by the private sector to the government
   d) to exchange warnings about threats or vulnerabilities
   e) so that people from different sectors will get to know each other well enough to trust one another in emergencies.

2) A good first step in forming such relationships is for one or more people to create a list of people and organizations in the country with specific cyber skills and responsibilities in all of the relevant sectors. Contact information for those people can then be noted on the list. It is probably best to keep such a list informal to avoid struggles over who is and who is not on the list.

3) In every country, there are likely to be numerous relevant sectors that have a helpful focus on cybersecurity – legislators, ministries, non-governmental organizations, computer security incident response teams, academia, the private sector, and individuals. Some of these may be wholly domestic and some may be affiliated with larger foreign entities.

III.B.5 Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.

1) To address cybercrime issues properly it is important that prosecutors and judges have some understanding of areas such as computers, software, and networks as well as of the increasing importance of electronic evidence. Similarly, legislators should have some understanding of those topics and of whether a country's laws are adequate to address cybercrime. One solution to this problem is training.

2) If basic technical training is required, it can come from a variety of sources, depending on the country's resources:
   a) any domestic service or ministry with technical competence, such as a law enforcement service or an information technology ministry;
   b) foreign governments;
   c) relevant multinational organizations;
   d) the local private sector;
   e) the international private sector, especially (but not exclusively) if it does business locally;
   f) relevant academia;
   g) domestic or foreign computer security incident response teams; and

h) domestic and foreign relevant non-governmental organizations.

3) It may also be helpful to train senior policy-makers, government officials, etc, about the threats to electronic networks (for example, how the national banking system could be attacked) and about the threats posed by electronic networks (for example, the use of the Internet to locate vulnerable children for sexual trafficking). Training regarding these aspects of electronic networks should be available from the sources above.

4) Training may be desired for prosecutors and judges regarding prosecution of cybercrime or other crime involving electronic evidence, or of the use of electronic evidence, or of methods of obtaining international cooperation. Such training may be available from:

a) any domestic service or ministry with the correct competence, such as a prosecutor's office or a justice ministry;
b) foreign governments;
c) relevant multinational organizations;
d) relevant academia;
e) relevant domestic and foreign non-governmental organizations, and
g) relevant individuals.

5) A country may wish to have training in legislative drafting. Such training may be available from the groups listed in the paragraph above. The local private sector and the international private sector, especially (but not exclusively) if it does business locally, may be possible sources of expertise. However, it is more likely that the private sector entities will be able to assist with electronic commerce laws than with cybercrime, criminal procedure, and international mutual legal assistance laws.

6) For all of these types of training, the sources may offer to give the training themselves in the requesting country or they may offer training modules (electronic or printed) that instructors from that country can use in doing the training themselves. In some cases, as with the CERT-CC training described at section III.B.3.4, such training can be provided without charge or with minimal charge.

7) In some countries, the key to national awareness of cybercrime issues has been the support of senior officials, or sometimes even one powerful senior official, particularly those who control budgets. If it is well-known that a minister is very interested in cybersecurity, his or her ministry – and perhaps the rest of the government – may offer better support to working-level people who are trying to accomplish something in the field.

III.B.6 Participate in the 24/7 Cybercrime Point of Contact Network.

1) In 1997, the Group of Eight major industrialized countries (G8) Subgroup on High-Tech Crime started the 24/7 Cybercrime Point of Contact Network at the direction of the Justice and Interior Ministers of the G8 to improve international assistance in urgent investigations that involve electronic evidence. Many cybercrime investigators felt that it was too difficult to learn where to obtain quick assistance from other countries. In addition, many investigators felt that decades-old mutual legal assistance treaties were not helpful for fast-moving cases involving, for example, midnight computer intrusions into a country's financial systems. This network has grown to include about 50 countries as of early 2008. The network is open to any country with the necessary capacity to assist as described below.

2) To join the network, countries must offer a contact point reachable twenty-four hours a day, seven days a week – thus the informal name, "the 24/7 network." The contact point can be a person who is reached directly or via an office. S/he must understand three things: 1) technology, so that requests can be transmitted without the delay of lengthy technological explanation; 2) his/her own domestic law; and 3) what domestic law allows him/her to do to assist other countries. If the contact point does not personally have these three types of knowledge, s/he must be able to reach any capable person in his/her government immediately, if necessary (not merely the next business day) who is authorized to assist.

3) Communications must go, at least initially, from the 24/7 contact point in Country A to the 24/7 contact point in Country B to ensure consistency and security. This means that contact points should not give out the contact information to other offices in their own countries. Rather, contact points should make the first international contact on behalf of a requesting office (for example, a provincial law enforcement force) in their countries. After initial cooperation between two countries has been established, a contact point may, if desired, withdraw from the investigation and let the relevant provincial law enforcement in Country A communicate directly with Country B.

4) By joining the network, countries do not guarantee that they will always assist each other, nor does the contact network replace normal mutual legal assistance between countries. Rather, the contact network guarantees only that a requesting country will receive intelligent, capable attention immediately, even in the middle of the night. After any initial assistance, countries may (or may not) require that slower mutual assistance channels be used.

5) Twenty-four-hour-a-day availability does not mean that an office is staffed day and night with a certain number of computer workstations and cyber investigators waiting to answer telephone calls or emails. Most countries do not operate such an office. More commonly, one law enforcement officer (possibly different officers on a rotating basis) in a country will be reachable by telephone – perhaps sleeping with a cell phone nearby.

6) To join, countries should contact the chair of the High-Tech Crime Subgroup of the G8 (membership is not restricted to G8 members; rather, almost 50 countries already belong. A short, simple form must be completed.[11] The process does not require formal international agreements such as memoranda of understanding or treaties. From time to time, the 24/7 network offers training and networking conferences for the contact points. Travel to these conferences has been subsidized as needed.

7) The unit that joins the network has the responsibility to let local or national law enforcement services or cybercrime units in its country know of its existence and of its availability to assist in making contacts outside the country.

[11] The form should be faxed to +1 202-514-6113, addressed to Coordinator, 24/7 Network, Computer Crime and Intellectual Property Section, US Dept of Justice, Washington, D.C., U.S.A. It may also be sent by email to richard.green@usdoj.gov

PART IV

Creating National Incident Management Capabilities: Watch, Warning, Response and Recovery

It is important for the government to create or identify a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, the private sector, academia, and the international community.

A key role for government in addressing cybersecurity at the national level pertains to preparing for, detecting, managing, and responding to cyber incidents that occur. Implementing an incident management mechanism requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, and international organizations is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Government has the key role in ensuring coordination among these entities.

IV.A Overview of the Goals under this Part

Establishing national incident management capabilities requires a series of closely related activities, including:

IV.A.1 Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to, and recover from cyber incidents.

IV.A.2 Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents.

IV.A.3 Participate in watch, warning, and incident response information sharing mechanisms.

IV.A.4 Develop, test, and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.

IV.B Specific Steps to Achieve these Goals

The development of a national incident management capability is a long-term effort that begins with establishing a national computer incident response team (CIRT)[12,13].

IV.B.1 Identify or establish a national CIRT capability.

1) Effective response to a significant cyber incident may limit the damage to information systems, ensure an effective means of responding, and reduce the length and cost of recovery. In conjunction with public and private sectors, an CIRT is needed as a focal point within government, especially in incidents of national significance, to coordinate defence against and response to cyber incidents. In these instances, CIRTs must work together with appropriate authorities, but would not direct or control their activities.

2) An CIRT is expected to provide services and support to prevent and respond to cyber security-related issues and serves as a single point of contact for cyber security incident reporting, coordination, and communications. The mission of an CIRT should include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for

---

[12] See WTSA Resolution 58. In some countries a CIRT is called a national computer security incidence response team (NCSIRT) or a national security incident response team (N-SIRT).

[13] The results of the work to be performed by the ITU-T under Resolution 58 may affect Part IV of these best practices.

critical information infrastructure. Specifically, an CIRT should perform several functions at the national level including but not limited to:

- detecting and identifying anomalous activity;
- analyzing cyber threats and vulnerabilities and disseminating cyber threat warning information;
- analyzing and synthesizing incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders;
- establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues;
- providing early warning information, including information about mitigating vulnerabilities and potential problems;
- developing mitigation and response strategies and effecting a coordinated response to the incident;
- sharing data and information about the incident and corresponding responses;
- tracking and monitoring information to determine trends and long term remediation strategies; and
- publicizing general cyber security best practices and guidance for incident response and prevention.

IV.B.2 Establish mechanism(s) within government for coordination among civilian and government agencies.

1) A key role for an CIRT is to disseminate information, including information about current vulnerabilities and threats, to interested stakeholders. One stakeholder community that must be engaged in response activities is relevant government agencies.

2) Effective coordination with these entities can take a number of forms, for example: maintaining a website for exchanging information; providing information via mailing lists, including newsletters, trends and analysis reports; producing publications that include alerts, tips, and information about various aspects of cyber security including new technologies, vulnerabilities, threats, and consequences.

IV.B.3 Establish collaborative relationships with the private sector to prepare for, detect, respond to, and recover from national cyber incidents.

1) The government and CIRT must collaborate with the private sector. As the private sector in many countries owns much of the critical information infrastructure and information technology assets, government must work with [the private sector] to achieve its overarching goal of effective incident management.

2) Collaborative relationships with the private sector that are built on trust allow governments to gain insight into much of the critical infrastructure that is owned and operated by the private sector. Public-private-peoples collaboration can help manage risk associated with cyber threats, vulnerabilities, and consequences and build situational awareness through information sharing, outreach and mutual engagements.

3) Encourage the development of sharing practices between the private sector and government that enable sharing of operational information in real time.

4) A few ways to encourage this collaboration may include identifying the benefits for both government and the private sector, developing and implementing programs that ensure the protection of sensitive proprietary data, establishing public-private working groups on cyber risk management and incident management, sharing incident response/management best practices and training materials, and collaboratively defining government and private sector roles and responsibilities for incident management, to put in place consistent, predictable protocols over time.

