Guest Speaker

Denny Wan

Dimensioning security capability Under APRA CPS 234 planning

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

About me

Denny Wan

- Cyber risk practitioner - Principal Consultant, Security Express
- Researcher @ Macquarie University – Cyber Insurance Pricing Strategies
- Chair – FAIR Sydney Chapter
- Chair – Australian Cyber Insurance Think Tank

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Overview of CPS 234

- Released 7th Nov 2018

Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018

Prudential Standard CPS 234 Information Security

https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Overview of CPS 234

- Released 7th Nov 2018

The key requirements of this Prudential Standard are that an APRA-regulated entity must:

- clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals;
- maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- notify APRA of material information security incidents.

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Overview of CPS 234

Sydney Branch Meeting: November 22

TWO presentations (2CPE) The Workplace of the Future, Steering the Ship into Unchartered Waters, People, Technology and Security & A Perspective on Upcoming APRA 234 Standards for the Industry

.

Speaker ONE: Aatef Khayat Director Dragonfly Technologies and former Optus Business CTO will discuss, **"The Workplace of the Future, Steering the Ship into Unchartered Waters, People, Technology and Security"**

Speaker TWO: Wilson Chiu Head Of Security at Police Bank Ltd will discuss **"A Perspective on Upcoming APRA 234 Standards for the Industry"**

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

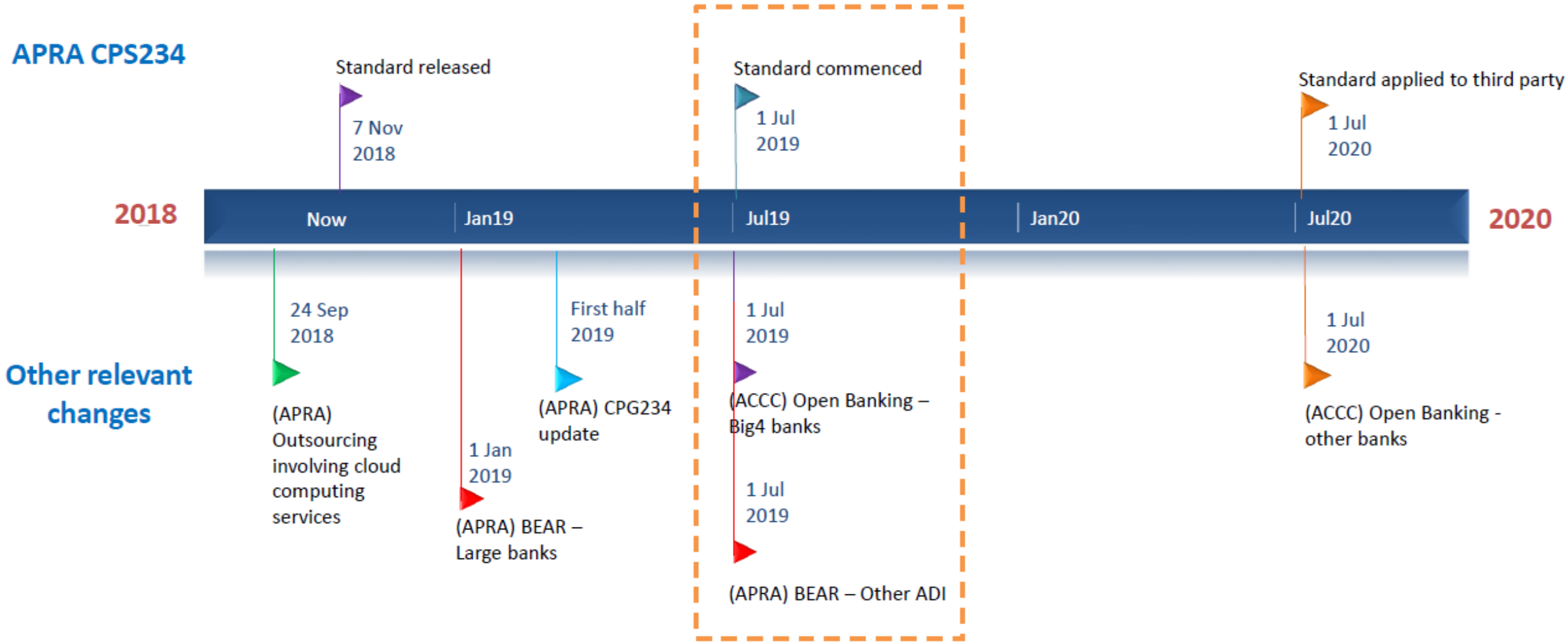
greenbox

DXC.technology

HUAWEI

https://www.aisa.org.au/Public/Events/Event_Display.aspx?EventKey=880b141d-e998-4a0a-b05e-5ffc9456282b

Exciting times ahead



Key takeaways

- Board and management are responsible
- Recognising of third party risk
- Acknowledge shortage of security skills and recommend use of external resource
- Comprehensive coverage instead of based on materiality
- APRA notification

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Anatomy of CPS 234

36 requirements in CPS234

Ref	Sections
13-14	Roles and responsibilities
15-17	Information security capability
18-19	Policy framework
20	Information asset identification and classification
21-22	Implementation of controls
23-26	Incident management
27-31	Testing control effectiveness
32-34	Internal audit
35-36	APRA notification

