Session 6B
Assuring IT Security – Keeping cyber safe

Presented by

Mark Sercombe PFIIA CIA
Principal Consultant
Technology Risk

Assuring IT Security - Keeping cyber safe

IIA Local Government Internal Audit Forum
9 November 2017

Mark Sercombe
Principal Consultant
p: +61 (0) 416 107 657
e : msercombe@technologyrisk.com.au
www.technologyrisk.com.au

Technology Risk

o

04 Emerging cyber risks

Internal audit's role 05

06 Cyber governance & reporting

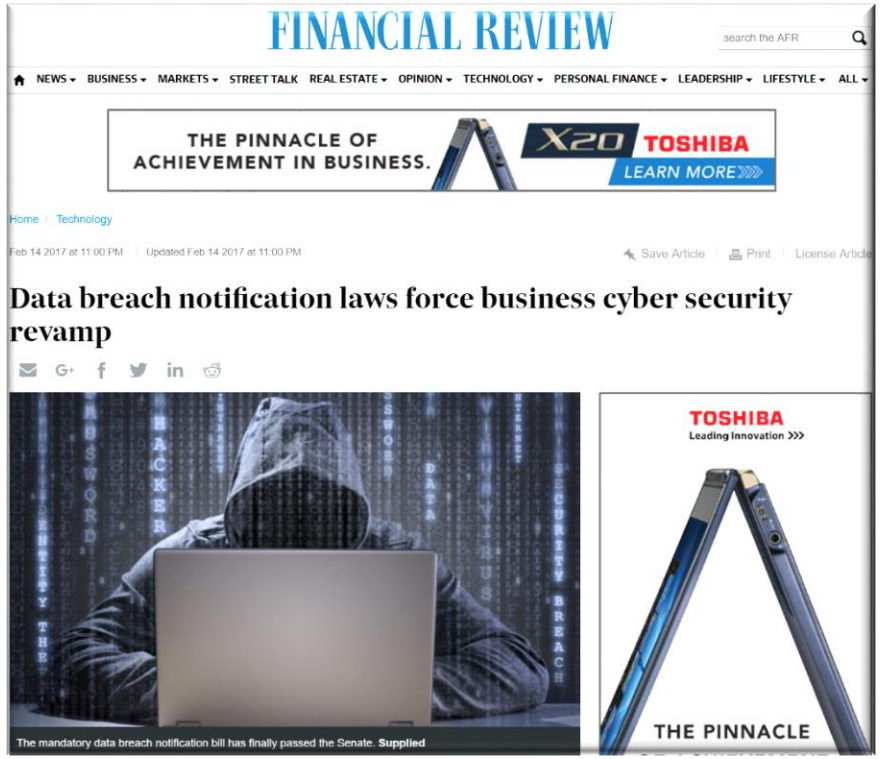
Discussion

Emerging cyber risks

- ***Now :*** **Breach Notification Scheme**
- *Soon :* The (external) auditors are coming
- *Later :* Internet of Thing(IoT)

Notifiable Data Breaches
Commonwealth Privacy Act Amendment

What : may need to '*notify any individuals Likely to be at risk of serious harm by a data breach.'*



Who : commercial 3rd parties **(NOT Local Government)**
Holding, or with access, to your Council's personal information

When : from 22 February 2018

Notifiable Data Breaches

Notifiable? : "*a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.*

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure."

•https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

Notifiable Data Breaches

'Examples…include when:

- *a device containing customers' personal information is lost or stolen*
- *a database containing personal information is hacked*
- *personal information is mistakenly provided to the wrong person"*

•https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

Notifiable Data Breaches - *serious harm?*

- Not defined but Act…*"list(s) a number of relevant matters to assessing whether serious harm is likely, including the kind of information, sensitivity of the information, the security protections in place, the type of person or people who obtained the information and the nature of the harm….."*

- *"……..notification is more likely to be required in relation to:*
  - *a targeted hack to obtain consumer password data,*
  - *rather than where an encrypted list of staff names and titles was accidentally emailed to a director of the company."*

https://www.herbertsmithfreehills.com/latest-thinking/new-mandatory-data-breach-reporting-law-passed

- Will the 'seriousness' be Council's judgement?

- More information? OAIC webinar 21 November https://t.co/7fyY791v6D

Notifiable Data Breaches?

Sites ABC

NEWS LOCATION: Sydney, NSW Change

Just In Australia World Business Sport Science Arts Analysis Fact Ch

Print Email Facebook Twitter More

Red Cross Blood Service admits to personal data breach affecting half a million donors

Updated 28 Oct 2016, 5:41pm

The personal data of 550,000 blood donors that includes information about "at-risk sexual behaviour" has been leaked from the Red Cross Blood Service in what has been described as Australia's largest security breach.

The organisation said it was told on Wednesday that a file containing donor information was placed on an "insecure computer environment" and "accessed by an unauthorised person".

The file contained the information of blood donors from between 2010 and 2016.

The data came from an online application form and included "personal details" and identifying information including names, gender, addresses and dates of birth, a Red Cross statement said.

Red Cross Blood Service chief executive Shelly Park said "due to human error" the unsecured data had been posted on a website by a contractor who maintains and develops the Red Cross website.

PHOTO: The file contained the information of blood donors from between 2010 and 2016. (ABC Adelaide: Brett Williamson)

MAP: Melbourne 3000

Key points:

- Data from blood donor registration form posted insecurely online
- Leak included identifying information and "personal details" of 550,000 donors
- All copies of the data believed to be destroyed

The Sydney Morning Herald

NEWS SITE OF THE YEAR

News Sport Business World Poli

MAY 20 2015

Telstra's Pacnet division suffers IT security breach

Show comments

SHARE TWEET MORE

Telstra's Asian telecommunications provider Pacnet data centre has been targetted in a security breach.