IV.B.4 Establish point(s) of contact within government agencies, the private sector and international partners to facilitate consultation, cooperation, and information exchange with the CIRT.

1) Identifying appropriate points of contact and establishing collaborative working relationships for consultation, cooperation, and information exchange are fundamental to a coordinated and effective national and international incident response mechanism. These relationships can promote early warning of potential cyber incidents and exchange of information about trends, threats, and responses among incident response entities and other stakeholders.

2) Maintaining up-to-date points of contacts and communication channels with stakeholder communities can provide proactive, timely information exchange about trends and threats and expedite responses. It is important, to the extent possible, to establish contacts based on departmental functions rather than with individuals to ensure communication channels remain open even when individuals leave an organization. Relationships often begin by establishing trust with particular individuals, but should evolve into more formal, institutional arrangements.

IV.B.5 Participate in international cooperative and information sharing activities.

1) Governments should encourage collaboration with organizations, vendors, and other appropriate subject matter experts to (1) advance incident response as a discipline worldwide, (2) promote and support possibilities for CIRTs to join the existing global and regional conferences and forums, in order to build capacity for improving the state of the art in incident response on a regional basis, and (3) collaborate on the development of materials for establishing national CIRTs and for effectively communicating with the CIRT authorities.

IV.B.6 Develop tools and procedures for the protection of the cyber resources of government entities.

1) Effective incident management also requires the development and implementation of policies, procedures, methodologies, security controls and tools to protect government cyber assets, systems, networks, and functions. For a CIRT, these can include Standard Operating Procedures (SOPs), guidelines for internal and external operations, security policies for coordinating with stakeholders, implementation of secure information networks for CIRT operations, and secure communications. As a focal point for incident response, CIRTs should coordinate with each other and help enable collaboration with other incident response entities. Governments should also provide continual incident response training to new and existing staff.

IV.B.7 Develop a capability through the CIRT for coordination of governmental operations to respond to and recover from large-scale cyber attacks.

1) If there is an incident that rises to the level of national significance, there will be a need for a central point of contact to coordinate with other governmental entities as with other stakeholder communities, such as the private sector. It is important to develop plans and procedures to ensure that the CIRT is prepared to address a possible incident.

IV.B.8 Promote responsible disclosure practices to protect operations and the integrity of the cyber infrastructure

1) Occasionally, vulnerabilities in information technology products such as hardware and software may be discovered. Decisions on public disclosure should be made on a case by case basis so that vulnerability information is not misused. Vendors should be given ample time in advance of any such disclosure to such vulnerabilities.

PART V

Promoting A National Culture of Cybersecurity

Considering that personal computers are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and use information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Government must take a leadership role in bringing about this Culture of Cybersecurity and in supporting the efforts of other participants.

V.A Overview of the Goal under this Part

V.A.1 Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity[14], and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures[15].

1) The promotion of a national culture of security addresses not only the role of government in securing the operation and use of information infrastructures, including government operated systems, but also outreach to the private sector, civil society and individuals. Similarly, this element covers training of users of government and private systems, future improvements in security, and other significant issues including privacy, spam, and malware.

2) According to the OECD, the key drivers for a culture of security at the national level are E-government applications and services, and protection of national critical information infrastructures. As a result, national administrations should implement E-government applications and services to both improve their internal operations and provide better services to the private sector and to citizens. The security of information systems and networks should be addressed not solely from a technological perspective, but should include elements such as risk prevention, risk management, and user awareness. The OECD found that the beneficial impact of E-government activities is moving beyond public administrations towards the private sector and individuals. E-government initiatives appear to have acted as a multiplier fostering the diffusion of a culture of security.

3) Countries through collaborative activities, preferably by some type of agreement, should adopt a multidisciplinary and multi-stakeholder approach to implement cyber security, and some are establishing a high-level governance structure for the implementation of national policies. Awareness raising and education initiatives are considered very important, along with the sharing of best practices, collaboration among participants, and the use of international standards.

4) International cooperation is extremely important in fostering a culture of security, along with the role of regional organizations to facilitate interactions and exchanges.

V.B Specific Steps to Achieve this Goal

V.B.1 Implement a cybersecurity plan for government-operated systems.

1) The initial step for government action to secure government-operated systems involves developing and implementing a national security plan. Preparation of that plan should address risk management, as well as security design and implementation. Periodically, both the plan and its implementation should be reassessed to measure progress and to identify areas where the plan or implementation need improvement. The plan should also include provisions for incident management, including response, watch, warning, and recovery, and information sharing linkages. The security plan should also address action called for in V.B.2 for training of users of these government systems and collaboration among government, the private sector and civil society on

---

[14] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[15] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

security training and initiatives. User awareness and responsibility are the key issues to be addressed by training.

V.B.2 Implement security awareness programs and initiatives for users of systems and networks.

1) An effective national cybersecurity awareness program should promote cyber security awareness among and within the general public and key communities, maintain relationships with governmental cyber security professionals to share information about cyber security initiatives, and develop collaboration to promote collaboration on cyber security issues. There are three functional components to consider when developing an awareness program: (1) stakeholder outreach and engagement, which builds and maintains trusted relationships among and between the private sector, government, and academia to raise cyber security awareness and effectively secure cyberspace; (2) coordination, which works to ensure collaboration on cybersecurity events and activities across the government; and (3) communications and messaging, which focuses on development of internal (within the government agency responsible for this program) and external communications (other government agencies, industry, educational institutions, home computer users, and general public).

V.B.3 Encourage the development of a culture of security in business enterprises.

1) Developing a Culture of Security in business enterprises can be achieved in a number of innovative ways. Many government initiatives have been directed at awareness-raising for small and medium-sized enterprises. Government dialogue with business associations or public-private-people collaboration can help administrations design and implement education and training initiatives. Examples of such initiatives include: making information available (off line and online), e.g. booklets, manuals, handbooks, model policies and concepts; setting up web sites specifically targeted at SMEs and other stakeholders; provision of (online) training; provision of an online self-assessment tool; and offering financial assistance and tax support or other incentives for fostering the production of secure systems or taking proactive steps toward enhancing cyber security.

V.B.4 Support outreach to civil society with special attention to the needs of children and youths, persons with disabilities, and individual users.

1) Some governments have cooperated with the business sector to raise citizens' awareness of emerging threats and measures that should be taken to counter them. Some countries organize specific events, such as an information security day, week, or month with activities planned to promote information security to a broad audience, including the general public. Most initiatives aim to educate children and students either through school mechanisms including teachers, professors and parents, or by direct distribution of guidance material. The support material used varies from web sites, games, and online tools, to postcards, textbooks, and diplomas for exams taken. Examples of such initiatives include delivering training courses to parents to inform them about security risks; providing support material for teachers; providing children with tools to play online while receiving educational messages related to information security; developing textbooks and games; creating an exam and a diploma; and a quiz about how to surf the web safely.

2) Government and the private sector can share the lessons they have learned in developing security plans and training users; learn from others' successes and innovations; and work to improve the security of domestic information infrastructures.

V.B.5 Promote a comprehensive national awareness program so that all participants – businesses, the general workforce, and the general population – secure their own parts of cyberspace.

1) Many information system vulnerabilities exist because of a lack of cyber security awareness on the part of users, system administrators, technology developers, procurement officials, auditors, chief information officers, and corporate boards. These vulnerabilities can present serious risk to the infrastructures even if they are not actually a part of the infrastructure itself. For example, the security awareness of system administrators is often a weak spot in an enterprise security plan. Promoting private sector efforts to train personnel and adopt widely-accepted security certifications for personnel will help reduce these vulnerabilities. Government coordination of national outreach and awareness activities to enable a culture of security will also build trust with the private sector.

Cyber security is a shared responsibility. Portals and websites can be a useful mechanism to promote a national awareness program, enabling government agencies, businesses, and individual consumers to obtain relevant information and carry out measures that will protect their portions of cyberspace.

V.B.6 Enhance Science and Technology (S&T) and Research and Development (R&D) activities.

1) To the extent that government supports science and technology and research and development activities, some of its efforts should be directed towards the security of information infrastructures. Through the identification of cyber R&D priorities, countries can help shape the development of products with security built-in as well as address difficult technical challenges. To the extent that R&D is conducted in an academic institution, there may be opportunities to engage students in cybersecurity initiatives.

V.B.7 Review existing privacy regime and update it to the online environment.

1) This review should consider privacy mechanisms adopted by various countries, and by international organizations, such as the OECD. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, continue to represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line.

V.B.8 Develop awareness of cyber risks and available solutions.

1) Addressing technical issues requires that governments, businesses, civil society and individual users work together to develop and implement measures that incorporate *technological* (i.e., standards), *process* (e.g., voluntary guidelines or mandatory regulations) and *personnel* (i.e., best practices) components.

2) An example of a threat is spam with associated threats such as Malware. A number of organizations, including ITU-T SG17 Question 4, are working on issues regarding spam. Annex A provides a high level overview of this issue.

3) Identity management is an example of a technological tool to address various cybersecurity needs. A number of organizations, including ITU-T SG17 Question 10, are working on identity management. Annex B provides a high level overview of this issue.

