

Master Class: Data Breach Compliance and Preparedness

Presented by: Davis Pulikottil

Contact details: National Practice Manager - GRC, Sense of Security

Level 8, 66 King Street, Sydney NSW 2000, AUSTRALIA

T : +61 (02) 9290 4451 | M : +61 (0) 490147654 | davisp@senseofsecurity.com.au

Mar-18

Compliance, Protection & Business Confidence



CONSULTANCY

A pure-play consultancy business in Information Security and Risk Management since 2002



APPROVALS

CREST approved
Supported by the Commonwealth of Australia's AG's Department
Recommended by the Department of the Prime Minister and Cabinet



INTELLECTUAL PROPERTY

Our knowledgebase, methodologies and security standards



PCI SSC ENDORSEMENT

SOS is a Qualified Security Assessor Company (QSAC) endorsed by the Payment Card Industry Security Standards Council (PCI SSC) to perform PCI DSS assessments



RESEARCH

Threat Intelligence - Vulnerability Research



CERTIFICATION

Sense of Security has been awarded ISO 27001:2013 certification



DAVIS PULIKOTTIL
Practice Manager
GRC, Sense of Security

Davis is a security professional with over 12 years of experience. He specialises in compliance, governance, risk assessment, application security solutions, penetration testing, security assurance, and identity and access management. He has extensive experience with the financial, government, healthcare, telecommunication and utilities sectors and provides valuable insight into cybersecurity risk.

Davis is an innovative and adept information security practitioner having successfully delivered information security assurance and identity and access management engagements to global clients across four different continents. He has delivered unique technical training sessions to analysts and mentored security professionals to improve skills in identifying advanced and targeted threats.

As the SOS GRC Practice Manager, Davis is involved in management of the overall practice, and is also a contributor as a senior consultant on many important client engagements.

Cyber and Digital Resilience

1

Data Breach Notifications & Compliance

2

Incident Response preparedness

3

Business & insurance risk implications

4

Protecting Identifiable Data

5

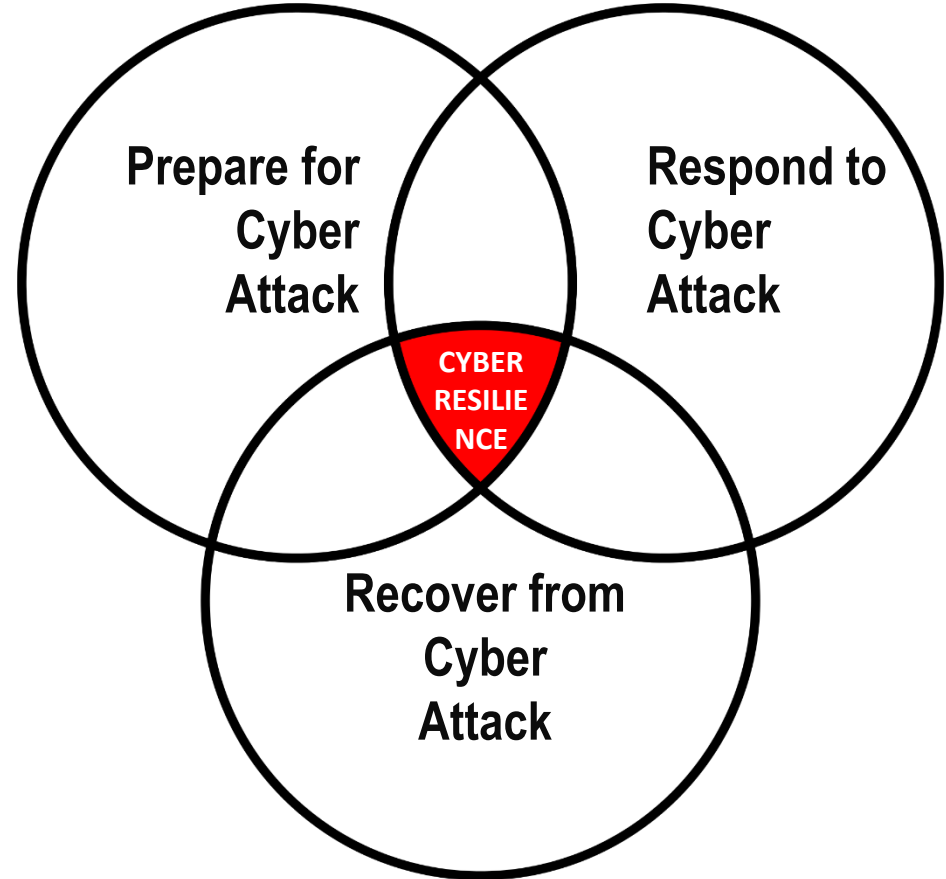
Achieving data privacy & data governance