The breach occurred prior to Telstra taking ownership of Pacnet, and Telstra was made aware of it on finalisation of the purchase on April 16 this year.

nine.com.au News 9Honey Finance Sport TV Celebrity Fashion & Beauty Homes Diet & Fitne

9NEWS Your location: SYDNEY Change

National Local Just in World Videos Live Today Show ACA

Ad closed by Google

Stop seeing this ad Why this ad?

News / Health

More than a thousand patient records from NSW hospitals found in garbage bin

By Chris OKeefe | 11:33am Apr 21, 2017

Emerging cyber risks

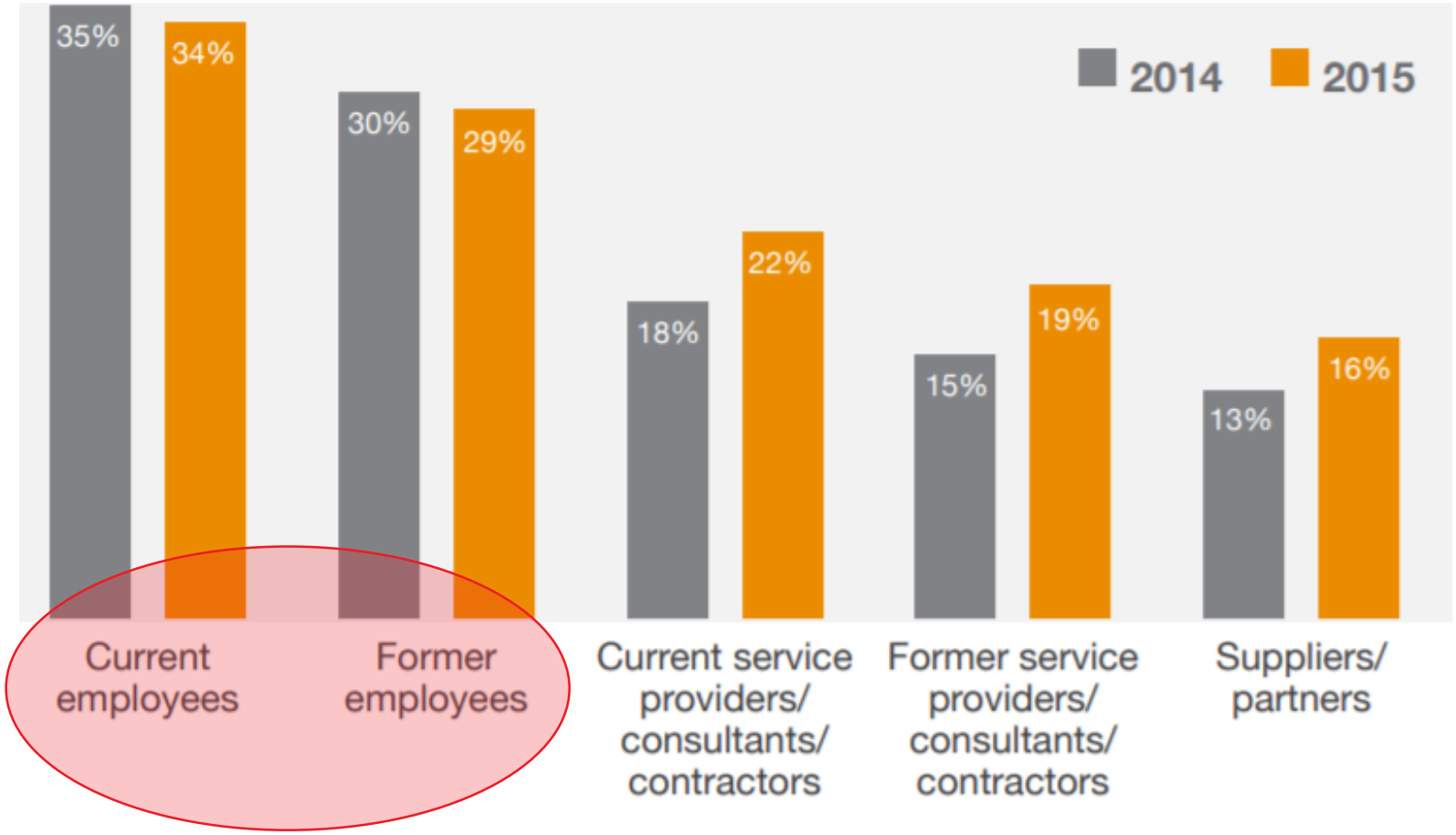
- *Now : Breach Notification Scheme*
- ***Soon : The (external) auditors are coming***
- *Later :* Internet of Thing(IoT)

'The Insider Threat'

'Employees remain the most cited source of compromise'

- Not all malicious behavior
- 'Unwittingly' compromised through:
  - loss of mobile devices
  - targeted phishing schemes

PwC 2014 Info Sec Survey Pg 14



http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

The 'Essential Eight'

To Limit the extent of incidents & recover data

- **Restrict administrative privileges**
- Patch operating systems
- Multi factor authentication
- Daily back up of important data

To Prevent Malware:

- Patch applications
- Application whitelisting
- Disable untrusted Microsoft Office macros
- User application hardening