Appendix 1

List of acronyms

APECTEL	Asia-Pacific Economic Cooperation Telecommunications and Information Working Group
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (USA)
CCIPS	Computer Crime and Intellectual Property Section (of US Department of Justice)
CERT	Computer Emergency Response Team
CERT-CC	Computer Emergency Response Team Coordination Center (of Carnegie- Mellon University, USA)
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIRT	Computer Incident Response Team
COE	Council of Europe
CPNI	Centre for the Protection of National Infrastructure (UK)
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures List (USA)
DHS	Department of Homeland Security (USA)
DOJ	Department of Justice (USA)
EU	European Union
FAR	Federal Acquisition Regulations (USA)
FCC	Federal Communications Commission (USA)
FIRST	Forum of Incident Response Security Teams
G8	Group of Eight (Nations)
ICT	Information & Communication Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats
ISAC	Information Sharing and Analysis Centers (various, such as IT-ISAC; USA)
IT-ISAC	Information Technology Information Sharing and Analysis Center)
ITAA	Information Technology Association of America
LAP	London Action Plan
MSCM	Mobile Service Commercial Message
NIAC	National Information Assurance Council (of ITAA)
NIATEC	National Information Assurance Training and Education Center (at University of Idaho USA)
NIST	National Institute of Standards and Technology (USA)
NRIC	Network Reliability and Interoperability Council (FCC USA)
NSTAC	National Security and Telecommunications Advisory Committee (DHS USA)
NVD	National Vulnerability Database (USA)

OECD	Organisation for Economic Co-operation and Development
OVAL	Open Vulnerability Assessment Language
PSTN	Public Switched Telecommunication Network
R&D	Research and Development
S&T	Science and Technology
SME	Small and medium-sized enterprise
SMS	Short Message Service
SOP	Standard Operating Procedures
TCPA	Telephone Consumer Protection Act (USA)
UNGA	United Nations General Assembly

Appendix 2

National implementation strategy for cybersecurity cooperation & measures of effectiveness

The approach outlined below uses a program methodology designed to move countries forward in developing strong cyber security systems as a national priority. This methodology is divided into three distinct program stages that will move a country from an initial assessment of capabilities to program implementation and evaluation. This staged approach is set forth below:

Program Methodology for Cybersecurity Cooperation and Measures of Effectiveness

Stage 1 – Assess, evaluate and recommend a plan for a cooperative exchange program.

- **Assess:** The first step is for a country to conduct an assessment of the current status of its security program. This is accomplished by a team of experts using a standardized assessment instrument.
- **Evaluate:** Information gathered during this assessment provides an understanding of the strengths and weaknesses of the country's current cybersecurity program, and determines where efforts should be focused.
- **Recommend:** Understanding gained from the evaluation provides the basis for a plan to meet the country's requirements.

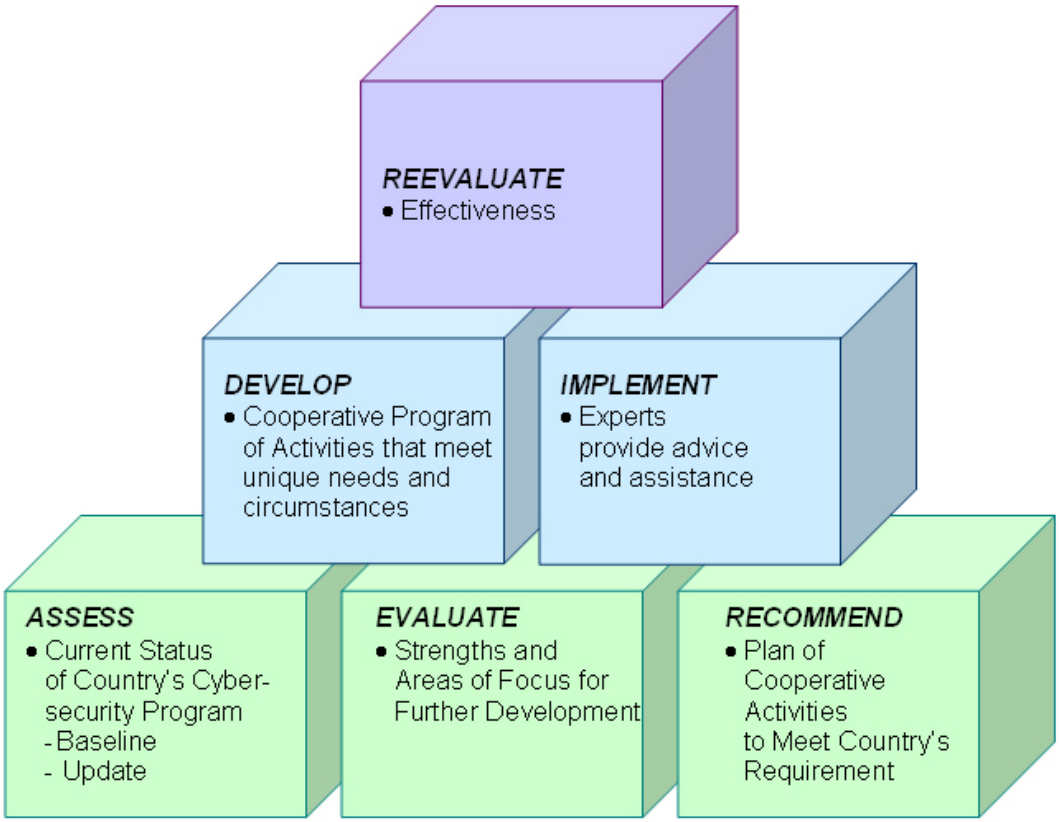
Stage 2 – Cooperative program development and implementation.

- **Cooperative Program Development**: Country experts meet either internally or with international counterparts to design, shape and adjust activities to meet the unique needs and circumstances of the particular country. The activities can encompass a range of cooperative exchange activities and identification of long-term material requirements.
- **Implement Program**: Domestic and perhaps international experts implement the program and offer concrete advice.

Stage 3 – Cooperative program evaluation to measure success and complete the program.

- **Cooperative Program Evaluated**: Periodically, the cybersecurity cooperative program is re-evaluated for effectiveness internally or with country counterparts. Areas deemed deficient may become the subject for further cooperative exchanges and the foregoing process starts over. If a country is cooperating with others, such cooperation can phase out once the country's program is assessed as effective.

Figure 1: Program Methodology for Building Capacity in Cybersecurity



Measures of Effectiveness

The following is one approach to measure performance over time in this area and to demonstrate progress to senior officials. The approach constructs a chain of logic that links basic inputs (country- or region-specific programs that consume time, money and staff resources) to the outcome finally desired (increased cybersecurity). The chain is illustrated below:

Measurement Category:	**Performance Element:**
Basic input:	**Country programs:** • Time • Money • Personnel
Basic work processes:	**Work, including possibly cooperative exchanges, in:** • National Strategy development • Legal framework development • Incident Management • Public-private-people Collaboration • Culture of Cybersecurity

Basic outputs: **Number of:**

- Meetings or cooperative exchanges
- Contacts with senior policy and technical officials

Intermediate results: **Country actions:**

- New cybercrime laws and regulations
- Enforcement actions
- Establishment of CSIRT
- Government-Industry awareness programs
- Incident response inquiries
- Participation in international organizations' cybersecurity activities
- Adherence to international conventions and guidelines

Eventual result: Reduced cybersecurity risk resulting from a national legal and policy framework, incident response, and awareness efforts.

Final outcome: Increased national cybersecurity and global security.

Annex A

Case Study: Spam

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 6
(09/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1240 series – Supplement on countering spam and associated threats

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Supplement 6 to ITU-T X-series Recommendations

ITU-T X.1240 series – Supplement on countering spam and associated threats

Summary

Supplement 6 to ITU-T X-series Recommendations states that in order to deal effectively with spam, governments need to employ a variety of approaches, including effective laws, technological tools, and consumer and business education. This supplement reviews the international forums where the issue of spam is being addressed. As a case study, for illustrative purposes, it provides some information about the way the U.S. and Japan have approached the spam problem.

Source

Supplement 6 to ITU-T X-series Recommendations was agreed on 25 September 2009 by ITU-T Study Group 17 (2009-2012).

CONTENTS

Supplement 6 to ITU-T X-series Recommendations

ITU-T X.1240 series – Supplement on countering spam and associated threats

1 Scope

The topic of this supplement is spam and associated threats. This supplement is intended for national administrators who are newcomers to the concept of spam and would like some basic information about it.

This supplement looks at the tools that need to be employed to combat spam effectively and describes the work that some international forums are doing in this area. It provides, as a case study and for illustrative purposes, a description of what the U.S. and Japan are doing to combat spam.

2 References

None.

3 Definitions

This supplement defines the following terms:

3.1 **phishing**: An attempt to fool an individual into going to the wrong website with the intent of stealing that individual's private information.

3.2 **spam**: Although there is no universally agreed definition of spam, the term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS).

4 Abbreviations and acronyms

This supplement uses the following abbreviations:

ADSP	Author Domain Sending Practices
APEC TEL	Asia-Pacific Economic Community – Telecommunication and Information Working Group
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (U.S.)
CNSA	Contact Network of Spam Authorities (European Union)
DKIM	Domain Keys Identified Mail
FCC	Federal Communications Commission (U.S.)
FTC	Federal Trade Commission (U.S.)
ISP	Internet Service Provider
JEAG	Japan Email Anti-abuse Group (Japan)
LAP	London Action Plan
MAAWG	Messaging Anti-Abuse Working Group
MMS	Multimedia Messaging Service
MSCM	Mobile Service Commercial Messages
OECD	Organization for Economic Co-operation and Development

OP25B	Outbound Port 25 Blocking
SMS	Short Messaging Service
SPF	Sender Policy Framework

5 Conventions

None.

6 Background

6.1 **Spam** has gone from being nuisance communications containing commercial advertisements to a facilitator of a more serious cybersecurity problem. For example, spam can be a vehicle for deception, spreading malware such as viruses and spyware, and inducing consumers to provide confidential information that can later be used to commit identity theft (i.e., phishing). Spammers take advantage of the fact that they can send their messages from anywhere in the world to anyone in the world at an extremely low cost to themselves. This makes spam an international problem that must be addressed through international cooperation.