6

Source: <http://4.bp.blogspot.com/-tM08-IUVWnc/UUqbSkvLv4I/AAAAAAAAANE/i9mEIOGyfeo/s1600/map16.png>

ASIC defines Cyber Resilience as:

**Ability of
organisation to
prepare for,
respond to and
recover from
a cyber attack.**





There is simply no such
thing as 100% cyber
security



Source: <https://i.pinimg.com/736x/f1/aa/94/f1aa949b7fd798aabafb3eab0a60dd7f--medusa-fortune.jpg>.

Source: <http://www.taggerd.su/files/files/securityseal-green-602x577.jpg>

As well as being focused on preventing cyber attacks, organisations need also have strategies in how they respond to attacks when they occur, and how they recover from attacks





Indeed, there have been a recent string of high-profile cyber-attacks against Australian and global organisations.



Source: <http://www.abs.gov.au/>. Source: <http://www.bom.gov.au/>. Source: <https://www.ashleymadison.com/>. Source: <https://www.redcross.org.au/>



One of the most costly attacks was the hack of Yahoo. Shortly after Verizon announced its US \$4.83 billion acquisition of the firm, Yahoo revealed that years earlier it had been subject to a massive cyber-attack causing the privacy of more than one billion accounts breached. This resulted in the re-opening of negotiations and ultimately Yahoo agreed to drop the purchase price on the deal by US \$350 million.

Source: <https://media.shellypalmer.com/wp-content/images/2016/02/yahoo-compressor.jpg>

- Digital economy is key to Australia's future
- Australian businesses are continually increasing their investment in digital technologies


Source: <http://alexmooremedia.com/alexander-moore-digital-media-3-key-members/>



- With the advent of the digital economy, the risks that come with a cyber-attack run through every part of an organisation
- Australia simply cannot succeed in this new digital world if our organisations are not cyber resilient



Source: <http://alexmooremedia.com/alexander-moore-digital-media-3-key-members/>

A photograph of a city street scene. On the left, there are several historic, multi-story buildings with ornate architectural details, including arched windows and decorative facades. One building has signs for "FUNCTIONS" and "POOL ROOM". In the background, a modern, tall white building with many windows is visible. To the right, a tall, thin, silver tower (the Sydney Tower Eye) rises into the sky. The street is busy with pedestrians and a white taxi is visible in the foreground. A semi-transparent dark grey box with white text is overlaid on the center of the image.

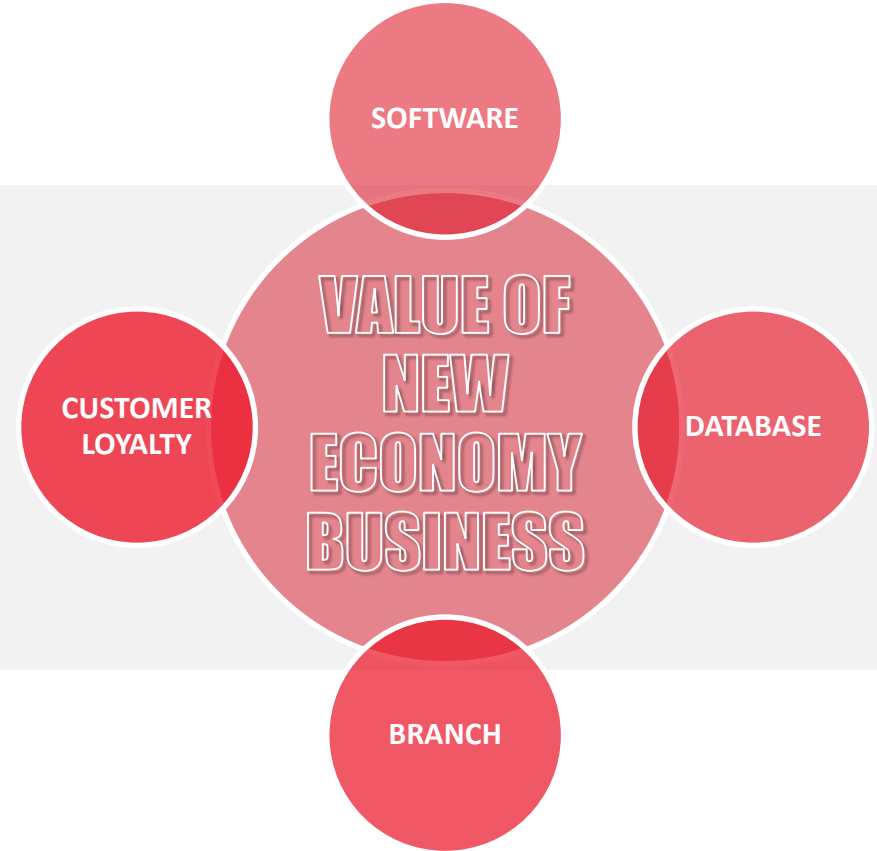
Increasingly, a business' value is tied up in its intellectual property assets, including data. This is particularly true for organisations that operate online or in the service and retail sector.