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Anatomy of CPS 234

briefing note
385
Jan 2019

CPS 234: Will you comply? Information Security standard for APRA regulated organisations

By Denny Wan[1] and Tahiry Rabehaja[2]

Synopsis

In November 2018, the Australian Prudential Regulation Authority (APRA) released Prudential Standard CPS 234 making the board of regulated entities accountable for ensuring the adequacy and sustainability of their information security program. APRA's standard was published 9 months after the Notifiable Data Breach scheme[3] came into effect in the first quarter of 2018. The CPS 234 comes into full force in July 2019 with a 12 month extension for third party supplier contracts until July 2020.

https://riskfrontiers.com/rf2018/wp-content/uploads/2019/01/Briefing-Note-385.pdf

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

CPS 234 is a board problem

To ensure compliance, clause 13 explicitly makes the board of the regulated entities be ultimately accountable:

13. The Board[4] of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[5]

15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

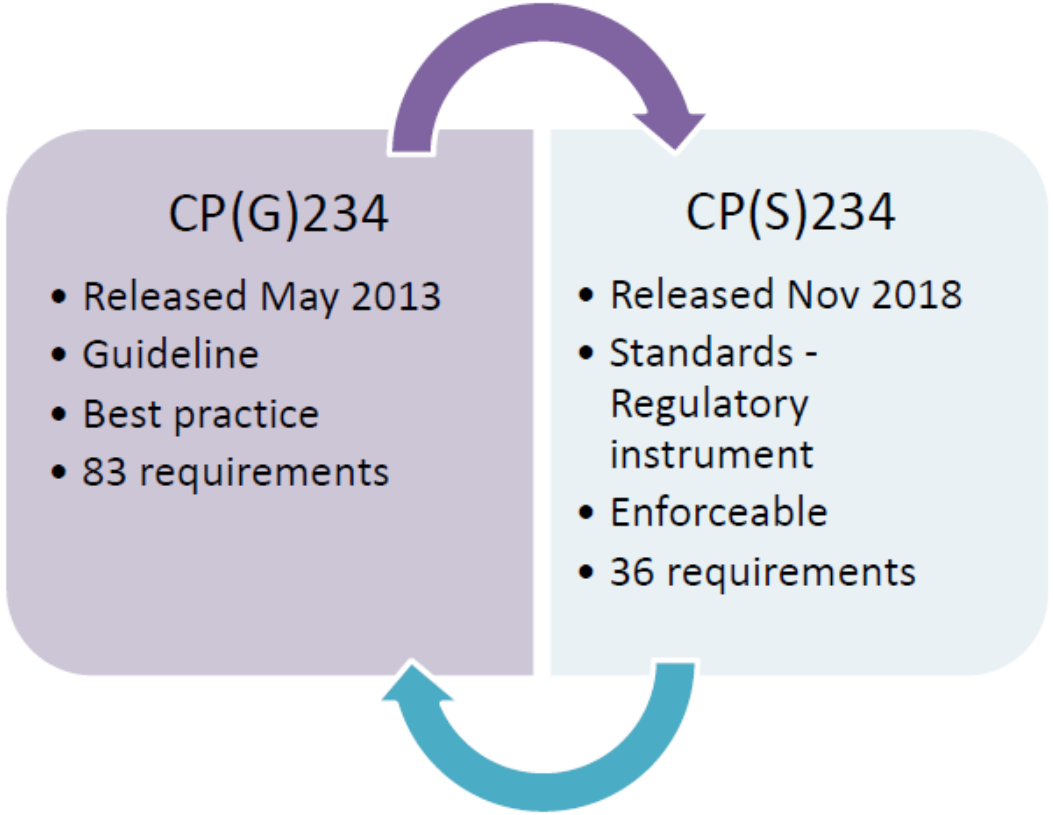
LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

CPG 234 vs CPS 234



Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Sections in CPG 234

1. IT security risk
2. An overarching framework
3. User awareness
4. Access Control
5. IT asset life-cycle management controls
6. Monitoring and incident management
7. IT security reporting and metrics
8. IT security assurance

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

CPG 234

1. IT security risk
2. An overarching framework
3. User awareness
4. Access Control
5. IT asset life-cycle management controls
6. Monitoring and incident management
7. IT security reporting and metrics
8. IT security assurance

CPS 234

Ref	Sections
13-14	Roles and responsibilities
15-17	Information security capability
18-19	Policy framework
20	Information asset identification and classification
21-22	Implementation of controls
23-26	Incident management
27-31	Testing control effectiveness
32-34	Internal audit
35-36	APRA notification

CPG 234

An overarching framework

Hierarchy of policies, standards, guidelines and procedures

22. An IT security risk management framework outlines a regulated institution's approach to managing IT security and is typically embodied in a hierarchy of policies, standards, guidelines and procedures. It would typically align to other enterprise frameworks such as project management, outsourcing management and risk management.

23. The IT security risk management framework would typically enable the design and implementation of the IT security controls. The strength of controls would normally be commensurate with the criticality and sensitivity of the IT asset involved.

24. The establishment and ongoing development of the IT security risk management framework would normally be directed by an overarching IT security strategy and a supporting program of work. This strategy would typically be aligned with a regulated institution's IT and business strategies, as appropriate.