6.2 **Phishing** takes advantage of the fact that, due to a basic characteristic in the Internet's e-mail system[16], anyone can send e-mail to anyone with almost no form of authentication. Phishing is an attempt to fool someone into going to the wrong website with the intent of stealing that individual's private information. Phishing exists in large part because sometimes people expect to receive e-mail from a popular site and they simply do not realize that the mail is not from the legitimate site. Because there is little authentication in e-mail, it is difficult to determine whether a message is legitimate without careful inspection of the message. Such careful inspection requires substantial knowledge of the underlying mechanisms used on the web.

Phishing also exists because most people find it difficult to verify that the websites they are going to are legitimate. Sometimes we do not look closely at the URL of a web page before entering sensitive information, and sometimes we just do not know what the correct URL should be.

The web servers used to "phish" sensitive information are often themselves the victims of malware, making it again extremely difficult to track phishers.

6.3 **Malware**, or malicious software that is made to run on a device without the knowledge or permission of the owner, is also a substantial problem.

7 National approaches to deal effectively with spam and associated threats

7.1 **National strategy and spam**: With respect to a national strategy, countries should develop and maintain a combination of effective laws, law enforcement authorities and tools, technological tools and best practices, and consumer and business education to effectively deal with spam.

7.2 **Legal and regulatory foundation and spam**: With respect to a legal foundation and regulatory framework, authorities that have jurisdiction over spam must have the necessary authority to investigate and take action against violations of laws related to spam that are committed from their country or cause effects in their country. Authorities that have jurisdiction over spam should also have mechanisms to cooperate with foreign authorities. Requests for assistance from foreign authorities should be prioritized based on areas of common interest and in cases where significant harm occurs.

7.3 **Government-industry collaborations and promotion of national awareness of spam and associated threats**: All interested persons, including enforcement authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of laws related to spam. Government

[16] The Internet e-mail system was designed in the 1970s when access to the Internet was limited to a very few researchers and government members. There was no need to authenticate the identity of individuals sending e-mail, and therefore no effort was made to design the system to do so. While the e-mail system has evolved since then, this basic omission has been present ever since.

enforcement agencies should partner with industry and consumer groups to educate users and promote information sharing. Government enforcement agencies should cooperate with the private sector to promote the development of technological tools to fight spam, including tools to facilitate the location and identification of spammers.

Phishing is often a preventable crime. Governments should work together with the private sector to improve means of protecting citizens from phishing, and educating consumers and businesses on safe authentication methods.

Governments can also play a role in educating the public on the need to keep malware in check by making use of tools such as anti-virus software and by applying the latest operating system patches and trusted computing techniques.

8 International (multilateral) countering spam initiatives

Several multilateral fora are working on initiatives to combat spam. These include:

8.1 London Action Plan

The U.S. Federal Trade Commission (FTC) and U.K. Office of Fair Trading hosted an International Spam Enforcement Conference in London in 2004, which led to the creation of a London Action Plan on International Spam Enforcement Cooperation (LAP). As of July 2008, government agencies and private sector representatives from more than 25 countries have endorsed the plan. The LAP encourages interested parties, including spam enforcement agencies and private sector stakeholders, to consider applying for membership in the organization.

The purpose of the LAP is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. The LAP builds relationships among these entities based on a short document that sets forth a basic work plan for improving international enforcement and education cooperation against illegal spam. This document is non-binding, asking participants only to use best efforts to move the work plan forward. http://londonactionplan.org/

Since its inception, the LAP has held annual workshops, typically in conjunction with the European Union's Contact Network of Spam Authorities (CNSA). In October, 2007, the LAP and CNSA co-located their annual joint workshop with the messaging anti-abuse working group (MAAWG) conference in Arlington, Virginia, which facilitated increased law enforcement cooperation with the private sector. In October 2008, the LAP and CNSA are co-locating their annual joint workshop with Eco's 6th German Anti-Spam Summit in Wiesbaden, Germany.

8.2 OECD Spam Toolkit and Council Recommendation on Spam Enforcement Cooperation

In April 2006, the OECD Spam Task Force released an Anti-Spam "Toolkit", which contains recommendations to help policy makers, regulators and industry players orient their policies relating to spam solutions and restore trust in the Internet and e-mail. The Toolkit contains eight elements, including anti-spam regulation, industry driven solutions and anti-spam technologies, education and awareness, and global cooperation/outreach. Recognizing that international cooperation is key to combating spam, the OECD governments also approved a "Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam", which urges countries to ensure that their laws enable enforcement authorities to share information with other countries and do so more quickly and effectively. http://www.oecd-antispam.org/sommaire.php3.

8.3 APEC TEL Symposium on spam

In April 2006, APEC TEL held a symposium on "Spam and Related Threats" that brought together thirty speakers and panelists to discuss the evolution of the spam problem and establish a common agenda of action for the TEL. The main topics addressed included:

1) the development and application of national anti-spam regulatory regimes, including enforcement and codes of practice;

2) the role of industry in combating spam, including government-industry collaboration;

3) technical responses to spam;

4) cross-border cooperation and enforcement, including the Council of Europe's Convention on Cybercrime and the OECD Council Recommendation on Enforcement Cooperation as primary tools for enhancing cooperation; and

5) the need for targeted consumer education and awareness raising.

Concrete steps the TEL agreed to take going forward included:

1) encouraging information sharing on regulation and policy, drawing on resources such as the OECD Spam Toolkit;

2) developing a contact list for APEC spam authorities to augment similar resources developed by the OECD and the ITU;

3) encouraging economies to apply for membership in voluntary cooperation forums such as the London Action Plan or the Seoul-Melbourne Agreement;

4) cooperating with the OECD on information sharing and guidance-related initiatives; and

5) supporting capacity building for developing economies to better deal with spam.

9 Case study of some activities to counter spam

This clause presents activities for countering spam in some countries.

9.1 United States

9.1.1 Laws establishing requirements for those who send commercial e-mail (CAN-SPAM Act)

In 2003, the United States enacted the "CAN-SPAM Act", which establishes requirements for those who send commercial e-mail, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The main provisions of the CAN-SPAM Act include the following:

- **It bans false or misleading header information**: Your e-mail's "From", "To", and routing information – including the originating domain name and e-mail address – must be accurate and identify the person who initiated the e-mail.
- **It prohibits deceptive subject lines**: The subject line cannot mislead the recipient about the contents or subject matter of the message.
- **It requires that your e-mail give recipients an opt-out method**: You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future e-mail messages to that e-mail address, and you must honour the requests. You may create a "menu" of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial e-mail. When you receive an opt-out request, the law gives you 10 business days to stop sending e-mail to the requestor's e-mail address. You cannot help another entity send e-mail to that address, or have another entity send e-mail on your behalf to that address. Finally, it is illegal for you to sell or transfer the e-mail addresses of people who choose not to receive your e-mail, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.
- **It requires that commercial e-mail be identified as an advertisement and include the sender's valid physical postal address**: Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial e-mail from you. It also must include your valid physical postal address.

The U.S. Federal Trade Commission (FTC) is authorized to use its civil law enforcement authority to enforce the CAN-SPAM Act and to obtain civil penalties of up to USD 11'000 per violation. Since 1997, when the

FTC brought its first enforcement action targeting unsolicited commercial e-mail, or "spam", the FTC actively has pursued deceptive and unfair spam practices through 94 law enforcement actions, 31 of which targeted violators of the CAN-SPAM Act.

CAN-SPAM also gives the Department of Justice the authority to enforce its criminal sanctions. The CAN-SPAM Act provides for significant criminal penalties, including jail time for spammers. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

9.1.2 Rules prohibiting sending commercial e-mail to wireless devices

The United States also has adopted rules to protect consumers from receiving unsolicited commercial messages (spam) on their wireless devices. With some exceptions, the rules prohibit the sending of commercial electronic mail messages, including e-mail and certain text messages, to wireless devices such as cell phones. The rules apply only to messages that meet the definition of "commercial" used in the CAN-SPAM Act – and to those messages where the main purpose of the message is a commercial advertisement or to promote a commercial product or service. Non-commercial messages, such as messages about candidates for public office or messages to update an existing customer about his or her account, are not subject to the rules.

Mobile service commercial messages (MSCMs) include any commercial message sent to an e-mail address that has been provided by a mobile service provider of a subscriber's wireless device. MSCMs are prohibited unless the individual addressee has given the sender express prior authorization (known as an "opt-in" requirement). The rule prohibits sending any commercial messages to addresses that contain domain names that have been listed on the FCC's list for at least 30 days or at any time prior to 30 days if the sender otherwise knows that the message is addressed to a wireless device. To assist senders of commercial messages to know which addresses belong to wireless subscribers, the rules require that wireless service providers supply the Federal Communications Commission (FCC) with the names of the relevant mail domain names. Short messaging service (SMS) messages transmitted solely to phone numbers are not covered by these protections. Auto-dialled calls are already covered by other laws.

Under the FCC's rules, the FCC can impose monetary forfeitures against spammers ranging from up to USD 11'000 per violation for non-licensees and to up to USD 130'000 per violation for common carrier licensees. In addition to monetary penalties, the FCC can issue a cease and desist order against a spammer that has violated any provision of the Communications Act or any FCC rule authorized by the Act. In addition, under the Communications Act, anyone who violates a provision of the Act is subject to criminal prosecution by the Department of Justice (in addition to a monetary penalty), and may face imprisonment for up to 1 year (up to 2 years for repeat offenders). To date, the FCC has not initiated any enforcement proceedings related to such commercial messages.

9.1.3 Approaches to limit phishing

As was discussed above, a basic premise that spammers and phishers count on is the lack of knowledge regarding who the sender is. The Internet Engineering Task Force (IETF) has released two standards, Domain Keys Identified Mail (DKIM) [b-IETF RFC 4871] and Author Domain Sending Practices (ADSP) [b-IETF RFC 5617] that improve a recipient's ability to identify senders. Vendors have begun to make implementations available to customers. There is also at least one free[17] implementation of the standard available. A source for assistance is the Anti-Phishing Working Group (APWG), an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing incidents http://www.antiphishing.org.

