Virtual Event

Building Cyber Resilience with a Professional workforce

a session by IFIP IP3 at the WSIS Forum 2021
Tuesday, April 13, 11:00 GMT

Join us in ifip's jubilee year!
www.ifip.org/jubilee60

How to Protect infrastructure, privacy, consumers and facilitate global skills transfer

Anthony Wong

IFIP Vice President

AGW Lawyers & Consultants

http://www.linkedin.com/in/wonganthony

e anthonywong@agwconsult.com

How to Protect infrastructure, privacy, consumers and facilitate global skills transfer

Since 2018, major developments in Cybersecurity Workforce developments as alerted to by the previous speakers:

- **EU European Cybersecurity Skills Framework https://www.enisa.europa.eu/**
- **UK Government through the UK Cyber Security Council https://www.theiet.org/impact-society/uk-cyber-security-council-formation-project/**
- **And Others**

Australia Introduces Cyber Security Strategy 2020

- Digitization and the use of AI and autonomous systems, IoT, increased connectivity with enhanced computational functionality and connectivity will increase likelihood of cyber-attacks and potential vulnerabilities
- Investment of $1.67 billion over ten years in cyber security – the largest ever financial commitment to cyber security
- Australian Strategy to:
  - increase access to reliable cyber security advice and assistance for families and businesses;
  - boost law enforcement's capacity to combat cyber criminals;
  - improve threat information sharing with industry; and
  - support initiatives to grow a skilled cyber workforce.

Australian ACS Cyber-Security Framework Overview

In September 2018 I presented on the Australian ACS Cyber-Security Framework *at the 24th IFIP World Computer Congress 2018, Poznan Poland*

The presentation available from: PowerPoint Presentation (ipthree.org)

www.ipthree.org/wp-content/uploads/Cyber-Security-specialism-framework-in-action-Anthony-Wong.pdf

ACS Cyber Security Specialism

Background

- Developed in Australia by the ACS.
- Designed to provide a level of Assurance, Trust and to address the growing shortage of cyber security expertise.
- Launched by Australian Minister Assisting the Prime Minister for Cyber Security, the Hon Dan Tehan in Canberra in Sept 2017.
- Raise professional standards for cyber security specialists.
- Highlight the Duty of Care for cyber security professionals.

ACS Professional Certifications

Background

In September 2017, ACS announced an extension of our professional certifications scheme by introducing Cyber Security specialisations.

IFIP IP3 presented to the United Nations Internet Governance Forum (IGF) Geneva, Switzerland 17 December 2017

On "Trust and the IFIP Duty of Care for Everything Digital (iDOCED)"

Refer Transcript:
IGF Presentation (sched.com)
IGF 2017 - Day 0 - Salle 5 - Good Governance is a Professional Standard, Which Builds Trust and Cybersecurity in the Entire Digital Ecosystem | Internet Governance Forum (intgovforum.org)

In the IGF Geneva Presentation, I referred to

Example 1 – Australian Security of Critical Infrastructure Bill 2017 (Australian)

- Australian sabotage laws will be modernised to cover all major critical infrastructure including utilities
- "The Bill will regulate approximately 100 assets in the highest-risk sectors of ports, electricity and water. If any of these assets were disrupted, they would have a significant impact on Australia's economic interests and services for large populations.
- Part 1, Division 2 – Definitions outlines the thresholds for determining which assets will be classed as 'critical infrastructure' and who constitutes a reporting entity or an operator, upon whom the obligations under the Bill will fall."
- This Bill will impose reporting requirements on two sets of entities: direct interest holders and responsible entities.
- Direct interest holders of a critical infrastructure asset will be required to provide interest and control information in respect of the asset. Responsible entities for a critical infrastructure asset (effectively the main licensed body) will be required to provide operational information, such as system access abilities and operator and outsourcing arrangements.
- These entities will have six months to report the required information from the commencement of the legislation.

