
INSPIRING OUR NEXT TECH SUPERHEROES
Think Ahead. Create the Future. Change the World.
acs
superhero.acs.org.au

Cyber-Security Framework Overview

By Anthony Wong, ACS Immediate Past President,
IFIP IP3

24th IFIP World Computer Congress

September 18 2018

Poznan Poland

Cyber-Security Framework Overview

- Cybersecurity, Privacy and Technological challenges – what are Organisation and Government seeking?
- Aligning Business and Organisation priorities with security professionals
- The Professionalisation of Cybersecurity and Privacy practitioners
- Challenges & key issues – is EU GDPR transforming the landscape?
- What if we don't?

ACS Professional Certifications

Background

Certified Professional (CP) is aligned to level 5 of the Skills Framework for the Information Age accredited by IFIP IP3.

Certified Technologist (CT) is aligned to level 3 of the Skills Framework for the Information Age accredited by IFIP IP3.

Duty of Care for Governments

- Requirement to work with international organisations on:
  - ✓Regulations
  - ✓Standards
  - ✓Mandatory professional standards & accreditations
  - ✓Develop partnership agreements with other countries
- Legislate for mandatory reporting of cyber attacks
- Engage in trusted threat intelligence sharing
  - ✓State-sponsored attacks

‘Cyber Security’ for Governments?

Overview

- Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.’
- Has implications from Government perspectives on
  - *Cyber Law*
  - *Domestic Cyber Policy*
  - *International Cyber Policy*
  - *Communicating Cyber Security Issues*
  - *Offensive Cyber Effects / warfare*
  - *Cyber Economy- start ups and commercialisation*
  - *Cyber intelligence and forensics*
- Estimation that we in Australia need 8000 more practitioners to meet status quo by 2025 and 10-11,000 to deal with growth - >1 million globally

Cyber Security, Privacy and Technological challenges

- Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 – CSO https://www.csoonline.com/.../cybersecurity-labor-crunch-to-hit-35-million-unfilled-j...
  - Jun 6, 2017 - The cyber crime epidemic is expected to triple the number of open ... alone will need 1 million cybersecurity professionals by 2020 to meet the demands ... If that's true, then the cybersecurity workforce shortage is even worse ...
- Cybersecurity Jobs Report 2018-2021 - Cybersecurity Ventures https://cybersecurityventures.com/jobs/
  - Feb 23, 2018 - A 2016 skills gap analysis from ISACA estimated a global shortage of 2 million cybersecurity professionals by 2019 (a half-million more than ...
- The Evidence Is in the Numbers: We Need More Cyber Security Pros https://www.tripwire.com › Home › News
  - Mar 18, 2018 - Fighting Cyber Crime Requires Professionals, Talent Which is in Short ... primary factors contributing to today's cyber security talent shortage:.
- Global Shortfall of 1.8 Million Cyber Security Pros Expected by 2022 https://www.esecurityplanet.com/.../global-shortfall-of-1.8-million-cyber-security-wor...
  - Feb 16, 2017 - A recent survey of more than 19,000 cyber security professionals found that the world is expected to face a shortfall of 1.8 million cyber security ...
- Cybersecurity world faces 'chronic shortage' of qualified staff https://www.theregister.co.uk/2017/.../chronic_shortage_qualified_cybersecurity_bods...
  - Aug 24, 2017 - Cybersecurity world faces 'chronic shortage' of qualified staff ... per cent of them have reported a shortage of information security professionals.
- Cybersecurity Faces 1.8 Million Worker Shortfall By ... - Dark Reading https://www.darkreading.com/careers-and.../cybersecurity...18...shortfall.../1329084
  - Jun 7, 2017 - (ISC)2's Global Information Security Workforce Study, which queried 19,000 cybersecurity professionals worldwide, found 66% of survey ...
- Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022 ...blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
  - Feb 15, 2017 - The workforce gap is estimated to be growing, with the projected shortage reaching 1.8 million professionals by 2022. While the gap is not ...

ACS Cyber Security Framework

Background

The approach of contextualizing existing international frameworks identified as best practice by the ACS, for appropriate implementation in the domestic Australian market has been taken.