[17] "Free" here refers to the ability to implement this feature royalty-free under conditions specified by the patent holder.

This standard enables "white list validation", or the ability to verify that, for example, it really is your bank or your friends or associates that are trying to reach you. This standard in and of itself will limit some forms of phishing, but not all.

9.2 Japan

9.2.1 Law enforcement

There are two laws to restrict the e-mail sending in order to suppress e-mail spam in Japan. The main elements of these laws are as follows.

- The following rules apply to sending advertisement messages using e-mail. (Opt-in)
  - Sending advertisement messages using e-mail, without recipients' consent to receive them, is prohibited.
  - The sender organization is required to keep evidence of consent from the recipients while sending the advertisement messages to the recipients.
  - The advertisement messages need to provide information about the procedure to stop sending the advertise message, sender's name, etc.
  - If the recipient uses the correct procedure to notify the organization that it does not want to receive advertisement messages, the organization cannot send any more advertisement messages to the recipient.
- Sending e-mail messages with faked sender information, such as e-mail address, IP address and domain name, is prohibited.
- Sending e-mail messages to fictitious recipient addresses automatically generated by a computer program is prohibited.

9.2.2 Council for Promotion of Anti-Spam Measures

A wide-range of concerned parties such as ISPs, advertisers, ASPs for delivering ad-mails, security vendors, consumer organizations, administrations, etc, organized Council for Promotion of Anti-Spam Measures in 2008. The council adopted a "Declaration toward Eradication of Spam" in November 2008.

9.2.3 Cyber Clean Center (CCC)

The Cyber Clean Center (CCC), which finds PCs infected by bot, was established after the close collaboration among Japanese government, ISP related organizations and major ISPs. This center works as follows.

- The CCC manages a large scale honey pot system, which receives infection activities from malware (usually bot) infected PCs. The honey pot system collects IP addresses of infecting PCs and program codes of malware (bot).
- Lists of IP addresses and the date/time they were detected are sent to each ISP. Each ISP identifies its subscribers with these IP addresses and informs them that their PCs may be infected by malicious software. Each ISP also sends them the information about CCC (link to the web page) and disinfection software.
- The CCC analyzes the collected program codes. If the program code is a previously unidentified one, new disinfection software which can disinfect this new malicious program code is made and released.

This activity contributes to repression of bot infection activities in Japan. Because most spam mail messages are sent from the bot infected PCs, this also contributes to decrease spam mail sending from Japan.

9.2.4 Outbound Port 25 Blocking (OP25B)

When ISP subscribers send and receive e-mail messages, they use an e-mail service that is provided by the ISP in general. So the subscribers send their e-mail messages to the ISP's mail servers, and the ISP's mail servers relay the messages to destination e-mail servers. ISP subscribers do not normally send their e-mail messages directly to the destination e-mail servers. Because bot or virus infected PCs send spam mail directly to the e-mail servers of destination address, such e-mail messages do not pass through the ISP's mail servers. If the communications from subscribers' PCs that bypass ISP network using SMTP (TCP with destination port number 25) can be stopped, many spam messages can be blocked. Therefore the Japanese government, ISPs and the related organizations investigated the following issues in close cooperation with each other.

- Impact to subscribers when the TCP of outbound port 25 blocking (OP25B) [b-MAAWG MP25] is introduced.
- Restrictions on blocking specific communications under current Japanese laws.

After these investigations, many ISPs apply the OP25B under the following activities. JEAG (Japan Email Anti-abuse Group) plays an important role in this process by publishing a recommendation to ISPs to urge introducing OP25B.

- Although the introduction of OP25B is not mandatory for Japanese ISPs, 52 ISPs, including almost major ISPs, have introduced the OP25B by July 2009.
- Many ISPs introducing the OP25B provide TCP port 587 with SMTP AUTH, as an alternative way to communicate, not to decrease the service quality. Users can submit mail messages from other ISP adapting OP25B to such ISP's mail server.

9.2.5 Sender authentication technologies

Sender authentication technologies are techniques to detect source address spoofing of e-mail. JEAG published a recommendation to introduce these techniques, and the Ministry of Internal Affairs and Communications published a document "Important legal matters concerning the introduction of sender authentication at the receiving side by an ISP". Currently almost all major mobile communication operators and some of ISPs have introduced the Sender Policy Framework (SPF) [b-IETF RFC 4408], one of the sender authentication technologies, and their subscribers can use the result of authentication for filtering. The rate of published SPF record for "jp" domains is 35.99% in August 2009. Moreover several ISPs have started to introduce DKIM [b-IETF RFC 4871] as additional sender authentication.

9.2.6 Spam mail sender information exchange among mobile communication operators

Almost all cellular phones in Japan have the capability to handle general e-mail messages. Because many spam mail messages are sent from mobile cellular phones in Japan, all mobile communication operators exchange information about spam mail senders with the following steps.

- The ID of any individuals who wish to make a contract for mobile phones is checked under the "Mobile Phone's Improper Use Prevention Act".
- If a mobile communication operator finds a cellular phone user who sends spam mail messages which violates "Act on Regulation of Transmission of Specified Electronic Mail", the user information is provided to all other mobile communication operators.

So if a user sends spam mail messages from a cellular phone, the user will have difficulty entering into a contract for mobile phones usage in Japan.

A related nonprofit organization sets sensors, collects spam messages and analyzes them. It provides information about spam mail senders to originating ISPs in Japan and exchanges this information with some agencies in foreign countries.

Bibliography

[b-IETF RFC 4871] IETF RFC 4871 (2007), *Domainkeys Identified Mail (DKIM) Signatures*. http://www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617 (2009), *DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)*. http://www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] MAAWG Recommendation (2005), *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction*. http://www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408 (2007), *Sender Policy Framework (SPF) fo Authorizing Use of Domains in E-*Mail*, Version 1*. http://www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (United States Code). This Act is documented in the following laws: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. http://www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] Messaging Anti-Abuse Working Group Conference reports: http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html.

Annex B

Identity Management

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 7

(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Supplement on overview of identity management in the context of cybersecurity

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Supplement 7 to X-series Recommendations – ITU-T X.1250-series

Supplement on overview of identity management in the context of cybersecurity

Summary

The security of the traditional public circuit-switched telephone network (PSTN) has been addressed over many decades of operation. However, the same cannot be said for distributed public packet-switched networks with multiple-service providers, such as the Internet and Next Generation Networks (NGNs). Such networks use one common transport platform for control traffic and for user traffic which, in addition to the possible anonymity of such traffic and the possibility of generating unidirectional traffic, makes such networks vulnerable to misuse. All electronic services (e-services such as e-business, e-commerce, e-health, e-government) are open to attack. This problem can be at least partly addressed by improving confidence in the identity of users, network devices and service providers, so that they can be authenticated, granted appropriate access, and audited. Because identity management provides greater assurance and trust in user, service provider, and network device identities, it improves security by reducing exposure to security risks. This aspect of cybersecurity is something that service providers need to consider at a business and technical level, and that governments need to consider on a national level as part of the national cybersecurity plan.

Introduction

Identity management (IdM) is a way to manage and control the information that is used in the communications process to represent entities (such as service providers, end-user organizations, people, network devices, software applications and services). A single entity may have multiple digital identities in order to access various services with differing requirements, and these may exist in multiple locations.

IdM is a key component of cybersecurity because it provides the capability to establish and maintain trusted communications among entities. IdM supports authentication of an entity. It also enables the authorization of a range of privileges (rather than all-or-nothing privileges) and makes it easier to change privileges if an entity's role changes. IdM also improves an organization's ability to apply its security policies by enabling an entity's activity on the network to be monitored and audited. IdM can provide access to entities both inside and outside an organization. In short, a good IdM solution provides capabilities to support authentication, provisionand manage identities, and audit an entity's activities.

IdM is a critical component in managing security and enabling nomadic, on-demand access to networks and e-services. Along with other defensive mechanisms (e.g. firewalls, intrusion detection systems, virus protection), IdM plays an important role in protecting information, communications and services from cybercrimes such as fraud and identity theft. One consequence of this is that users' confidence will grow that e-transactions will be secure and reliable. In turn, this will increase users' willingness to use IP networks for e-services.

In implementing an IdM system, fundamental privacy concerns must be addressed. This means developing methods to ensure that identity information is accurate and to prevent identity information from being used for purposes beyond those for which it was collected.

1 Scope

Identity management has emerged as a critical component that will improve security by providing greater assurance by verifying the validity of identity information. This Supplement provides a general overview of this new service.

The use of the term "identity" in this supplement relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

2 References

None

3 Definitions

Definitions can be found in other Recommendations of the X.1250 series

4 Abbreviations and acronyms

IdM – Identity Management

IP – Internet Protocol

PSTN – Public Switched Telephone Network

5 Conventions

None

6 Importance of IdM to global network infrastructure protection and multi-national coordination for security

Proper implementation and use of IdM capabilities and practices in various national, regional, and international networks will enhance the security of the global network infrastructure. IdM best practices and implementations are important and necessary to provide assurance of identity information and of the integrity and availability of the global network infrastructure.

IdM capabilities can be used to support national and international emergency telecommunications services by identifying users authorized for special services.

In addition, IdM capabilities can be used to prevent, detect, and support coordination of responses to, national and international cybersecurity incidents. In some instances, IdM may help authorities and entities coordinate their efforts to trace and locate the source of such incidents.

7 Identity management as an enabler of trusted communication between two entities

One important function of IdM is the authentication of users, networks or services. In an authentication process involving two entities, one entity makes assertions about its identity to the other. Depending on the second entity's security requirements, these assertions may need to be validated before the second entity will trust the first enough to grant it privileges. This process may be required in both directions.

There are various levels of authentication trust ranging from little-or-none, weak (e.g., user name and password), to strong (e.g., public key infrastructure (ITU-T X.509)). A risk assessment can identify the appropriate level of authentication. There may need to be higher levels of authentication for one entity than for the other, for example, because one entity controls critical resources.