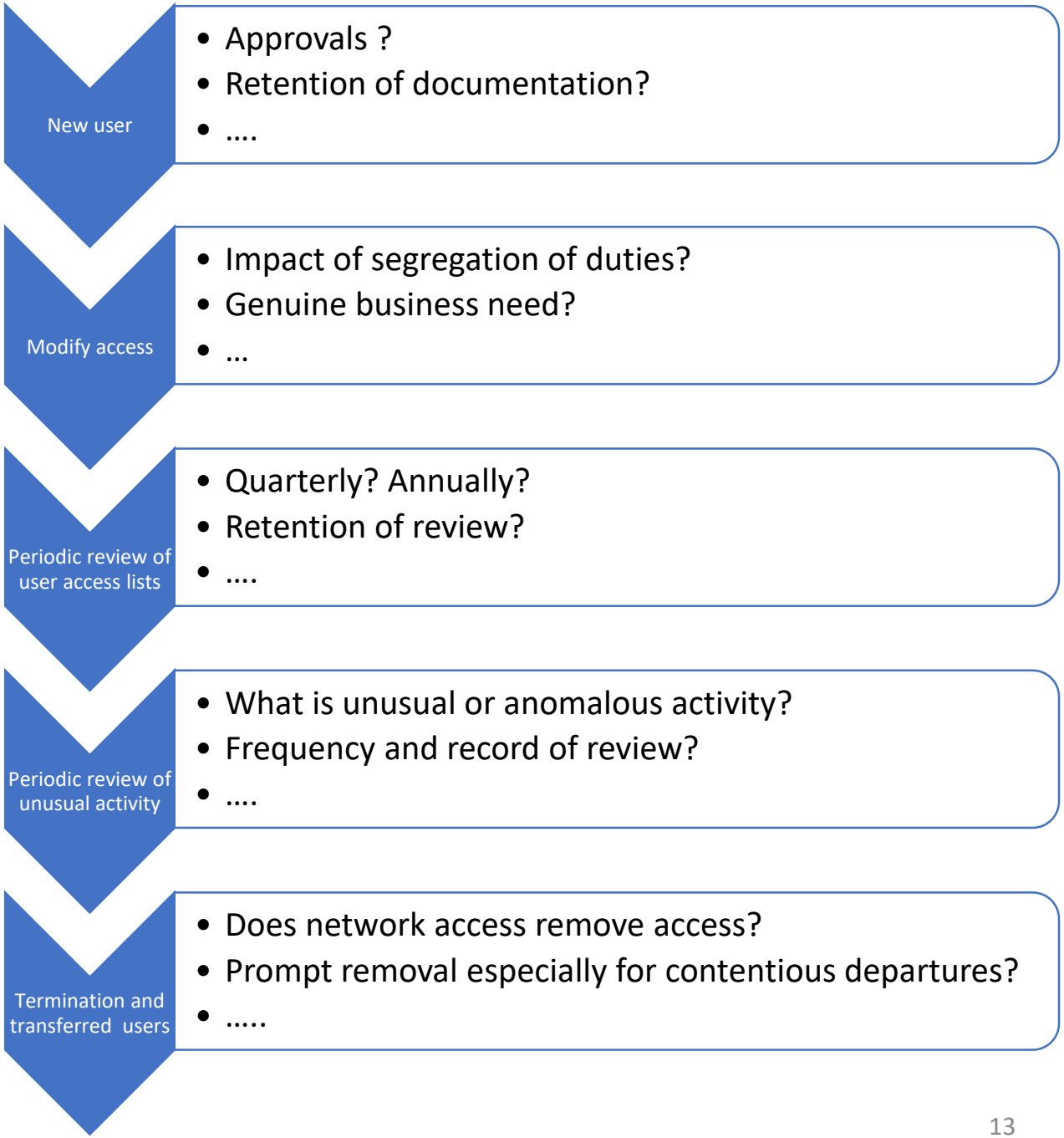
https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