A principles-based approach

26. APRA envisages that a regulated institution would adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework. Common IT security principles include:

    (a) defence-in-depth and diversity of controls, where multiple layers and types of controls are used to address risks in different ways. Therefore, should one control layer be compromised, other control(s) limit the impact on a regulated institution;

    (b) denial of all features, permissions, functions and protocols unless required to conduct business operations. This reduces the number of attack approaches that may be used to compromise IT assets;

    (c) timely detection and reporting of IT security breaches. This minimises the time in which a compromise of an IT asset can impact on a regulated institution;

    (d) appropriately controlled error handling. Errors should not allow unauthorised access to IT assets or other IT security compromises;

CPS 234

Policy framework

18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.[8]

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Materiality considerations

39 submissions received for the draft CPS 234 covering 5 main areas:

Chapter 2 - Response to submissions

2.1 Identifying and classifying information assets

2.2 Third party arrangements

2.3 Notifications to APRA

2.4 Transition matters

2.5 Scope of application

Two main concessions:

1. Extension of notification period
2. Delay 3rd party contracts compliance by 12 months to July 2020

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Materiality considerations

Information security is a business problem

APRA has made it clear in its response to the submission to the draft CPS 234[5] that it intentionally makes the boards accountable for information security. This clearly means that information security is a business problem and not just an IT challenge. In its response, APRA explained that some submissions sought clarification on the "materiality rules". Page 7 of the response gives one example of such a request:

various requests for the application of a materiality threshold in relation to certain requirements in CPS 234 as the basis for determining the need to apply requirements or the degree of work required in applying certain requirements in the standard. For example, some submissions argued for a materiality threshold to apply in relation to testing the effectiveness of information security controls, and in determining the need to escalate and report testing results to the Board or senior management where security control deficiencies are identified that cannot be remediated in a timely manner;

Response to submissions on public consultation of draft CPS 234

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Materiality considerations

The following emphasis is further stated on page 8 under the section “APRA Response”:

This reflects the fact that ensuring the information security of all information assets remains the responsibility of the regulated entity and that the Board is ultimately responsible for the information security of the regulated entity.

A reasonable interpretation of APRA’s response is that the board is responsible for determining the materiality of information risk and adequacy of the controls. This interpretation is echoed by several commentators [6] [7] [8].

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Cyber risk is a business problem

- It is not a matter of technology but business and investment priorities
- Clause 15 demands ".. *security capability* ***commensurate*** *with the size and extent of threats to its information assets* .."
- Boards are required to demonstrate the cyber security investment is proportionate and sufficient to reflect the threat
- It is no longer sufficient to just approve the cyber security budgets
- Boards need to set cyber security strategies from a business perspective
- Boards are responsible for ***prioritisation*** of investment strategies

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

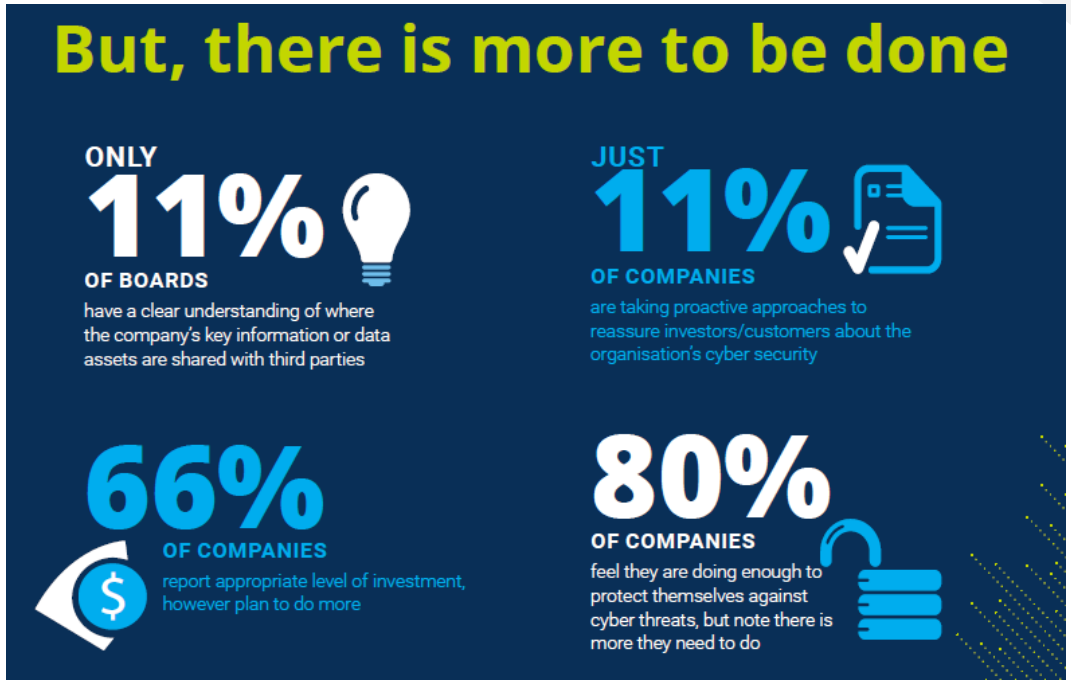
greenbox

DXC.technology

HUAWEI

ASX 100 Cyber Health Check Report (2016)

- Confirmed high level of board awareness of cyber risk
- Now is time to act



http://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Factor Analysis of Information Risk (FAIR)

- Prioritisation requires quantification of risk not effort

What is the FAIR Institute?