8 Protection, maintenance, revocation and control of identity data

Other important functions of IdM are to protect, maintain, and control trusted identity data, including the ability to ascertain the current status of an identity.

Laws or policies may require that personally identifiable information is protected and that identity information is prevented from being used for purposes beyond those for which it was collected. Ensuring that identity data continues to be valid is another primary concern. For the services that use them to be viable, identity data must be properly maintained so that it is accurate, timely and consistent.

Where relevant, management of identity data attributes should include the capability to check the identity data to see if it has been revoked.

In many cases, entities will want to control the use of their own data and private information.

9 "Discovery" of trusted sources of identity data

IdM also encompasses the concept of "discovery" of trusted identity data. In a highly distributed, multi-provider environment (such as the Internet and Next Generation Networks), identity data necessary to provide trust in the identity and related assertions of an entity can be located in different places on the network. Entities may have multiple digital identities with different sources of identity information in different locations. When one of the two entities in an authentication process is nomadic, the other entity will need to locate and establish a trust relationship with an appropriate source of identity information in order to complete the process of authenticating the nomadic entity. The concept of discovery of sources of trusted information is similar to what occurs today in mobile cell phone usage.

10 Electronic government services (e-government services)

The advantages to an entity of implementing IdM include risk reduction, trust enhancement, increased functionality and the potential for cost reduction. These reasons for implementing IdM are equally valid when the entity is a government. In e-government services, the main objectives are also to cut costs and to provide more efficient and more effective services to the government's citizens and business partners.

Like other entities, governments are confronted by the challenge of how to effectively and efficiently utilize identity in the networked world. In order to make e-government services a reality, a government must perform risk analyses on the e-services it intends to offer and implement suitable protective measures. The sensitive nature of many e-government services (for example, e-health) may require a government to require strong authentication.

11 Regulatory considerations in connection with IdM

National administrations and regional groups need to consider a number of potential regulatory issues in connection with IdM implementation, such as privacy and data protection, national security and emergency preparedness, and mandatory settlements between carriers. Governments not only utilize identity management techniques but may also impose it on other entities to meet a broad array of national policy and security objectives.

Bibliography

Various forums are working on IdM issues. These include:

ARK (California Digital Library Archival Resource Key): http://www.cdlib.org/inside/diglib/ark/

3GPP SA3: http://www.3gpp.org/SA3-Security?page=type_urls

ETSI TISPAN WG7: http://www.etsi.org/tispan/

EU eID Roadmap:
http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

European Citizen Card: http://europa.eu.int/idabc/servlets/Doc?id=19132

FIDIS (EU Future of Identity in the Information Society): http://www.fidis.net/

FIRST (Forum of Incident Response and Security Teams): http://www.first.org/

Guide project (EU Government User Identity for Europe):
http://www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Handle: http://www.handle.net/

Higgins: http://www.eclipse.org/higgins/index.php

IDSP (American National Standards Institute Identity Theft Prevention and Identity Management Standards Panel (IDSP)):
http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

IGF (ORACLE Identity Governance Framework):
http://www.oracle.com/technology/tech/standards/idm/igf/index.html

ITRC (Identity Theft Resource Center): http://www.idtheftcenter.org/

Internet Engineering Task Force: http://sec.ietf.org/

ITU-T Study Group 17 (Security) Focus Group on IdM:
www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

ITU-T Study Group 17 (Security) Question 10:
http://www.itu.int/ITU-T/studygroups/com17/index.asp

ITU-T Study Group 13 (Future Networks) Question 13:
http://www.itu.int/ITU-T/studygroups/com13/index.asp

Liberty Alliance Project: http://www.projectliberty.org/

Light Weight Identity: http://lid.netmesh.org/wiki/Main_Page

MODINIS-IDM Consortium: http://www.egov-goodpractice.org and
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

National Identity Card Schemes: e.g. http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/
http://en.wikipedia.org/wiki/Identity_document

OASIS (Organization for the Advancement of Structured Information Standards):
http://www.oasis-open.org/home/index.php

OECD (Organisation for Economic Co-operation and Development) Workshop on Digital Identity Management in Trondheim, Norway, May 8th-9th 2007: http://www.oecd.org/sti/security-privacy/idm

OMA (Open Mobile Alliance): http://www.openmobilealliance.org/

The Open Group: http://www.opengroup.org

OSIS (Open Source Identity System): http://osis.idcommons.net/wiki/Main_Page

PAMPAS (EU Pioneering Advanced Mobile Privacy and Security (PAMPAS): http://www.pampas.eu.org/

PERMIS (EU Information Society Initiative in Standardization (ISIS) PrivilEge and Role

Prime (EU Privacy and Identity Management for Europe): https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

W3C (World Wide Web Consortium): http://www.w3.org/

Yadis: http://yadis.org/wiki/Main_Page

Annex C

Links and references

This reference list of materials will be updated regularly, taking into consideration the outputs of the ITU Global Cybersecurity Agenda and the outputs of the project implementing Resolution 45 (WTDC-06), the work carried out by ITU-T Study Group 17 (the leading Study Group on security in ITU-T) relevant WTSA Resolutions, as well as the follow-up on WSIS action line C5 on cybersecurity and the results of the work on relevant PP-06 Resolutions (such as Resolution 130, 131 and 149).

Part I: Developing and Obtaining Agreement on a National Cybersecurity Strategy

I.C.1 Awareness Raising (I.B.1, I.B.2)

International

- UNGA Resolution 55/63 on "Combating the criminal misuse of information technologies": http://www.un.org/Depts/dhl/resguide/r55.htm
- UNGA Resolution 56/121 on "Combating the criminal misuse of information technologies": http://www.un.org/Depts/dhl/resguide/r56.htm
- UNGA Resolution 57/239 on "Creation of a global culture of cybersecurity": http://www.un.org/Depts/dhl/resguide/r57.htm
- UNGA Resolution 58/199 on "Creation of a global culture of cybersecurity and the protection of critical information infrastructures": http://www.un.org/Depts/dhl/resguide/r58.htm
- United Nations World Summit on the Information Society (WSIS) Geneva Declaration of Principles and Plan of Action and Tunis Commitment and Plan of Action for the Information Society: http://www.itu.int/WSIS/index.html
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2005): http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- International CIIP Handbook 2006 (Vol. 1): http://www.isn.ethz.ch/pubs/ph/details.cfm?id=250
- ITU cybersecurity-related resources: http://www.itu.int/cybersecurity/
- ITU Global Cybersecurity Agenda: http://www.itu.int/cybersecurity/gca/
- ITU Cybersecurity Gateway: http://www.itu.int/cybersecurity/gateway/
- ITU Development Bureau's cybersecurity webpage: http://www.itu.int/ITU-D/cyb/
- ITU Child Online Protection initiative and related guidelines: http://www.itu.int/cop/

I.C.2 National, Regional and International Strategies (I.B.2, I.B.3, I.B. 4, I.B.5, I.B.7)

International

- ITU National Cybersecurity/CIIP Self-Assessment Toolkit: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- ITU and ETH Zurich – A Generic National Framework for Critical Information Infrastructure Protection (CIIP): http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
- ITU Telecommunication Development Sector, Study Group Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity: http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf

- ITU Global Cybersecurity Agenda: http://www.itu.int/cybersecurity/gca/
- ITU Cybersecurity Guide for Developing Countries, Rev. 2009 : http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- ITU WTDC Resolution 45: Mechanisms for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006): http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
- ITU Telecommunication Standardization Sector, Study Group 17 Question 4 Compendium – Catalogue of Approved ITU-T Recommendations Related To Telecommunication Security: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090003MSWE.doc
- ITU Telecommunication Standardization Sector, Study Group 17 Question 4 – Security in Telecommunications and Information Technology: http://www.itu.int/pub/T-HDB-SEC.03-2006/en/
- ITU BDT Study on the Financial Aspects of Network Security: Malware and Spam: http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: http://www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html
- OECD Implementation Plan for co-ordinated national online security policies: http://www.oecd.org/dataoecd/23/11/31670189.pdf
- World Bank report on "Cyber security: a new model for protecting the network": http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf
- Information Technology Association of America (ITAA) White Paper on Information Security: http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf

Regional

- APEC Telecom and Information Working Group – APEC Cybersecurity Strategy (2002): http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf
- CITEL Blue Book: Telecommunication Policies for the Americas (2005) sections 8.4-8.5: http://www.citel.oas.org/publications/azul-fin-r1c1_i.pdf
- Council of the European Union Resolution: Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment (2007): http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf
- Doha Declaration on Cybersecurity (2008): http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf
- European Union Communication on "A Strategy for a Secure Information Society" (2006): http://ec.europa.eu/information_society/doc/com2006251.pdf
- European Union Safer Internet Programme: http://europa.eu.int/information_society/activities/sip/index_en.htm
- European Network and Information Security Agency (ENISA) Commissioned Study on "Security Economics and the Internal Market" (2008): http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm
- OAS Inter-American Strategy to Combat Threats to Cybersecurity (2004): http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

National

- Australia's Critical Infrastructure Protection Modelling and Analysis Program (CIPMA): http://www.csiro.au/partnerships/CIPMA.html
- Crisis and Risk Network (CRN) International CIIP Handbook: An Inventory and Analysis of National Protection Policies: http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
- Germany National Plan for Information Infrastructure Protection: http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National_Plan_for_Information_Infrastructure)_Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf
- Japan's National Strategy on Information Security (tentative translation): http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
- National Implementation Strategies of 11 OECD Members: http://www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- New Zealand's Digital Strategy: http://www.digitalstrategy.govt.nz
- Singapore's Infocomm Security Masterplan 2: http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf
- Singapore's Strategy in Securing Cyberspace: http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21
- United Kingdom's Centre for the Protection of National Infrastructure (CPNI): http://www.cpni.gov.uk/
- United States National Strategy to Secure Cyberspace: http://www.whitehouse.gov/