Source: <https://qph.ec.quoracdn.net/main-qimg-e6f14b193618f37b42f2b79d7d3dd605-c>



A cyber-attack can cripple a business

Source: <https://actu.epfl.ch/image/32985/652x367.jpg>

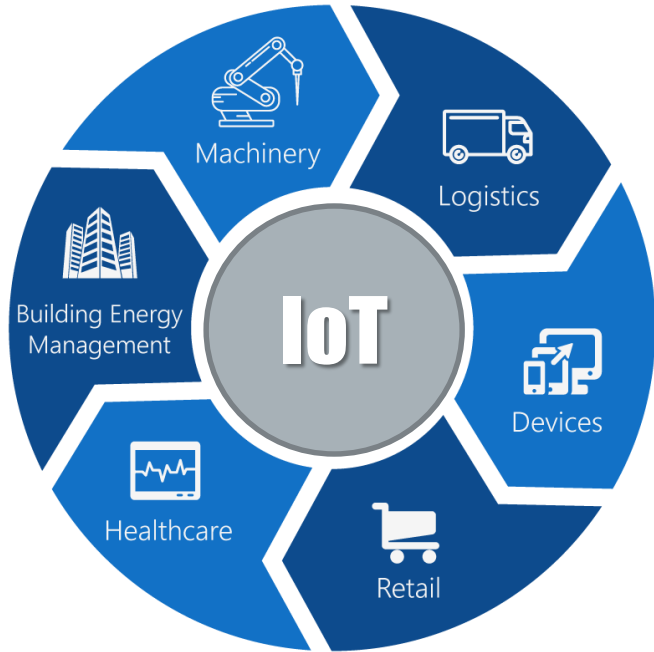




Cyber resilience is just as important for businesses with traditional models.

For example, mining and construction companies are increasingly connected to the internet as plant and machinery is switched on to the Internet of Things (IoT)

Source: <https://static01.nyt.com/images/2015/06/24/technology/24bits-mckinsey/24bits-mckinsey-blog480-v2.jpg>



IoT connected devices have the capacity to autonomously input, communicate, analyze and act upon information. While IoT technology increases productivity and control, it will also bring new challenges for businesses that have not previously had to consider cyber security as a significant risk.

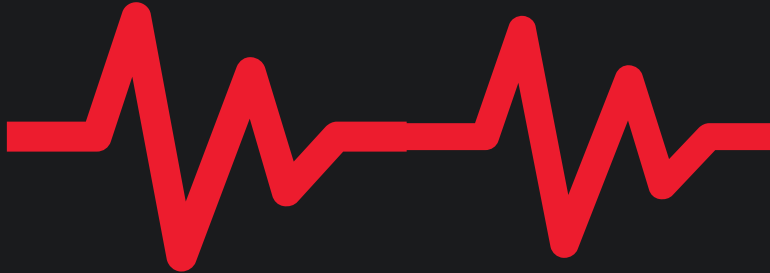
TESTCASES



Source: https://stackify.com/wp-content/uploads/2017/03/How_to_Write_Test_Cases-1-793x397.jpg



**Coffee
Break
30:00**



Cyber resilience framework should be based on recognized security standards such as ISO/IEC 27001, NIST

Best practice requires that the framework take a threat-based approach and identify which assets matter most to the business and what is most likely to be targeted

Objective of Framework

Understand effectiveness of governance processes on how business is addressing cyber risks

Awareness of the Board and senior executives on cyber security risks and opportunities

Assist in identifying areas of improvement

Benchmark security maturity against similar organisations



UNDERSTANDING THE THREAT

Board or executive leadership's awareness of organisation's cyber security threat landscape and effectiveness of organisation's cyber security strategy.