Effective Preventative Controls

- A managed access life cycle

- Not an ‘event’ but a process

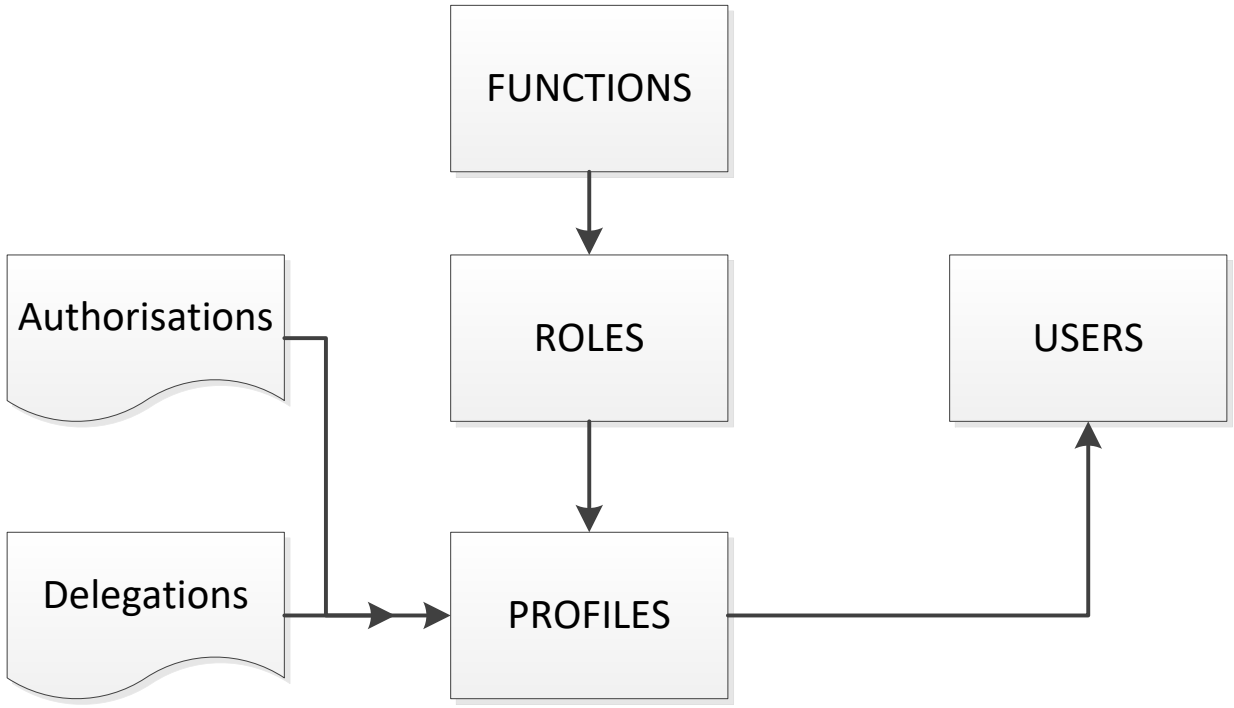
- Focus on elevated privileges



Technology One - tips and techniques include :

1. Keep it Simple…..
   - many Functions can be attached to Roles
   - …….Roles are attached to a Profile
   - …….which are attached to Users
   - additional access….may be applied using Authorisations & Delegations

2. Understand the :
   - powerful profiles
     - ‘SUPERUSER
     - ‘ALL_ROLES
   - Bypass Logins



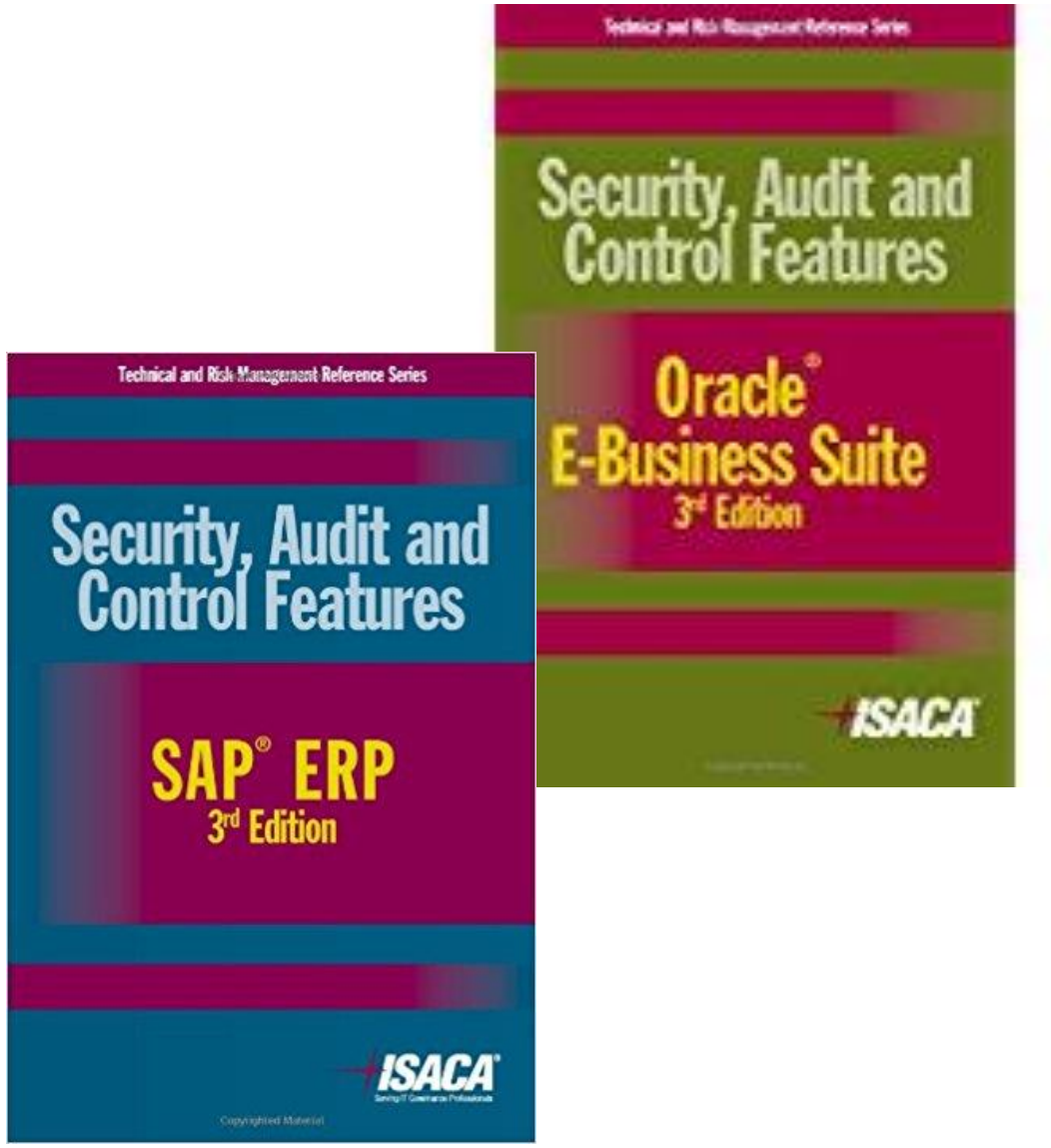
Civica Authority - tips and techniques include :

1. Powerful profile – ‘All permissions’

1. Logging of key transactions affecting financial statements :

    - Enabled?
    - Reviewed?