I.C.3 Assessment and Program Development (I.B.5, I.B.7, I.B.8)

- Control Objectives for Information and Related Technology (COBIT) 4.1: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (executive summary free; registration required to download full version)
- Information Technology Infrastructure Library (ITIL) Security Management: http://www.itil-itsm-world.com/ (fee required)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series, Information technology – Security techniques – Information security management systems: http://www.iso27001security.com/index.html
- ISO/IEC 13335, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066 (fee required)
- ISO/IEC 17799, 2005 Information technology – Security techniques – Code of practice for information security management: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612 (fee required)
- ISO/IEC 21827, Systems Security Engineering – Capability Maturity Model (SSE-CMM®): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731 (fee required)

- ITU-BDT Study on Financial Aspects of Network Security: Malware and Spam: http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- ITU WTSA Resolution 50 on Cybersecurity (Rev. Johannesburg, 2008): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf
- ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf
- ITU WTSA Resolution 58: Encourage the creation of national computer incident response teams, particularly for developing countries (Johannesburg, 2008): http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
- NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook (Feb 1996): http://csrc.nist.gov/publications/nistpubs/800-12/
- NIST SP 800-30, Risk Management Guide for Information Technology Systems (Jul 2002): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems (Dec 2007): http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (Dec 2007): http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program (October 2003): http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, (July 2002): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM): http://www.cert.org/octave/

I.C.4 International Assistance Points of Contact (I.B.6)

- Anti-Phishing Working Group (APWG): http://www.antiphishing.org
- Forum of Incident Response Security Teams (FIRST): http://www.first.org
- Institute of Electrical and Electronics Engineers: http://www.ieee.org
- Internet Engineering Task Force: http://www.ietf.org
- Messaging Anti-Abuse Working Group: http://www.maawg.org
- World Information Technology Services Alliance: http://www.witsa.org
- World Wide Web Consortium: http://www.w3c.org

Part II: Establishing National Government-Industry Collaboration

II.C.1 Structures for Government-Industry Collaboration

International

- Cyber Security Industry Alliance: http://www.csialliance.org/about_csia/index.html
- OECD Anti-Spam Toolkit – Co-operative Partnerships Against Spam: http://www.oecd-antispam.org/article.php3?id_article=243
- StopSpamAlliance.org: http://stopspamalliance.org/

Regional

- Middle East: Report on 14th GCC eGovernment and eServices Forum: http://www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/

National

- Australia Business-Government Partnership: The Trusted Information Sharing Network for Critical Infrastructure Protection: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA)
- United States Information Sharing and Analysis Centers (ISACs) & Coordinating Councils:
  - Financial Services ISAC: http://www.fsisac.com/
  - Electric Sector ISAC: http://www.esisac.com/
  - Information Technology ISAC: http://www.it-isac.org
  - Telecommunications ISAC: http://www.ncs.gov/ncc/
  - Network Reliability and Interoperability Council (NRIC): http://www.nric.org/
  - National Security and Telecommunications Advisory Committee (NSTAC): http://www.ncs.gov/nstac/nstac.html
- United States Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel: http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
- United States Information Technology Association of America White Paper on Information Security: http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- United States IT Sector Coordinating Council (SCC): http://www.it-scc.org
- United States National Cyber Security Partnership: http://www.cyberpartnership.org/
- United States National Information Assurance Council (NIAC) report on sector partnership model working group: http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- United States National Infrastructure Protection Plan: http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- United States Sector Specific Plans: http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- United States IT Sector Specific Plan: http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- United States National Telecommunications and Information Administration: http://www.ntia.doc.gov/

II.C.2 Cybersecurity Information Sharing

International

- Messaging Anti-Abuse Working Group: http://www.maawg.org

National

- United States NIST, Computer Security and Research Center: http://csrc.nist.gov/
- United States US-CERT National Cyber Alert System: http://www.us-cert.gov/cas/

II.C.3 Awareness Raising and Outreach: Tools for Governments and Business

International

- Building a Security Awareness Program: http://www.gideonrasmussen.com/article-01.html

- Center for Internet Security Resources and Publications on Enterprise Security: http://www.cisecurity.org/resources.html
- Corporate Strategies for Security Awareness: http://articles.techrepublic.com.com/5100-10878_11-5193710.html
- Common Sense Guide to Cybersecurity for Small Businesses: http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
- EDUCAUSE Security Awareness Resources for Governments and Industry: http://www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/BrowseSecurityAwarenessResourc/8770?time=1215527945
- ENISA Information Security Awareness Initiatives (available in multiple languages): http://www.enisa.europa.eu/Pages/05_01.htm
- Interpol IT Security and Crime Prevention Methods (to prevent crime in companies): http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
- Interpol IT Crime Company Checklist: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp
- NoticeBored Security Awareness Posters: http://www.noticebored.com/html/posters.html
- OECD Anti-Spam Toolkit – Education and Awareness: http://www.oecd-antispam.org/article.php3?id_article=242
- SANS Security Policy Resources: http://www.sans.org/resources/policies/
- Security Awareness Toolbox – The Information Warfare Site: http://www.iwar.org.uk/comsec/resources/sa-tools/
- United States National Cyber Security Partnership – Awareness for Small Business and Small Business Resource Center: http://www.cyberpartnership.org/init-aware.html

National

- United States Federal Trade Commission: http://www.ftc.gov/infosecurity
- NIST 800-50 Security Awareness and Training Program: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Part III: Deterring Cybercrime/Legal Foundation and Enforcement

International

- Council of Europe: Convention on Cybercrime (2001): http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- G-8 High-Tech Crime Principles: http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- ITU background material related to harmonization of national legal approaches, international legal coordination and enforcement: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- ITU/InfoDev ICT Regulation Toolkit: http://www.ictregulationtoolkit.org/
- ITU Publication on Understanding Cybercrime: A Guide for Developing Countries: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
- ITU Toolkit for Cybercrime Legislation: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
- Interpol Information Technology Crime Resources: http://www.interpol.com/Public/TechnologyCrime/

- OECD Anti-Spam Regulatory Approaches: http://www.oecd-antispam.org/article.php3?id_article=1
- OECD Anti-Spam Toolkit: http://www.oecd-antispam.org/article.php3?id_article=265
- UNGA Resolution 55/63 on "Combating the criminal misuse of information technologies": http://www.un.org/Depts/dhl/resguide/r55.htm
- UNGA Resolution 56/121 on "Combating the criminal misuse of information technologies": http://www.un.org/Depts/dhl/resguide/r56.htm
- United Nations Interregional Crime and Justice Research Institute (UNICRI) resources to improve knowledge and create new partnerships to counter cybercrime: http://www.unicri.it/
- UNCITRAL Model Laws on Electronic Commerce and on Electronic Signatures: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- United Nations Office on Drugs and Crime resources: http://www.unodc.org/

Regional

- APEC: Cybercrime-related documents, presentations and ministerial statements: http://www.apectelwg.org/
- Cairo Declaration of the Conference on Cybercrime: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
- Commonwealth Model Law on Computer and Computer Related Crime: http://www.thecommonwealth.org/Internal/38061/documents/
- Council of Europe: Convention on Cybercrime (2001): http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- OAS: Inter-American Cooperation Portal on Cyber Crime: http://www.oas.org/juridico/english/cyber.htm
- CERT/CC: How the FBI Investigates Computer Crime: http://www.cert.org/tech_tips/FBI_investigates_crime.html
- Cybercrimelaw: Survey of Cybercrime Legislation Worldwide: http://www.cybercrimelaw.net/index.html
- Council of Europe: Survey of Countries' Cybercrime Legislation: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Legprofiles.asp#TopOfPage
- Microsoft: "Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws": http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf
- OECD Member States' Anti-Spam Laws: http://www.oecd-antispam.org/countrylaws.php3
- United Nations "Models for Cyber Legislation in Economic and Social Commission for Western Asia (ESCWA) Member Countries": http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf
- United States Department of Justice (USDOJ) Computer Crime and Intellectual Property Section website: http://www.cybercrime.gov
- United States Department of Justice (USDOJ) Manual on Prosecuting Computer Crime (Chapter 1 – Computer Fraud and Abuse Act): http://www.cybercrime.gov/ccmanual/
- United States Secret Service – Best Practices for Seizing Electronic Evidence: http://www.forwardedge2.com/pdf/bestPractices.pdf

Part IV: Creating National Incident Management Capabilities: Watch, Warning, Response and Recovery

IV.C.1 National Response Plan and National CSIRT

International

- CERT Coordination Center (CERT/CC) at Carnegie Mellon University: http://www.cert.org/csirts/
- CERT/CC: Action List for Developing a CSIRT: http://www.cert.org/csirts/action_list.html
- CERT/CC: Creating a CSIRT: A Process for Getting Started: http://www.cert.org/csirts/Creating-A-CSIRT.html
- CERT/CC: Defining Incident Management Processes for CSIRTs: A Work in Progress: http://www.cert.org/archive/pdf/04tr015.pdf
- CERT/CC: CSIRT Frequently Asked Questions: http://www.cert.org/csirts/csirt_faq.html
- CERT/CC: Handbook for CSIRTs: http://www.cert.org/archive/pdf/csirt-handbook.pdf
- CERT/CC: Incident Management Capability Metrics Version 0.1: http://www.cert.org/archive/pdf/07tr008.pdf
- CERT/CC: Organizational Models for CSIRT: http://www.cert.org/archive/pdf/03hb001.pdf
- CERT/CC: CSIRT Services: http://www.cert.org/csirts/services.html
- CERT/CC: Staffing Your CSIRT – What Basic Skills Are Needed?: http://www.cert.org/csirts/csirt-staffing.html
- CERT/CC: State of the Practice of CSIRT: http://www.cert.org/archive/pdf/03tr001.pdf
- CERT/CC: Steps for Creating National CSIRTs: http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
- CERT/CC Virtual Training Environment (VTE): http://www.vte.cert.org/
- ENISA: A Step-by-Step Approach on How to Set Up a CSIRT: http://www.enisa.europa.eu/pages/05_01.htm
- ITU-IMPACT Collaboration and related resources: http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- GOVCERT.nl: CSIRT in a Box – Information on Setting up a CSIRT: http://www.govcert.nl/render.html?it=69
- United Kingdom's CPNI: The Warning, Advice and Reporting Point (WARP) Toolbox: http://www.warp.gov.uk/