LEADERSHIP

Level of cyber security governance at the board level



CYBER RISK MANAGEMENT

How cyber risk management is positioned within the enterprise risk management framework?



AWARENESS OF HELP

Board or executive management awareness of availability of third party assistance & involvement in optimal management of cyber security threats and incidents

Based on Cyber Health Check Survey developed by Australian Securities Exchange (ASX) and Australian Securities and Investment Commission (ASIC)

Information Gathering Methods

- Interviews with members of the Board or Executive Management Team members.
- Review documentation provided supporting cyber health check survey responses.

Health Check Rating

- Health check rating is assigned to the survey questions.
- Ratings are in the range 1-5, 5 being the best response to a given question.
- Ratings are as follows:

Non Existent

Basic

Emerging

Mature

Advanced



Source: https://www.opp.com/-/media/Images/Content-images/Consultancy/PeopleAssessment_Assessment_centres.gif?la=en&h=229&w=460&hash=F750A08B42FD136C275E036E49482D3F7694DE90



Level of Cyber Incident preparedness



Level of protection of customer data

Source: <https://irishtechnews.ie/171000-irish-firms-could-be-vulnerable-to-cyber-attacks-survey/>.

Source: <http://www.wealthengine.com/resources/blogs/top-5-essential-customer-data-points>

Regulates how personal information is handled. It defines **personal information** as:

...information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Common examples:

Individual's Name

Telephone Number

Bank Account Details

Signature

Date of Birth

Commentary/Opinion

Address

Medical Records

Australian Privacy Principles (schedule 1 of the Privacy Act 1988) outline how (**APP entities**) must handle, use and manage personal information.



- Most Australian and Norfolk Island Government agencies
- All private sector and not-for-profit organisations with an annual turnover of more than \$3 million
- All private health service providers and some small businesses



Source: <https://images.campgroundsigns.com/img/lg/K/Private-Sign-K-5382.gif>

The Act also regulates the privacy component of the

- Consumer credit reporting system
- Tax file numbers
- Health and medical research.



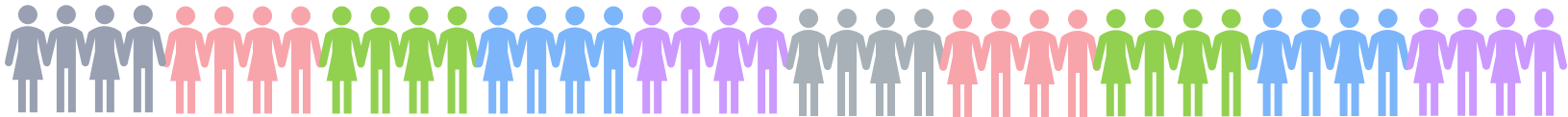
Notifiable Data Breaches scheme (under Part IIIC of the Act) establishes requirements for entities in responding to data breaches

Privacy Regulations (The Governor-General may issue regulations under s 100 of the Privacy Act 1988)

-


Commenced on 22 February 2018

- Obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm
- Notification must include recommendations about the steps they should take in response to the breach
- Australian Information Commissioner must also be notified of eligible data breaches
- Lodge their statement about an eligible data breach to the Commissioner through the Notifiable Data Breach statement form
- Agencies and organisations must be prepared to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification



Data Breaches that Require Notification

Eligible data breach arises when the following three criteria are satisfied:

- 
- A large, stylized number '3' composed of multiple concentric, multi-colored lines (red, orange, yellow, green, blue, purple) with a dashed outline. Inside the '3' is a green hexagon with a white asterisk. The background features faint, light blue and yellow curved lines.
1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity hold.
 2. This is likely to result in serious harm to one or more individuals.
 3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

Examples:

- 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

Source:

https://i0.wp.com/farm8.static.flickr.com/7233/27479939236_d6c5ac179c_o.gif?resize=640%2C480&ssl=1

Preventing serious harm with Remedial Action

- NDB scheme provides the opportunity to take positive steps to address a data breach in a timely manner and avoid the need to notify.
- If an entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity.
- For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.
- If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

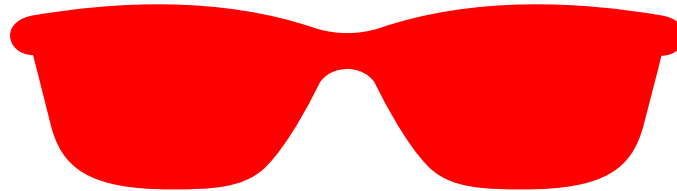


Source:

