

INSPIRING OUR NEXT TECH SUPERHEROES

Think Ahead. Create the Future. Change the World.



superhero.acs.org.au

Cyber-Security Framework in action

By Anthony Wong, ACS Immediate Past President

IFIP IP3, a technologist and a lawyer

Presented at the 24th IFIP World Computer Congress

September 21 2018

Poznan Poland

acs.org.au



On
September 18
2018
I spoke on
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?

Cyber-Security specialism framework in action

- What's happening around the world including EU GDPR?
- Framework for implementation

What's happening around the world – Cyber Skills shortages

- Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 – CSO <https://www.csoononline.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](http://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 ...

What's happening around the world – Data Breaches

Top stories

- [List of data breaches and cyber attacks in July 2018 – 139,731,894](https://www.itgovernance.co.uk/.../list-of-data-breaches-and-cyber-attacks-in-july-2018)
...<https://www.itgovernance.co.uk/.../list-of-data-breaches-and-cyber-attacks-in-july-2018>... Jul 30, 2018 - I imagine human error will continue to be the main cause of **data breaches** for decades to come – damn humans. I count this month's list of ...
- [List of data breaches and cyber attacks August 2018 – 215,000,000](https://www.itgovernance.co.uk/.../list-of-data-breaches-and-cyber-attacks-august-2018)
...<https://www.itgovernance.co.uk/.../list-of-data-breaches-and-cyber-attacks-august-2018>... Aug 29, 2018 - As we end the near of August, it's time to tally up the month's **breaches**.
- [These are 2018's biggest hacks, leaks, and data breaches | ZDNet](https://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2018/)
<https://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2018/> Jul 24, 2018 - January: A **database** used by the Department of Homeland **Security's** Office of the Inspector General was confirmed **breached** in January, ...
- Hackers stole customer credit cards in Newegg data breach TechCrunch · 23 hours ago
- [Equifax fined by ICO over data breach that hit Britons](#) BBC News · 13 hours ago
- [Equifax fined £500,000 for data breach of 15m UK customers](#) Telegraph.co.uk · 13 hours ago
- The British Airways hack is impressively bad | WIRED UK
<https://www.wired.co.uk/article/hacks-data-breaches-in-2018> BA is the latest company to be hit by hackers. We chart the biggest **data breaches** of 2018.
- Jul 9, 2018 - **Data breaches** have continued apace in **2018**, but their quiet cousin, **data** exposure, has been prominent this year as well. A **data** exposure, as the name suggests, is when **data** is stored and defended improperly such that it is exposed on the open internet and could be easily accessed by anyone who comes across it.



What's happening around the world including EU General Data Protection Regulation (GDPR)

- 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)

Some Key Considerations

- Require businesses to take appropriate technical and organisational security measures, including effective cyber security measures.
- Accountability and governance - Accountability principle in GDPR Article 5(2) requires demonstration of compliance with the principles.
- Enhanced measures including:
 - Data minimisation;
 - Pseudonymisation;
 - Transparency;
 - Allowing individuals to monitor processing; and
 - Creating and improving security features on an ongoing basis.
- Use of Privacy Impact Assessments (PIA) where appropriate.
- Records of processing activities (documentation).
- Obligation to provide comprehensive, clear and transparent privacy policies.
- In many circumstances, controllers and processors will need to appoint Data Protection Officers (DPOs).



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

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

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.



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

Certified Professional – Cyber Security

Reflecting the multi-disciplinary nature of Cyber Security, flexibility was consciously built into the specialism assessment process.

An applicant must be able to demonstrate in-depth capability in **four skills from the following list** of level 5 (or higher) of the Skills Framework for the information Age (SFIA). SFIA skills must be from the following skills:

- IT Governance
- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Penetration Testing
- Security Administration
- Programming/Software Development
- Systems Software
- Testing
- Asset Management

ACS Professional Certifications

Certified Technologist – Cyber Security

For CT - an applicant must be able to demonstrate in-depth capability in **four skills from the following list** of level 3 (or higher) of the Skills Framework for the information Age (SFIA). SFIA skills must be from the following skills:

- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Systems Development Management
- Asset Management
- Change Management
- Security Administration
- Incident Management
- Conformance Review

ACS Professional Certifications

Background

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

CYBER EXPERTS SERIES

DAVID THOMPSON



The next era of cyber security

IoT will change everything.



CYBER EXPERTS SERIES

PIERRE TRUTER



Can a plane be hacked to fall out of the sky?

And other questions to ask an aviation cyber security expert.



CYBER EXPERTS SERIES

CHARLES WIDDIS



Corporate espionage: it's real and it's terrifying

Hackers aren't stealing the information you'd expect.



CYBER EXPERT SERIES

JEFF YONG XUN XIE



Is blockchain the future of cyber security?

Why banning ICOs will hinder innovation.



CYBER EXPERTS SERIES

GARY GASKELL



An inconvenient (cyber) truth

The reason we ignore cyber security recommendations.



CYBER EXPERTS SERIES

JENNIFER ELLERTON



The breach is coming from inside the house

Who has the right to access information?



CYBER EXPERTS SERIES

RAYMOND FRANGIE



The dangers of 'non-existent' cyber security

Too many smart buildings are at major risk of an attack.



CYBER EXPERTS SERIES

GEORG THOMAS



Protecting privileged information

How does cyber security impact legal ethics?



CYBER EXPERTS SERIES

JO STEWART-RATTRAY



From boardroom to the UN

Cyber expert at the top of her IT governance game.



CYBER EXPERTS SERIES

DAVID RUDDUCK



The value of training your staff in cyber

Security skills pay off big time.





Thank you

E: anthony.wong@acs.org.au

IFIP IP3 Board Member, a technologist and a lawyer