Regional

- Asia Pacific CERT: http://www.apcert.org/index.html
- European CSIRT Network Resources: http://www.ecsirt.net/
- European Government CERTs (EGC) Group: http://www.egc-group.org/

National

- Australia: AusCERT: http://www.auscert.org.au
- Austria: CERT.at: http://www.cert.at
- Brazil: CERT.br: http://www.cert.br/
- Chile: CLCERT: http://www.clcert.cl/
- China: CNCERT/CC: http://www.cert.org.cn/

- Finland: CERT-FI: http://www.cert.fi
- Hungary: CERT-Hungary: http://www.cert-hungary.hu
- India: CERT-In: http://www.cert-in.org.in
- Italy: CERT-IT: http://security.dico.unimi.it/
- Japan: JPCERT/CC: http://www.jpcert.or.jp/
- Korea: KrCERT/CC: http://www.krcert.or.kr/
- Malaysia: MyCERT: http://www.cybersecurity.org.my
- Netherlands: http://www.csirt.dk/
- Poland: CERT POLSKA: http://www.cert.pl/
- Slovenia: SI-CERT: http://www.arnes.si/en/si-cert/
- Singapore: SingCERT: http://www.singcert.org.sg/
- Sweden: SITIC: http://www.sitic.se
- Switzerland: MELANI: http://www.melani.admin.ch
- Thailand: ThaiCERT: http://www.thaicert.nectec.or.th/
- Tunisia: CERT-TCC: http://www.ansi.tn/en/about_cert-tcc.htm
- Qatar: http://www.qcert.org
- United Arab Emirates: http://aecert.ae/
- United States National Response Plan: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- United States US-CERT: http://www.us-cert.gov/
- And other national CERT/CSIRT websites

IV.C.2 Cooperation and Information Sharing

International

- CERT/CC: Security vulnerabilities and fixes: http://www.cert.org/nav/index_red.html
- Clearing House for Incident Handling Tools (CHIHT): http://chiht.dfn-cert.de/
- Forum of Incident Response and Security Teams (FIRST) resources: http://www.first.org/
- ISP Security Support Service resources: http://www.donelan.com/ispsupport.html
- ITU Cybersecurity Gateway: Background Material related to Watch, Warning and Incident Response: http://www.itu.int/cybersecurity/gateway/watch_warning.html
- ITsafe warning system for small businesses and individuals: http://www.itsafe.gov.uk/
- OECD: Anti-Spam Toolkit: http://www.oecd-antispam.org/article.php3?id_article=265

Regional

- Trans-European Research and Education Networking Association (TERENA): http://www.terena.org/

National

- The Netherlands: Dutch National Alerting Service: http://www.waarschuwingsdienst.nl/render.html?cid=106
- United Kingdom's CPNI: The Warning, Advice and Reporting Point (WARP) Toolbox: http://www.warp.gov.uk/

- United States IT-ISAC: https://www.it-isac.org/
- United States IT Sector Coordinating Council (ISCC): Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan: http://www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf
- United States National Institute of Standards and Technology (NIST): http://csrc.nist.gov/

IV.C.3 Vulnerability Information/Tools and Techniques

- Build Security In – Collection of software assurance and security information to help create secure systems: https://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Common Vulnerabilities and Exposures List (CVE): http://www.cve.mitre.org/about/
- Open Vulnerability Assessment Language (OVAL): http://oval.mitre.org/
- United States National Vulnerability Database (NVD) for software: http://nvd.nist.gov/nvd.cfm

Part V: Promoting a National Culture of Cybersecurity

V.C.1 Government Systems and Networks (V.B.1, V.B.2, V.B.7)

International

- WSIS Action Line C5, Plan of Action: http://www.itu.int/wsis/implementation/index.html
- ITU Global Cybersecurity Agenda: http://www.itu.int/osg/csd/cybersecurity/gca/
- ITU WSIS Thematic Meeting on Countering Spam: http://www.itu.int/osg/spu/spam/meeting7-9-04/index.html
- WSIS Action Line C5, First Meeting Chairman's Report: http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- WSIS Action Line C5, Second Meeting Plan of Action: http://www.itu.int/wsis/docs/geneva/official/poa.html
- Second Meeting Agenda with links to presentations: http://www.itu.int/osg/csd/cybersecurity/WSIS/meetingAgenda.html
- WSIS Action Line C5, Third Meeting Report: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf
- Third Meeting Agenda with links to presentations: http://www.itu.int/osg/csd/cybersecurity/WSIS/agenda-3_new.html
- Microsoft: Computing Privacy, Internet Safety and Security Information for Policymakers Worldwide: http://www.microsoft.com/mscorp/twc/policymakers_us.mspx
- OECD Culture of Security portal with resources: http://www.oecd.org/sti/cultureofsecurity
- OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (2002): http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OECD: "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980): http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- OECD Report on "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries" (2005): http://www.oecd.org/dataoecd/16/27/35884541.pdf
- World Bank Information Technology Security Handbook – Information Security and Government Policies: http://www.infodev-security.net/handbook/part4.pdf
- UNGA Resolution 57/239 (Annexes a and b.): http://www.un.org/Depts/dhl/resguide/r57.htm

Regional

- ENISA: "Information Security Awareness Initiatives: Current practice and the measurement of success" (2007): http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf
- ENISA: "A Users' Guide: How to Raise Information Security Awareness" (2006): http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_ISawareness.pdf
- Europe's Internet Safety Information Source (InSafe): http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- OAS: Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (particularly Appendices) (2004): http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

National

- Brazil: Antispam.br resources: http://antispam.br/
- Brazil: Internet Safety Guidelines of the Brazilian Internet Steering Committee - CGI.br: http://cartilha.cert.br/
- OECD Initiatives to Promote a Culture of Security (by Country): http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html
- United States CERT site: http://www.us-cert.gov/
- United States DHS National Critical Infrastructure Protection R&D Plan: http://www.dhs.gov/xres/programs/gc_1159207732327.shtm
- United States Federal Agency Security Practices: http://csrc.nist.gov/fasp/
- United States Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39: http://www.acqnet.gov/FAR/
- United States Federal Plan for Cyber Security and Information Assurance R&D: http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- United States Information Security and Privacy Advisory Board: http://csrc.nist.gov/ispab/
- United States Homeland Security Presidential Directive/HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection": http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- United States Multi-State Information Sharing and Analysis Center: http://www.msisac.org/
- United States National Strategy to Secure Cyberspace: http://www.whitehouse.gov/pcipb/
- United States President's Information Technology Advisory Committee Report on Cybersecurity Research Priorities: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.2 Business and Private Sector Organizations (V.B.3., V.B.5., V.B.7.)

- Brazil Safe Internet Movement: http://www.internetsegura.org/
- Cisco Security Center (Best Practices section): http://tools.cisco.com/security/center/home.x
- Microsoft Trustworthy Computing: http://www.microsoft.com/mscorp/twc/default.mspx
- NIATEC Teaching Materials: http://niatec.info/index.aspx?page=105
- World Bank Information Technology Security Handbook – Security for Organizations: http://www.infodev-security.net/handbook/part3.pdf

- United States CERT Posters and Information Sheets for the Workplace: http://www.uscert.gov/reading_room/distributable.html
- United States DHS/Industry "Cyber Storm" exercises: http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm

V.C.3 Individuals and Civil Society (V.B.4., V.B.6, V.B.7.)

- Brazil: SaferNet Brazil: http://www.safernet.org.br/site/
- Be Safe Online (SUSI – Safer Use of Services on the Internet): http://www.besafeonline.org/
- CASEScontact security tips: http://casescontact.org/tips_list.php
- Childnet International resources for children: http://www.childnet-int.org
- Cyber Peace Initiative: http://www.cyberpeaceinitiative.org/
- CyberTipline: Teenagers learn how to stay safe online: http://tcs.cybertipline.com/
- Internet Safety Zone resources for children and parents: http://www.internetsafetyzone.co.uk/
- Interpol IT Crime Private Checklist: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp
- ITU Child Online Protection initiative and related guidelines: http://www.itu.int/cop/
- GetNetWise tools for families: http://kids.getnetwise.org/tools/
- OnGuard Online – tips to protect against fraud: http://onguardonline.gov/index.html
- MakeItSecure – information on common Internet dangers: http://www.makeitsecure.org/en/index.html
- Malaysia's eSecurity initatives: http://www.esecurity.org.my/
- NetSmartz: resources for parents and guardians: http://www.netsmartz.org/netparents.htm
- New Zealand's Netsafe: http://www.netsafe.org.nz
- SafeLine hotline for reporting illegal content: http://www.safeline.gr/
- Security Cartoon: http://www.securitycartoon.com/
- Stay Safe Online: http://www.staysafeonline.info/
- WiredSafety.org: http://www.wiredsafety.org/
- World Bank Information Technology Security Handbook – Security for Individuals: http://www.infodev-security.net/handbook/part2.pdf
- United Kingdom's Child Exploitation and Online Protection Centre resources: http://www.ceop.gov.uk/
- United Kingdom's Get Safe Online: http://www.getsafeonline.org/
- United States CERT for non-technical users: http://www.us-cert.gov/nav/nt01/

And other international, regional and national awareness-raising initiatives for end-users.

Printed in Switzerland
Geneva, 2010

Photo credits: ITU Photo Library