We have asked ourselves:

- What should a Cyber skilling framework look like?
- What does International Best Practice look like?
- How can we ‘Australianise’ it?

Cyber Security, Privacy and Technological challenges

Overview

- Definitions of ‘Cyber security’ still unclear.
- Strong demand for Cyber security practitioners but understanding of ‘professionalism’ not explicit.
- Pseudo Professional Standards.
- Australian Development of Professional Standards in Cyber Security.
- Cyber security and privacy issues are now mainstream in the boardroom and in mainstream news eg data breaches, Cambridge Analytica/Facebook.

ACS Cyber Security Specialism

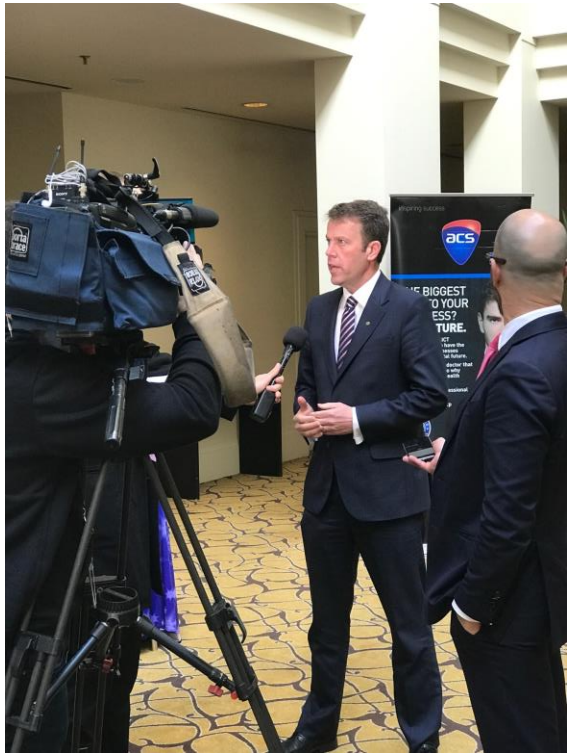
Background

- 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.
- Adopted by IFIP IP3 as a new specialism certification for member societies around the world.
- ACS support for the implementation of the Australian International Cyber Engagement Strategy announced by the Hon Julie Bishop MP, Minister for Foreign Affairs in October 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.



ACS Professional Certifications

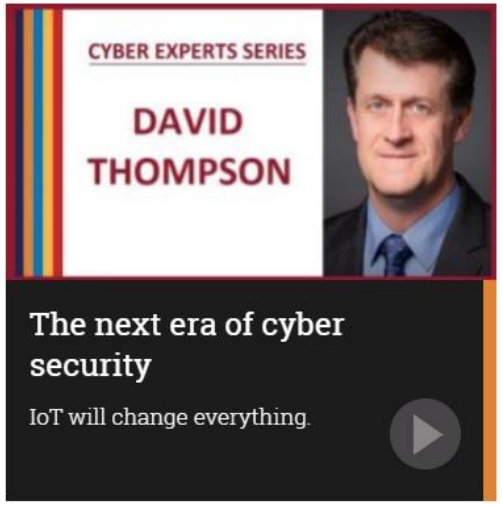
Background

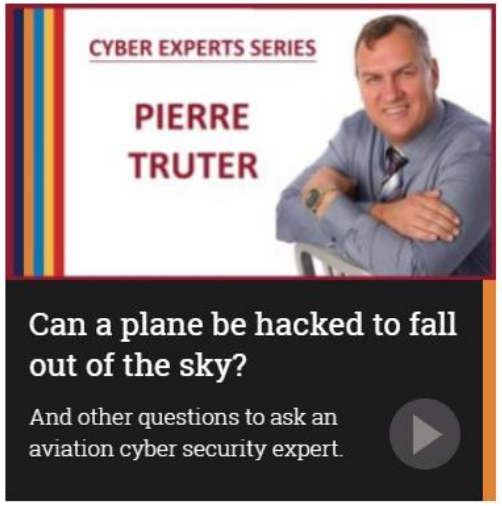
In September 2017, ACS announced an extension of our professional certifications scheme by introducing Cyber Security specialisations.

