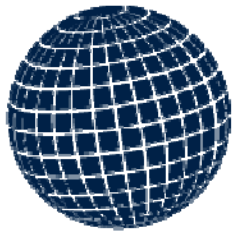


Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

ITU-D Study Group Question 3/2: Increasing the Scale and Effectiveness of Cyber Capacity Building

Taylor Roberts

Wednesday, September 24th, 2014

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Overview

- Oxford Centre perspective on Cyber Capacity Building
- Current Projects:
  - Cyber Capability Maturity Model
  - Cybersecurity Capacity Portal
- Request for Input

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Oxford Centre Capacity Dimensions

- D1: Cyber policy and strategy
- D2: Cyber culture and society
- D3: Cyber education, training and skills
- D4: Cyber legislation and regulation
- D5: Technology and Standards

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cyber Capability Maturity Model

- Designed to serve as a self-assessment tool
- Increase levels of cyber capacity across five dimensions
- Request for Input
- Five levels of maturity:
  1. Initial
  2. Repeatable
  3. Defined
  4. Managed
  5. Optimizing

Capacity Building Factors	Initial	Repeatable	Defined	Managed	Optimizing
D1-1: Creation of National Cyber Security Strategy	An initial national cyber security strategy document exists, driven forward by some department of government without broad consultation.	National strategy built on foundation of broad government consultation, allowing all departments to input with clear processes for strategy renew established.	National strategy renewal processes include specific mandate with appropriate processes to consult with wider public and private sectors and civic society. All areas of government have a common understanding of cybersecurity terminology.	Representation of the whole national strategy can be made with confidence by multiple stakeholders across government. Wider stakeholders feel they understand how their interests are represented, and are confident of the processes by which they can influence strategy.	Promotion of trust and confidence building measures (TCBM's) to ensure the continued contribution of all stakeholders including the private sector and international partners.
	No overarching national cybersecurity programme, budgets are distributed across various public offices with reliance on willingness to cooperate (perhaps with instruction to do so) as opposed to a single coordinated programme office.	Coordinated programme exists, however, budgets may still be distributed with a reliance on cooperation to achieve single programme.	Single programme ownership / designated coordinating body has been identified with budget. This programme stipulates goals, milestones, and metrics to measure progress. Clear roles and responsibilities of cybersecurity within government bureaucracy elucidated, including a designated coordinating body.	Evidence of repeated application of metrics and resulting refinements to operations and strategy, across the breadth of government involved in cyber security risk management.	Single model of nations cyber security posture exists with near-real-time feedback on the performance of risk controls, resulting in fast and active consideration of changes to priorities and redistribution and focusing of budgets.
	The strategy development may reflect societal values, traditions, and legal principles but will not be the result of wide constulation with stakeholders. Advice may have been sought from international partners.	Consultation processes will have been established for key stakeholder groups, including international partners. These processes will have been followed and learnings fed into strategy 'owners' and strategy renew processes.	National security risks and how they relate to wider stakeholder community understood, with metrics and mitigations defined and measurement processes established.	Exercises that provide an accurate picture of national cyber resilience regularly held.	Wide and continuous societal participation in cyber resilience activities and controls.
	Links will have been made to national risk priorities, but these will be ad-hoc and lack detail on how the strategy will help to address such risks.	Cyber security strategy is linked to national risks, priorities and objectives, and is contained within (and enhancing) existing National Security Strategy. Some metrics for success will have been established for some (but not all) aspects, and the methods for collecting data and applying metrics agreed. Critical national security assets in cyberspace have been identified.	Controls relating to the following aspects included in the strategy: public awareness of cyber issues, education and training of professionals, cybercrime mitigation efforts, national data collection/surviellence, national data security, the role of a national Computer Emergency Response Team, intenational standards and conventions on cybersecurity, national cyber defence exercises, investment in to cybersecurity research, and the role of National Critical Infrastructure	Strategy objectives and interventions assessed and modified (if required) in response to exercise results and learnings from cyber related events. All signfiicant events considered for cyber and physical components, with assessment of the performance of controls and their impact on physical security measures are explicitly made.	