Factor Analysis of Information Risk (FAIR) has emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk.

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk.

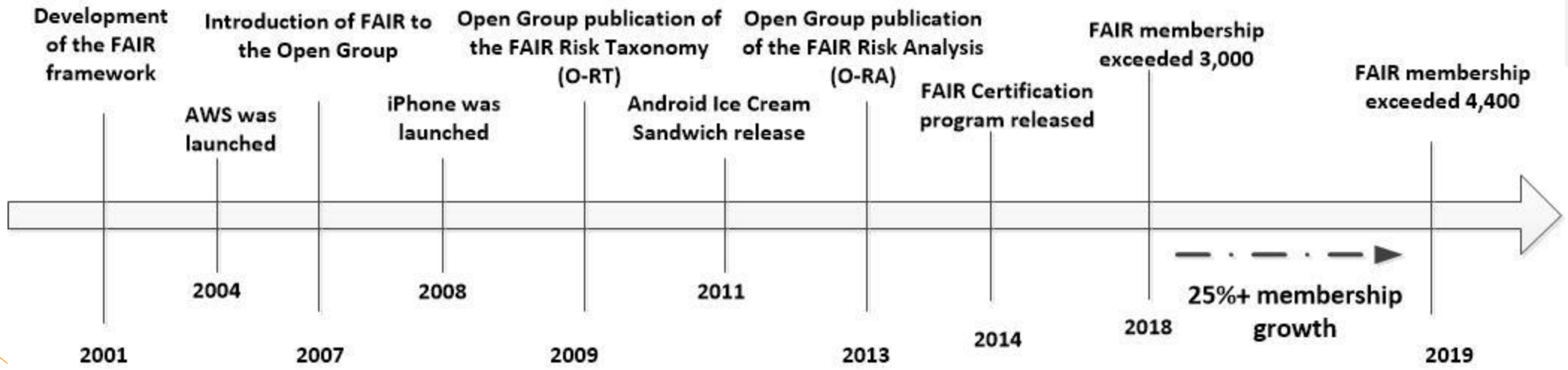
It provides information risk, cybersecurity and business executives with the standards and best practices to help organizations measure, manage and report on information risk from the business perspective. The FAIR Institute and its community focus on innovation, education and sharing of best practices to advance FAIR and the information risk management profession.

4,400+ Members Worldwide

30% Fortune 1000 Orgs.