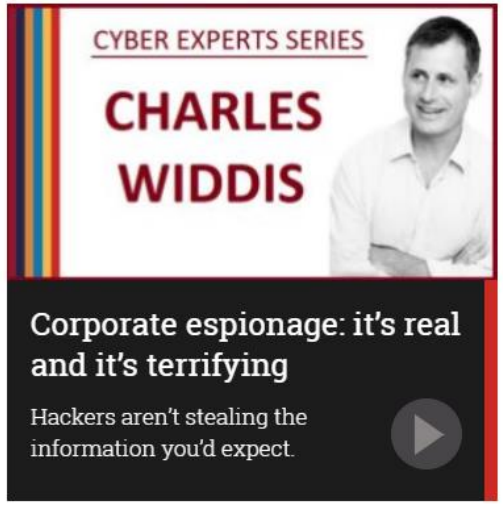
ACS Professional Certifications

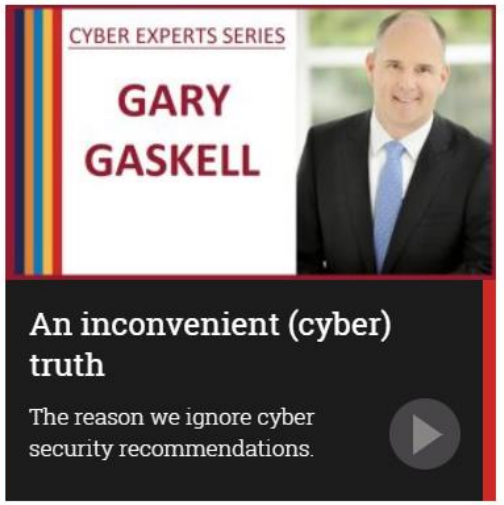
Background

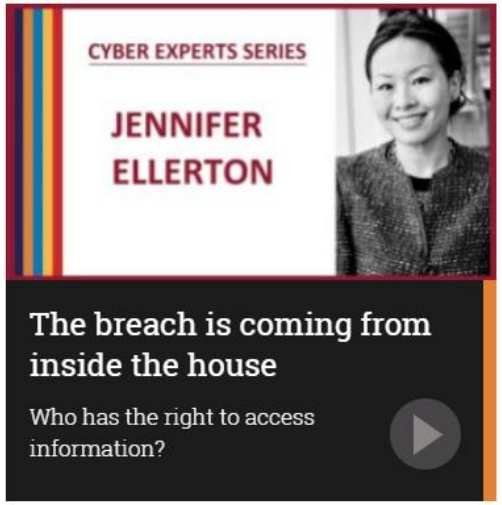
50+ Certified Professional (Cyber Security) across aviation, banking and finance, audit and risk, consulting, healthcare.