CYBERSECURITY CAPACITY PORTAL

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL | SAID BUSINESS SCHOOL | UNIVERSITY OF OXFORD

Home | Threat Spaces | Regions | Challenges | Dimensions | My desk | Search | Add content | Logout

Global | Working Groups | Private

Show unread | Type - Any - | Sort by Most active | Go

Tag cloud

Post

PORTAL HOW TO GUIDE

Portal Team
Global Cyber Security Capacity Centre

0 | 0 | 0 Comments

Post

The Role and Interplay between Nation States...

David A. Bray blogs on changing trends in global cyber security - who plays the key role?

David A. Bray
Senior Executive, U.S. Government

0 | 0 | 0 Comments

Post

Global Cyber Security Capacity Centre

Working Groups Meeting 18 June 2014 - Papers

Portal Team
Global Cyber Security Capacity Centre

0 | 0 | 0 Comments

Video

Aims of the Global Cyber Security Capacity Centre

Portal Team
Global Cyber Security Capacity Centre

0 | 0 | 0 Comments

Post

About the Global Cyber Security Capacity Centre

Portal Team
Global Cyber Security Capacity Centre

0 | 0 | 0 Comments

Article

ISS European Union Institute for Security Studies

EU-ISS: Cyber Capacity Building in Ten Points

Taylor Roberts
James Martin Fellow, Global Cyber S...

0 | 0 | 0 Comments

Article

The Internet Trust Bubble: Global Values, Beliefs and...

Video

The Internet trust bubble: Director's videoblog

Article

A New Privacy Paradox: Young people and privacy...

Article

Cyber Maturity in the Asia-Pacific Region 2014

CYBERSECURITY CAPACITY PORTAL

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL | SAID BUSINESS SCHOOL | UNIVERSITY OF OXFORD

Home | Threat Spaces | Regions | Challenges | Dimensions | My desk | Search | Add content | Logout

View | Edit | Voting details

Video

Professor William Dutton on cyber security, culture and attitudes within society

Posted By: Dr. David A. Bray
16 June, 2014

E-mail | Share | 0 | 0 | Bookmark | Mark as read

Print this

Professor William Dutton on cyber security, culture and attitudes within society. How can we avoid a culture of compliancy or a culture of fear?

Sharing

Shared with

Global | Working Groups | Private

Tags:

cybersecurity | nation states | industry | CERTs | Internet | Jurisdiction | Insurance | future | Dimension 2 | National CERT | trust | National Strategy | Transparency | cyber culture | culture | capacity-building | National CSIRT | industry roles | cyber leadership | cyber responsibility | open questions

Comments

Dr. David A. Bray

Mapping and measuring cybercrime part 1 at: http://cybercapacity.devclo... Mapping and measuring cybercrime part 2 at: http://cybercapacity.devclo... Can we create a multi-stakeholder global cybersecurity commons at: http://cybercapacity.devclo... (note, links might change if the domain name for this website changes) Hope this helps!

19 hours ago | delete | edit

Add your comment...

Submit

Related articles

Article

Cyber Maturity in the Asia-Pacific Region 2014

Posted By: **Taylor Roberts**
16 June, 2014

E-mail Share 0 0 Bookmark Mark as read

Print this

ASPI_cyber_maturity_2014.pdf Download

This report analyses the 'cyber maturity' of 14 countries across the Asia-Pacific region, which represent a wide geographical and economic cross-section of the region. Australia's closest allies, the United States and the United Kingdom, have been included to provide an additionalbenchmark for overall national cyber maturity.

Sharing

Shared with

Global | Working Groups | Private

Tags:

Asia | Pacific | ASPI | maturity model | Metrics

ASPI_cyber_maturity_2014.pdf Download

Comments

Add your comment...

Submit

Related articles

Article
ITU Global Cybersecurity Index Conceptual Framework

Article
SEI - Incident Management Capability Metrics

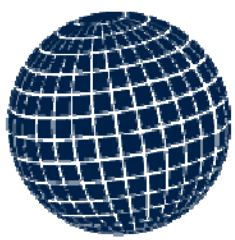
Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Requests for Input

- Cyber Capability Maturity Model (CMM)
  - Promote its application in assisting policy-makers perform effective and informed assessments of cybersecurity maturity
  - When possible, provide feedback to Oxford on its value and impact
- Cybersecurity Capacity Portal:
  - Use as a resource for global information on cybersecurity capacity building
  - Encourage utility, contribution, feedback, and requests for further information



Global
Cyber Security
Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Contact: Taylor Roberts

taylor.roberts@cs.ox.ac.uk

Office #: 01865 (2) 87365