Other? - tips and techniques in :

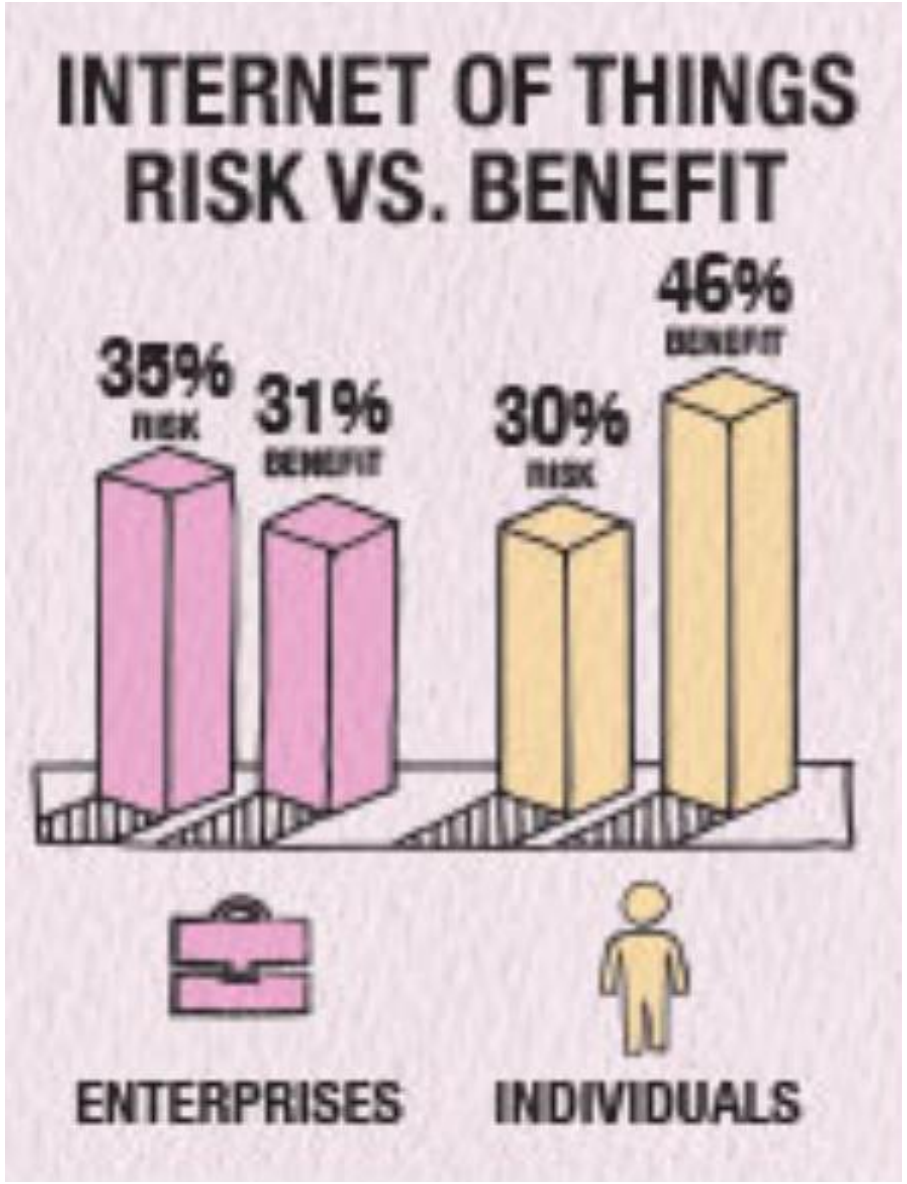


ISACA®
Trust in, and value from, information systems

https://books.google.com.au/books?id=31NYTTueqW8C&dq=sap+isaca+3rd+edition&hl=en&sa=X&ved=0ahUKEwiZ1OiOpJfXAhWCj5QKHZ1BBJoQ6AEIJjAA