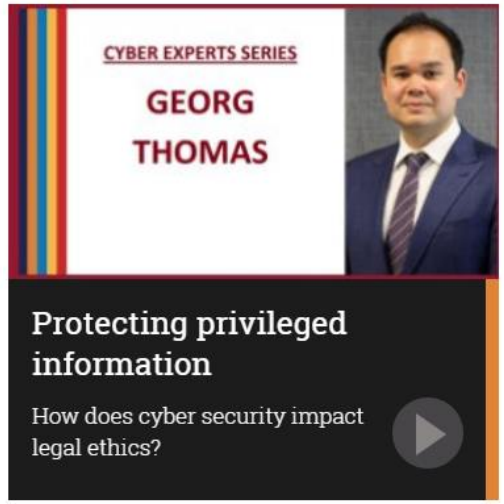


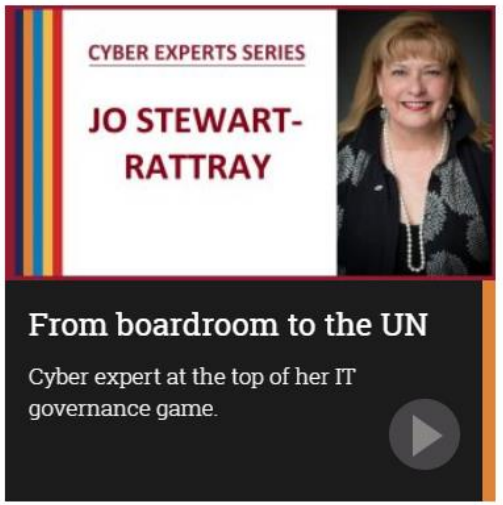


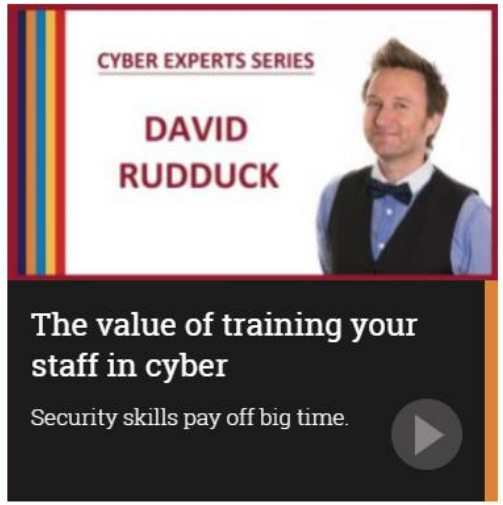












Aligning Business and Organisation priorities with security professionals

Draft NIST Special Publication 800-37 Revision 2 deals with Privacy Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy
https://www.youtube.com/watch?v=cDgCL363c3A

"A New Era of Privacy & Data Security" featured BigID Senior Director of Privacy Strategy Debra Farber CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP-panel discussed …the importance of collaboration between privacy and security teams

Black Hat 2018 and RSA 2018 (primarily security conferences)- privacy playing growing and more significant role

The Professionalisation of Cybersecurity and Privacy practitioners

Why do we need Professional Standards?

For Governments to develop cyber policy, legislation, technology, curricula and cyber industry growth we must:

- Establish the minimum independent professional standard of competence for a cyber security practitioner – cf. engineering
- Provide a complete requirement for full professional formation of a cyber security practitioner.
- Assure employer of the maintenance of competence through continuing professional development.
- Ensure compliance with an appropriate ethical and legal framework, resulting from the deployment of emerging technologies such as AI and machine learning with its accompanying societal challenges
- Support by a disciplinary code with a process for public complaint and sanctions.
- Without Professional Standards we cannot ensure good governance, duty of care, validation and verification of results, efficiency, effectiveness, an appropriate future work force in a cyber context.

EU General Data Protection Regulation (GDPR) transforming the landscape

- 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 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
- Significant penalties for non-compliance => fines up to 20 million Euros or 4 per cent of global turnover

EU General Data Protection Regulation (GDPR) transforming the landscape

Art. 37 GDPR requires designation of the data protection officer in certain circumstances:

And "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39"

Art. 39 GDPR Tasks of the data protection officer include at least the following tasks:

to inform and advise in relation to obligations pursuant GDPR (including **Art. 32 GDPR Security of processing)**

to monitor compliance with …in relation to the protection of personal data

…

Art. 32 GDPR Security of processing

taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…

…

EU General Data Protection Regulation (GDPR) transforming the landscape

Art. 38 GDPR Position of the data protection officer

shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data

Organisation shall support the data protection officer in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge

The controller and processor shall ensure that the data protection officer:

does not receive any instructions regarding the exercise of those tasks

shall not be dismissed or penalised …for performing tasks

directly report to the highest management level of the controller or the processor

shall ensure that any such tasks and duties do not result in a conflict of interests

What if we don't?

- Trust requires certainty in the areas of:
  - Security
  - Safety
  - Privacy
  - Reliability/Performance
  - Usability
  - Access
- A breach in *any one* of these areas will *diminish trust* and *discourage users from engaging* with systems/technology.

Thank you

E: ***anthony.wong@acs.org.au***

IFIP Councillor, a technologist and a lawyer