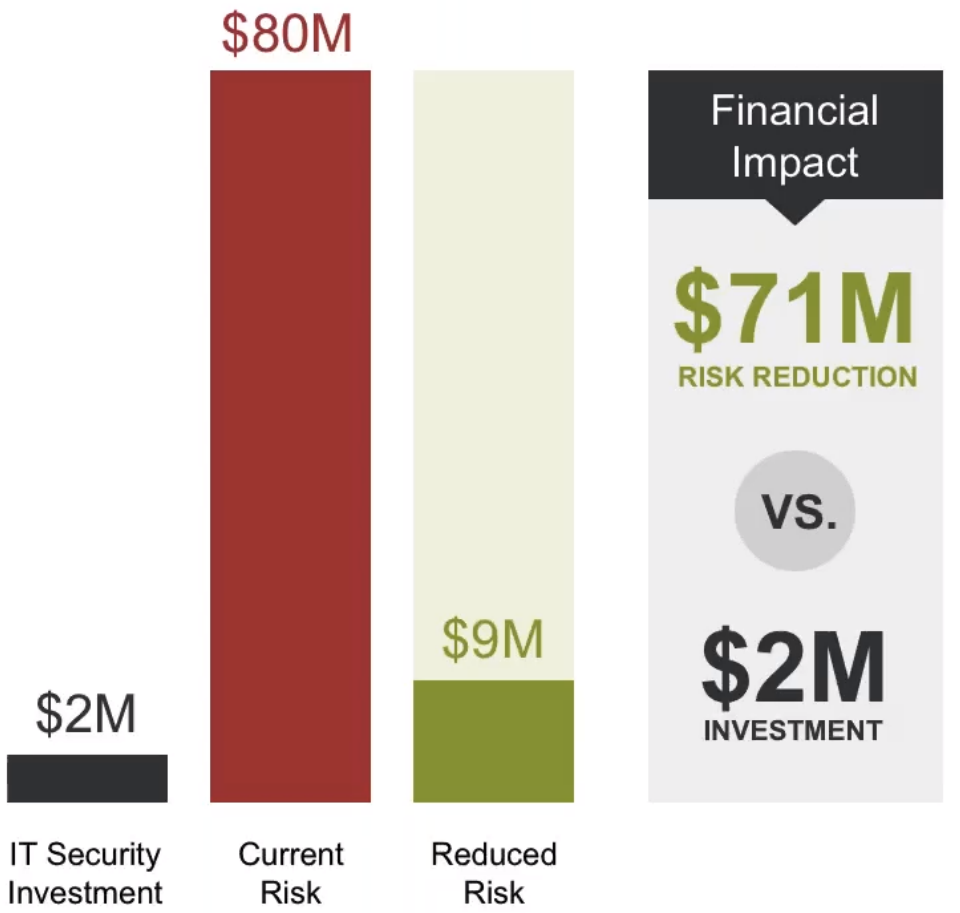
The FAIR Institute

History of FAIR



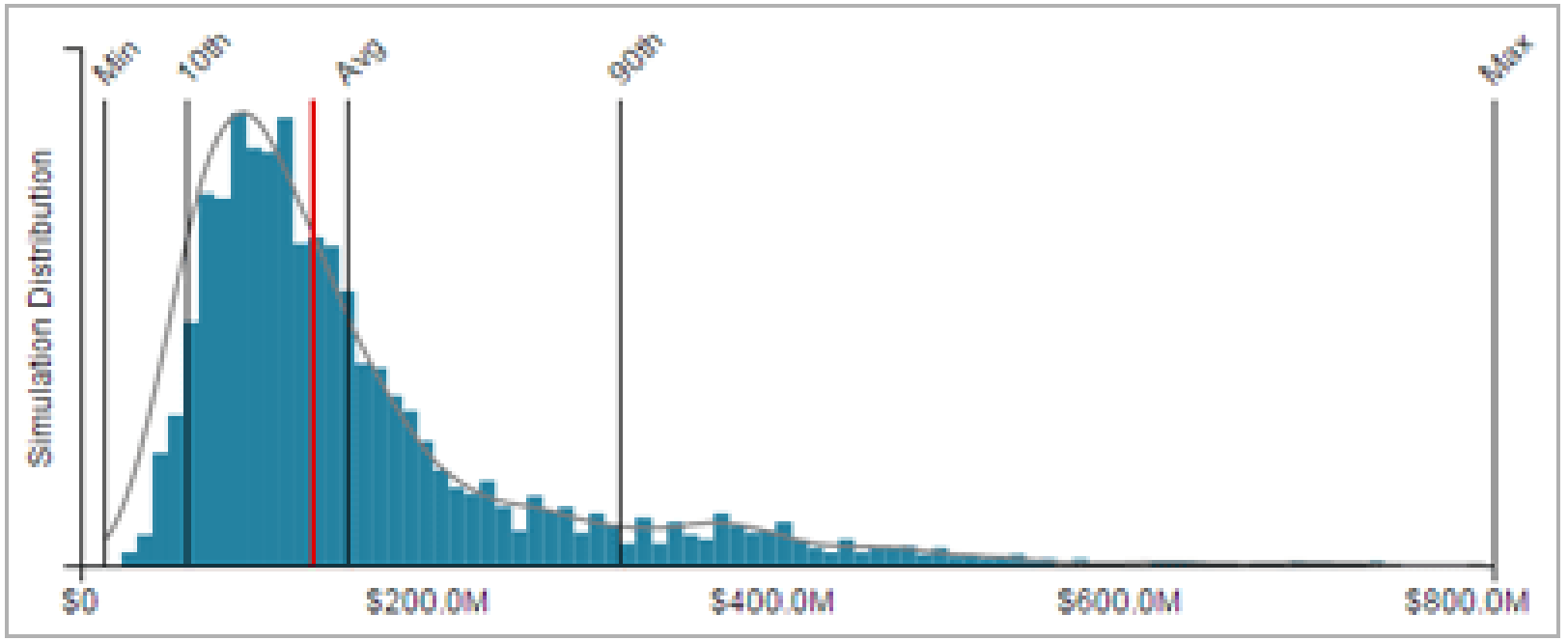
MULTIPLE DIMENSIONS OF ROI

USE CASES	ROI
Understand Loss Exposure	Preserve Business Value
Prioritize Risk Mitigations	Maximize Risk Reduction
Assess ROI of Security Initiatives	Optimize Cybersecurity Investments
Meet Cyber Regulations	Pass Compliance Audit
Optimize Cyber Insurance Coverage	Facilitate Risk Transfer



RiskLens

- Risk management is about dimensioning the **probabilities** of loss
- FAIR is a structured quantification approach expressed as distribution of **probabilities**



Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

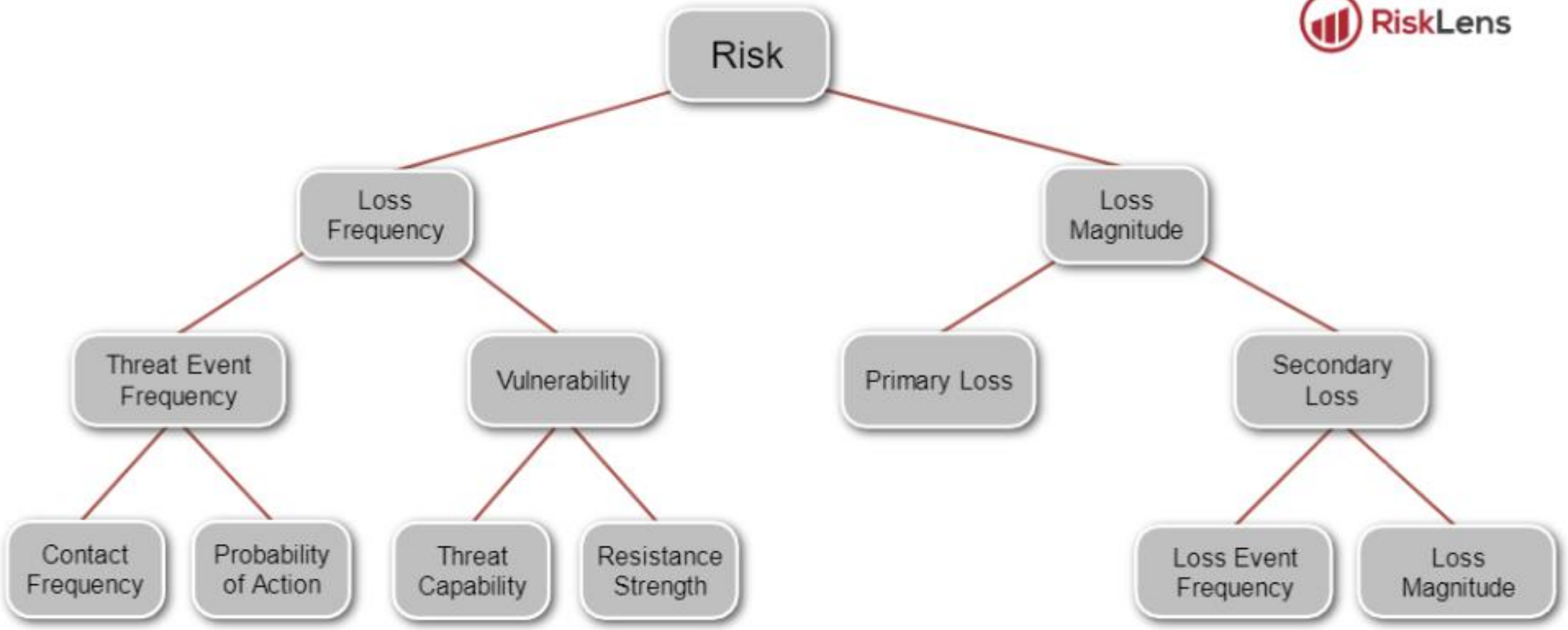
LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

FAIR is a taxonomy



RiskLens

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Agenda

- Overview of CPS 234
- Anatomy of CPS 234
- CPG 234 vs CPS 234
- Materiality considerations
- Cyber risk is a business problem
- Open Group FAIR
- Resources

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

FAIR standards are FREE to download

Open FAIR™ Certification

The Open Group Open FAIR™ Certification Program is aimed at meeting the needs of risk analysts and organizations employing risk analysts. The program is based upon Open Factor Analysis of Information Risk (FAIR), an open and independent information risk analysis methodology.

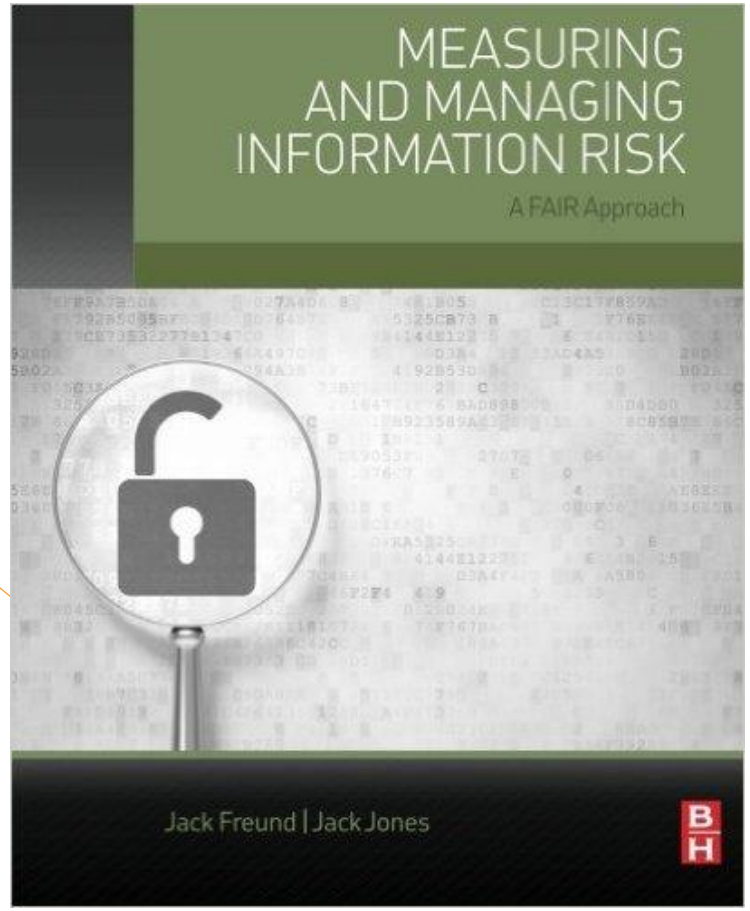
Open FAIR is gaining significant acceptance among large organizations as a leading risk analysis methodology. The Open Group has published two Open FAIR standards :

- Open Risk Taxonomy Technical Standard (O-RT). This standard defines a standard taxonomy of terms, definitions, and relationships used in risk analysis.
- Open Risk Analysis Technical Standard (O-RA). This standard describes process aspects associated with performing effective risk analysis.