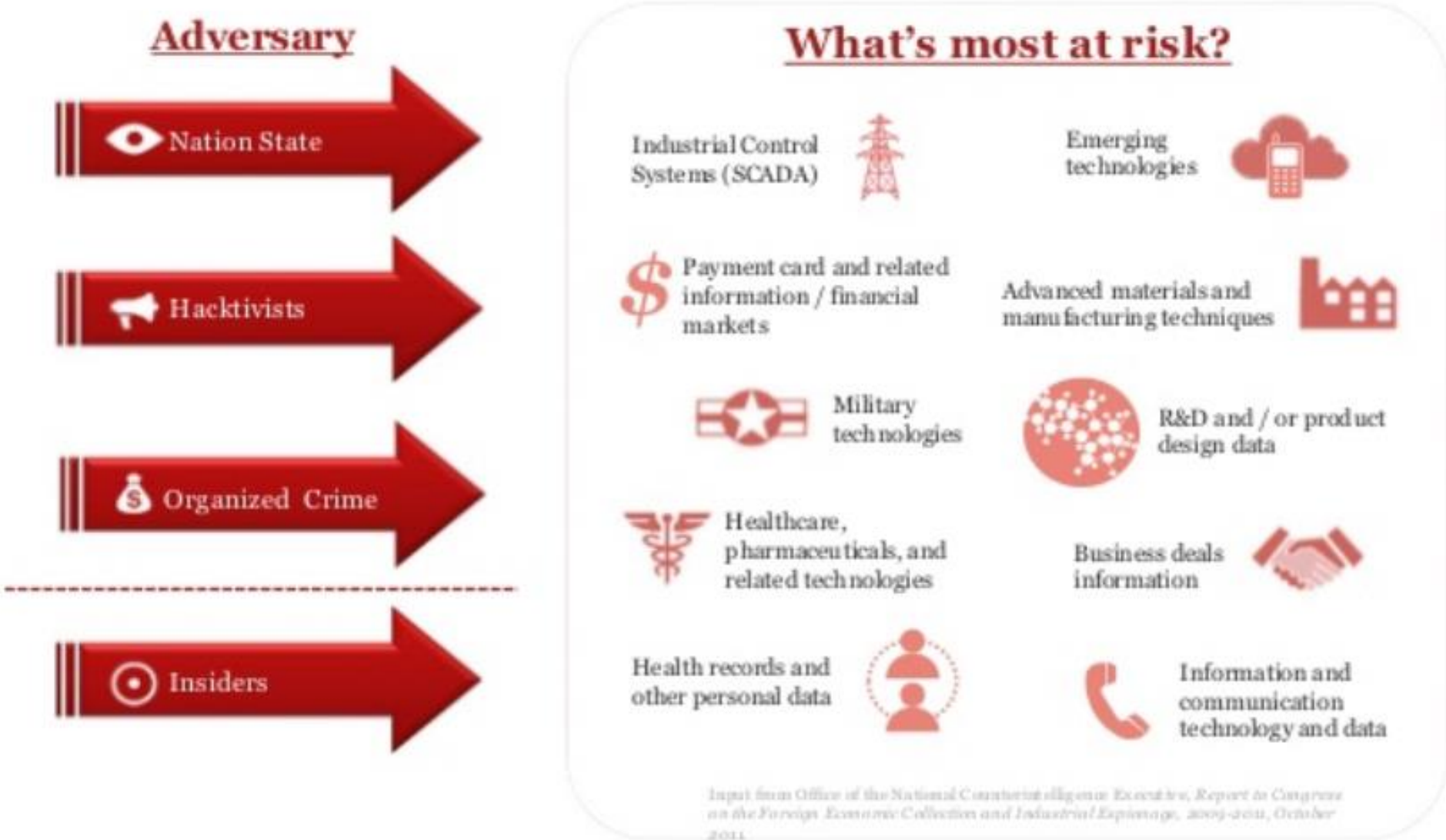
Emerging cyber risks

- *Now : Breach Notification Scheme*
- *Soon : The (external) auditors are coming*
- ***Later : Internet of Thing(IoT)***



https://www.isaca.org/SiteCollectionImages/Risk-Reward/2014/2014-Infographic-Global.jpg

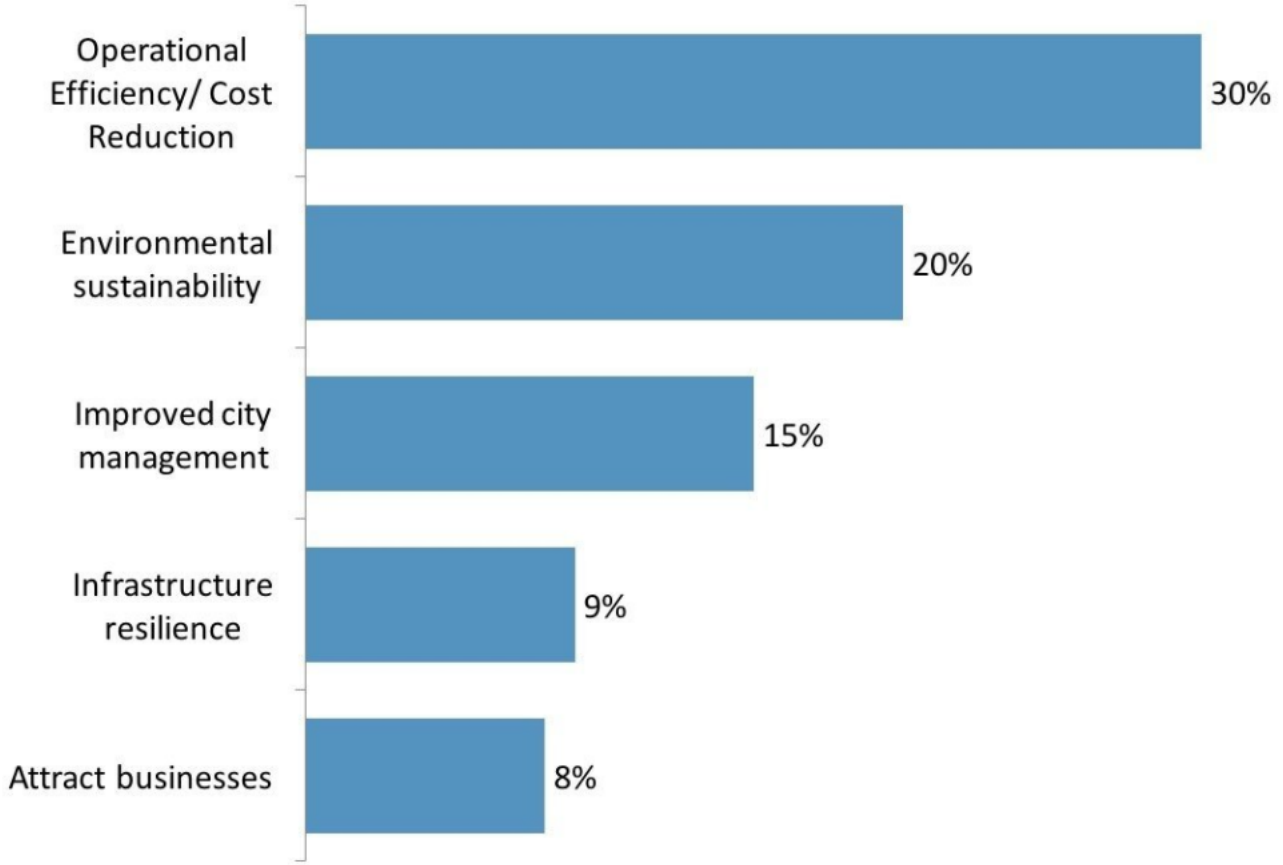
The Actors and The Information They Target



https://www.slideshare.net/EMA_SIEW/cyber-riskthreattoenergysecuritysingaporeministryofdefensev0

Top Smart City Drivers

Q: What Is The Primary Driver For Smart City Projects In The US?