- The legislation is now the Australian ***Security of Critical Infrastructure Act 2018***
- ***Source: Presentation by Professor Jill Slay, Australian Centre for Cyber Security, UNSW Canberra 2017**

In the IGF Geneva Presentation, I referred to

Example 2 – EU General Data Protection Regulation (GDPR)

- Access to data and its use has become a hot topic.
- At the rate of technological transformation, the debate is unlikely to abate anytime soon.
- The EU leads the world in legislating to protect and provide access to personal data with its EU General Data Protection Regulation (GDPR).
- Replacing the 1995 Data Protection Directive when it comes into operation in May 25, 2018.

Who is caught by the GDPR?

- Businesses with an establishment in the EU or that offer goods and services in the EU, or that monitor the behaviour of individuals in the EU may need to comply.

How to Protect infrastructure, privacy, consumers and facilitate global skills transfer

Since 2017, many major developments around the world in Cybersecurity regulation frameworks (to name a few) to Protect infrastructure, privacy, consumers, including:

- The EU *Cybersecurity Act* comes into force in June 2020 and introduces an EU-wide cybersecurity certification framework for the certification of ICT products, services and processes
- The US *IoT Cybersecurity Improvement Act* becomes law in December 2020
- In November 2020, Singapore passed amendments to the *Personal Data Protection Act* to include: mandatory data breach notification and enhancing the enforcement regime
- Australia has Breach Notification laws and is currently reviewing the Privacy Act including consideration of giving individuals direct rights of action
- In December 2020, Australia proposed enhancements to the *Security of Critical Infrastructure Act 2018*

Australia Extends Critical Infrastructure Legislation

- Many countries including Australia is looking at regulatory frameworks to support their Cyber Security Strategy
- Security Legislation Amendment (Critical Infrastructure) Bill 2020 supports Australia's Cyber Security Strategy 2020 and builds on the existing regulatory framework—Security of Critical Infrastructure Act 2018
- The proposed changes provide wider government powers, including:
  - government assistance and intervention to respond to serious cyber security incidents;
  - mandatory cyber incident reporting and a risk management program; and
  - creating additional cybersecurity obligations for critical infrastructure entities.

Australia Introduces Draft of Critical Infrastructure Bill

Proposed changes to ***Security of Critical Infrastructure Act 2018*** (Cth) to expand coverage and definition of 'critical infrastructure sector' beyond electricity, gas, water and maritime ports to additional 11 classes including:

1. communications;
2. data storage and processing;
3. defence;
4. financial services and markets;
5. food and grocery;
6. health care and medical;
7. transport;
8. higher education and research;
9. energy;
10. space technology; and
11. water and sewerage.

Facilitate global skills transfer

Cybersecurity is more than just technical

It is multi-disciplinary requiring understanding of many facets including:

- Maths
- Cryptography
- Psychology
- Economics
- Security
- Risks
- Auditing and
- Legal frameworks.

Facilitate global skills transfer

- Who has the right qualifications?
- How do we ensure alignment of competence frameworks?
  - European Cybersecurity Skills Framework
  - UK Cybersecurity Skills Framework
  - Australian ACS Cybersecurity Skills Framework
  - Other Cybersecurity Skills Framework
- Can we have a skills framework for a common understanding of the roles, competencies, skills and knowledge used by individuals, employers and training providers across the UN Member States?
- How do we foster a common benchmarking system for cybersecurity skills, collaboration on the various frameworks, and support the global skills transfer of cybersecurity specialists?

How to Protect infrastructure, privacy, consumers and facilitate global skills transfer

Thank You

Anthony Wong
Vice President, IFIP
AGW Lawyers & Consultants
http://www.linkedin.com/in/wonganthony
e anthonywong@agwconsult.com

ifip 60 YEARS

Virtual Event

Building Cyber Resilience with a Professional workforce

a session by IFIP IP3 at the WSIS Forum 2021
Tuesday, April 13, 11:00 GMT

Join us in ifip's jubilee year!
www.ifip.org/jubilee60