These two standards constitute the body of knowledge for The Open Group FAIR Certification Program.

https://www.opengroup.org/certifications/openfair

The FAIR Book by Jack Jones



FAIR Institute Membership Benefits

	General	Executive	Charter
FAIR Institute LinkedIn Group (Private)	✓	✓	✓
FAIR Institute Member Resources	✓	✓	✓
Early Access to FAIR Workgroups Output		✓	✓
Free e-copy of Chapter 3 of FAIR Book		✓	✓
Free copy of the FAIR Book			✓
Discount on FAIR Conference			✓

Free book for Executive and Charter members
https://www.fairinstitute.org/get-involved

Core

Huntsman Defence-Grade Cyber Security
tenable
dimension data
Sladen Legal
LastPass by LogMeIn
greenbox
DXC.technology
HUAWEI

ALL membership are still **FREE!** **Join now**

Supported by open source tools

HOME / THE OPEN FAIR™ RISK ANALYSIS TOOL BETA (90-DAY BETA EVALUATION LICENSE)

THE OPEN FAIR™ RISK ANALYSIS TOOL BETA (90-DAY BETA EVALUATION LICENSE)

REFERENCE: I181

AVAILABLE TO DOWNLOAD

Downloading the Beta Version of the Open FAIR™ Risk Analysis Tool

The Open FAIR Risk Analysis Tool can be used to perform a quantitative Open FAIR risk analysis as defined in The Open Group Risk Analysis (O-RA) and Risk Taxonomy (O-RT) standards. It is provided in the form of a Microsoft® Excel® spreadsheet.

The Beta version of the Open FAIR Risk Analysis Tool is available to all to download free-of-charge for non-commercial use. That will usually mean using it inside your organization. To use the Open FAIR Risk Analysis Tool for commercial purposes, a Commercial License will be made available with version 1.0 of the tool.

Availability

- Download Open FAIR™ Risk Analysis Macro File (xlam)
- Download Open FAIR™ Risk Analysis Tool User's Manual PDF File
- Download Open FAIR™ Risk Analysis Tool xlsx File

https://publications.opengroup.org/i181

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

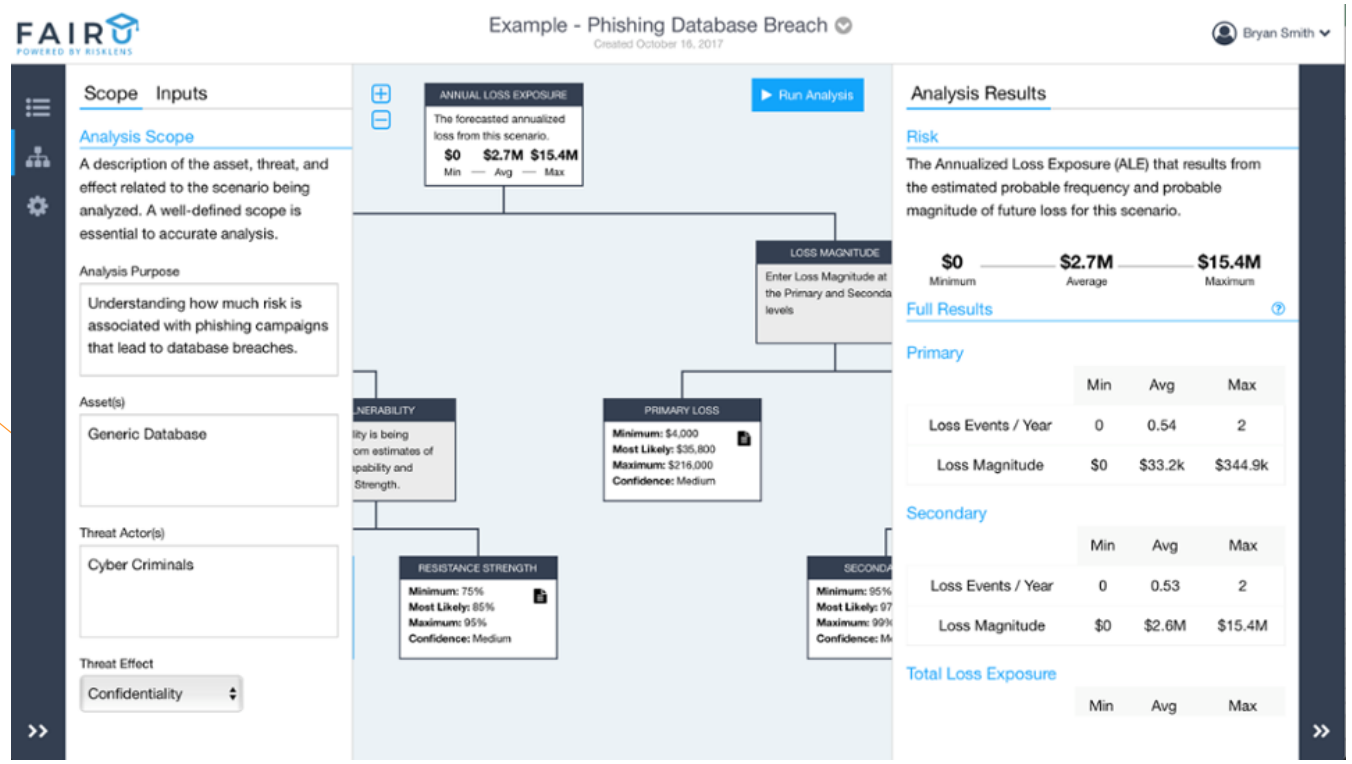
greenbox

DXC.technology

HUAWEI

FAIR-U

The Risk Analysis Training Application based on FAIR



https://www.fairinstitute.org/fair-u

FAIR-U
POWERED BY RISKLENS

1. Perform single FAIR-based risk analyses
2. Learn about the FAIR model and the different data inputs
3. Take advantage of embedded Monte Carlo simulations for your quantitative risk analysis
4. Communicate about risk in financial terms