BI INTELLIGENCE

Source: Black & Veatch, 2015

http://www.businessinsider.com/internet-of-things-smart-cities-2016-10/?r=AU&IR=T

itnews

Westfield ditches SMS feature over privacy issues

By Allie Coyne
Feb 3 2016
6:48AM

SECURITY IS POWERED BY SC MAGAZINE

0 Comments

Exclusive: Potential to track cars that aren't your own.

Westfield operator Scentre Group has removed the SMS notification feature of its ticketless parking service after being alerted to a potential privacy breach that could have allowed anyone to track someone else's vehicle.

Over the past few years Westfield has progressively rolled out ticketless parking to four of its 35 shopping centres around the country.

The service means vehicle license plates are scanned upon entry and exit by Park Assist technology, eschewing the need for a physical ticket.

https://www.itnews.com.au/news/westfield-ditches-sms-feature-after-privacy-concerns-413991

THE WALL STREET JOURNAL.

BUSINESS

Tornado-Siren False Alarm Shows Radio-Hacking Risk

Cyberattack in Dallas set sirens blaring by radio signal, authorities say

By *Robert McMillan*

April 12, 2017 8:08 p.m. ET

A cyberattack on the tornado-warning system in Dallas last week has highlighted the risks of hackers using radio waves rather than more common techniques of computer intrusion to breach security.

The attack set more than 100 warning sirens across the city blaring Friday night after an unknown person or group apparently gained control of the warning system. A city official said this week the hack occurred not by someone accessing city computer systems or software, but by radio. The official, Dallas city manager T.C....

Most Popular Vi

1. Metric vs. Imperial: T Measureme Mishaps
2. Inside an Immense F Operation i Kansas

https://www.wsj.com/articles/tornado-siren-false-alarm-shows-radio-hacking-risk-1492042082

Is it just our reputations at risk?

Heavily regulated industries have a higher per capita data breach resolution cost.

Per compromised record cost:

- healthcare $402
- life science industry $301
- financial services industry $264

notification

investigation

legal fees & fines

remediation

compensation

opportunity cost

http://www.hipaajournal.com/ponemon-institute-publishes-2016-cost-data-breach-study-3470/

04 Emerging cyber risks

Internal audit's role 05

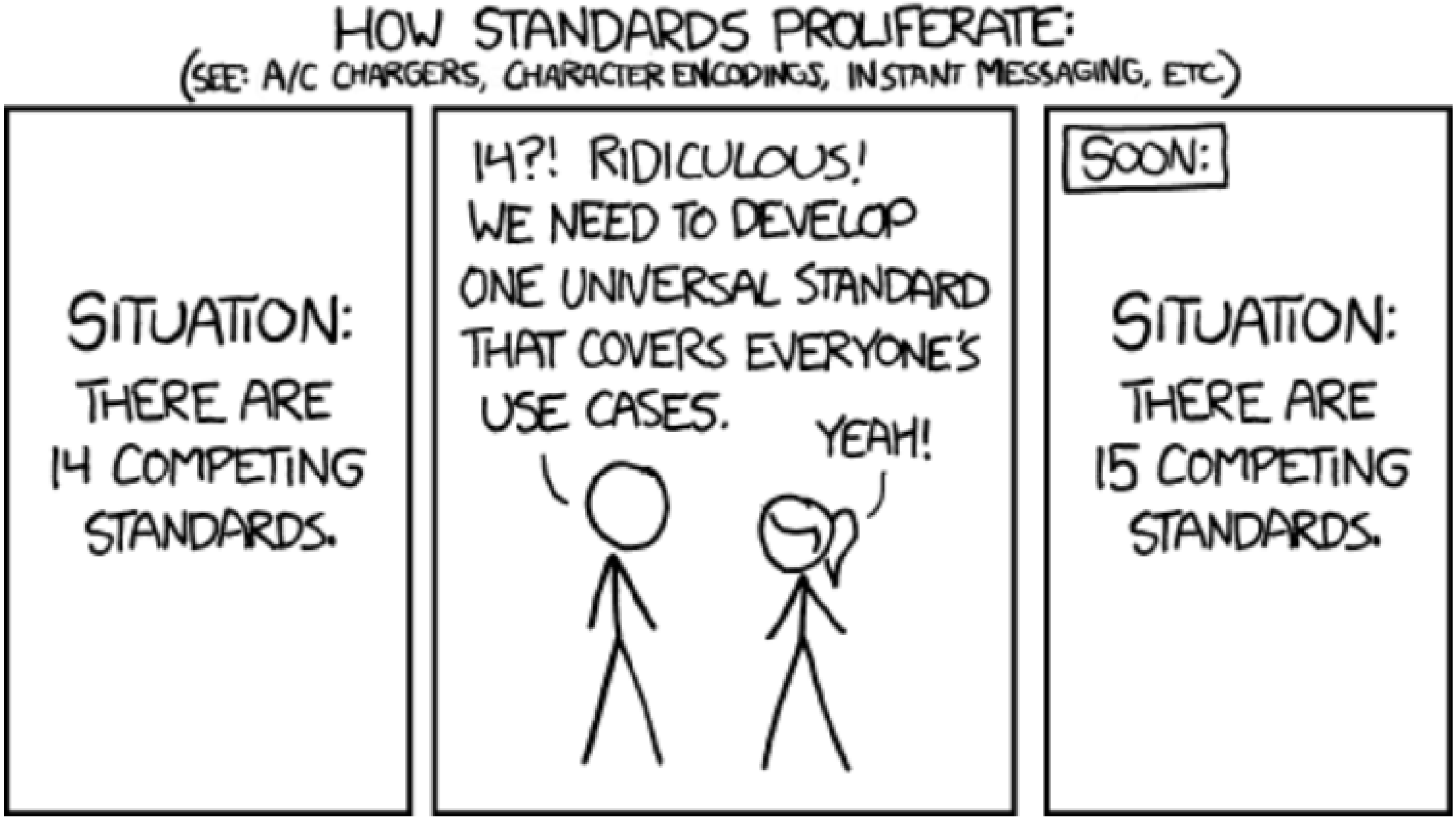
06 Cyber governance & reporting

Discussion

Internal audit's role

- High level of awareness
- Increasing expectations of assurance
- Readily available guidance
- Broad governance issues

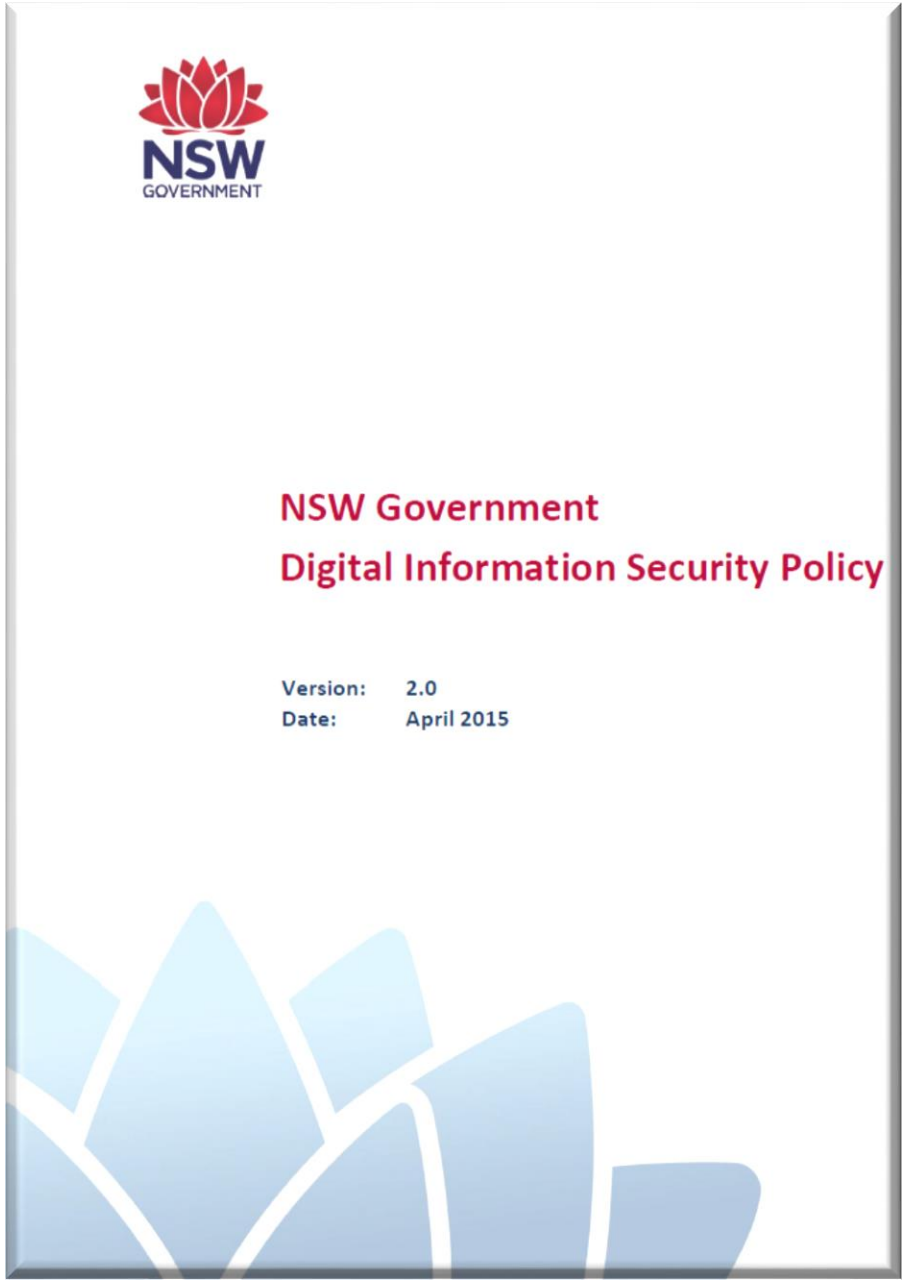
- Perception of technical skills required
- Overly focused on IT controls
- Abundance of inconsistent frameworks and guidance



https://xkcd.com/927/

A Framework to consider :

- 5 ‘Core’ Requirements
- 11 ‘Minimum Controls’



https://www.finance.nsw.gov.au/ict/priorities/managing-information-better-services/information-security

Cyber governance & reporting

1. Recognised as an evolving area
2. Consider :
   - Gap Analysis against a framework
   - Set out Management's role
   - Use Plain English

Advanced environments may include:

- Incident Reporting
- Maturity Models
- Internal Audit acts as assurer

04 Emerging cyber risks

Internal audit's role 05

06 Cyber governance & reporting

Discussion