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

FAIR Sydney and Melbourne Chapters

Melbourne, Australia

Chair: Jason Ha, Director of the Digital Trust Risk Assurance Practice at PwC

NEXT MEETING

Sydney, Australia

Chair: Denny Wan, Cyber Security Risk Expert, Security Express

NEXT MEETING

https://www.fairinstitute.org/fair-institute-chapters

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

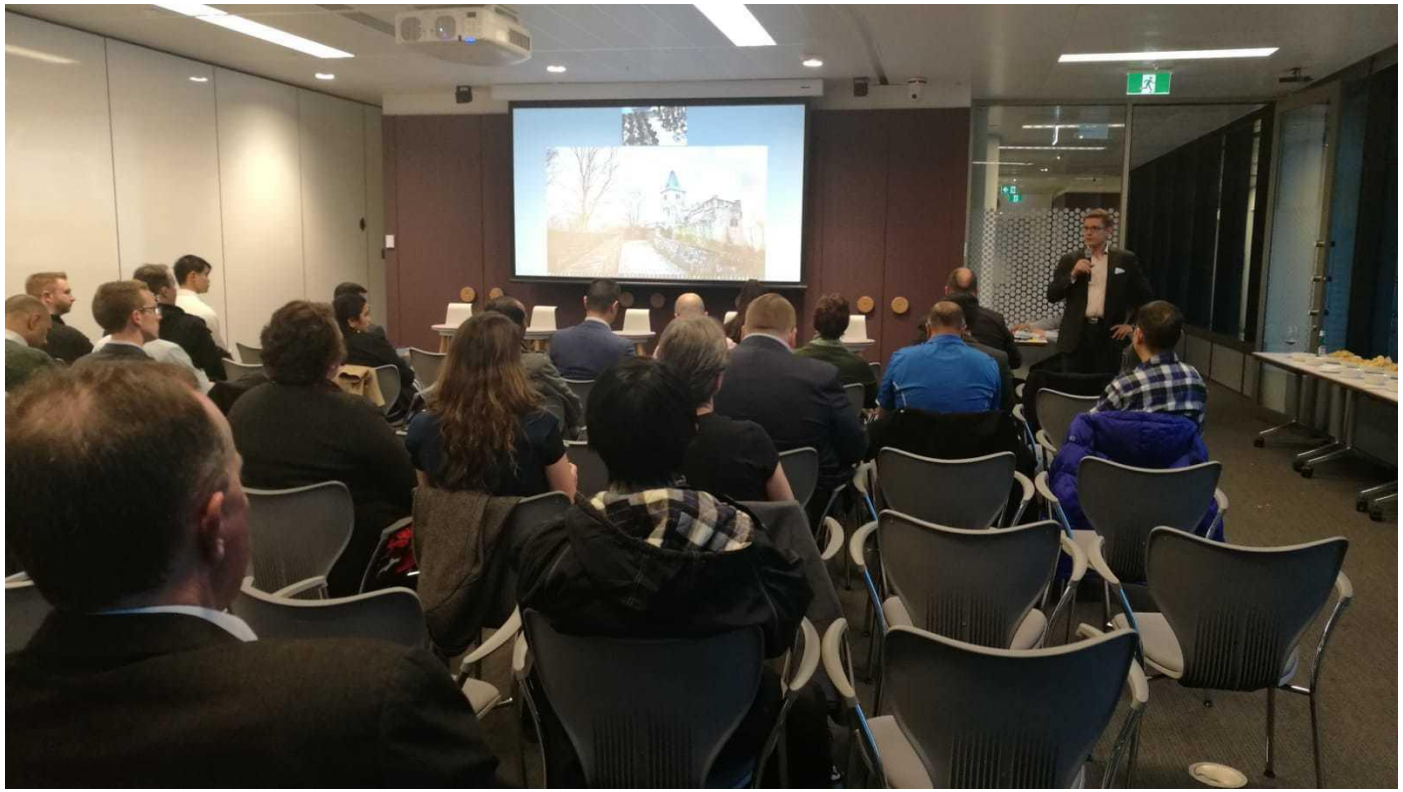
LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

FAIR Sydney Chapter meeting:
Next Thursday 28th Feb 5:30pm @ PwC Barangaroo



https://www.eventbrite.com.au/e/fair-sydney-chapter-meeting-tickets-55012065569

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI

Questions

Core

Huntsman Defence-Grade Cyber Security

tenable

dimension data

Sladen Legal

LastPass by LogMeIn

greenbox

DXC.technology

HUAWEI