<https://www.acnc.gov.au/images/ACNC/Conflictofinterest/Stages.png>

Why the NDB Scheme is Important

- Strengthens the protections afforded to everyone's personal information
- Improves transparency in the way organisations respond to serious data breaches
- Greater community confidence that personal information is being protected
- Encourages a higher standard of personal information security across Australia
- Provides individuals with the opportunity to take steps to minimise the damage



Who Must Comply With the NDB Scheme

Agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information includes:

Australian Government Agencies

TFN recipients, among others

Credit reporting bodies

Health service providers

Business and not-for-profits organisations with an annual turnover of \$3M or more

When entities hold personal information jointly



- Data breach of one entity will also be considered data breach of others
- Both entities are generally responsible for complying with the NDB scheme
- Scheme contains a number of mechanisms to avoid duplicate obligations
- Compliance by one entity will also be taken as compliance by other entities
- Scheme leaves it up to the entities to decide which of them should do so

When is information treated as held jointly?

An entity is taken to 'hold' personal information if it has possession or control of a record that contains personal information. 'Holds' extends beyond physical possession of a record to include a record that an entity has a right or power to deal with.

Examples:



Source: <https://www.ibm.com/cloud/>. Source: <https://logo.designcrowd.com/contest.aspx?id=1083249>. Source: <https://www.visa.com.au/>.
Source: <http://sinclairlawofficepc.com/sample-page-2/mastercard-logo-400x400/>. Source: <https://www.google.com.au/>

Responding to breaches of data held jointly

Generally, both entities are responsible for complying with the NDB scheme

If one entity has assessed the suspected breach

Others are not required to assess

If no assessment is done

All may be found to breach the assessment requirements

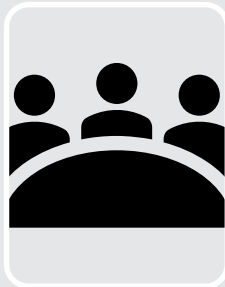
Only one entity need to inform customers and Commissioner

Others are not required to inform

If none of the entities notify

All may be found to breach the notification requirements

Allocation of responsibility for compliance



Each entity should be able to demonstrate they are meeting the requirements of the NDB scheme.



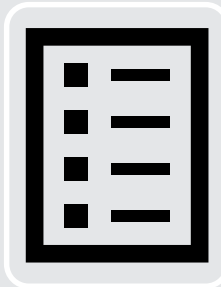
NDB scheme does not prescribe which entity should conduct an assessment



Nor which entity should notify individuals and the Commissioner



Allows entities to tailor their particular contractual and customer relationships



Entities should establish clear procedures for compliance: Communication Assessments, Responsibility for containment, remediation & notification



The entity with the most direct relationship with the individuals at risk of serious harm may be best placed to notify.



This will allow individuals to better understand the notification, and how the eligible data breach might affect them.

Source: <http://youthpoint.club/wp-content/uploads/2017/11/audit-1200x580-768x432.jpg>.

Source: <http://www.haenmar.com/wp-content/uploads/2018/01/Halal-Internal-Audit-300x214.png>.

Source: <http://www.hestanto.web.id/wp-content/uploads/2018/02/Kualitas-Audit-dan-Fee-Audit.jpg>.

Source: <https://thumbs.dreamstime.com/z/auditing-concepts-vector-auditor-table-examination-financial-report-tax-process-research-project-management-planning-97709688.jpg>

What to include in data breach statement

Entities are to prepare a statement and provide a copy to the AIC as soon as practicable
The OAIC has an online form for entities to lodge data breach statements which includes



Name and
contact
details of the
entity



Description of
the eligible data
breach



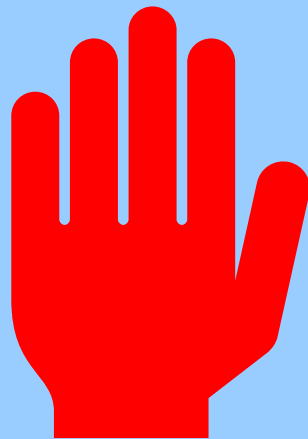
Kinds of
information
involved



Steps
recommended
that individuals at
risk of serious
harm take

When must entities assess a suspected breach?

1. Reason to suspect a serious breach: Resolve that suspicion by assessing whether an eligible data breach has occurred.
2. There has been an eligible breach: Promptly comply with the notification requirements.
3. A person with appropriate seniority is aware: An assessment should be done.
4. Should not unreasonably delay an assessment until its CEO or Board is aware of information.
5. Should have practices, procedures, and systems in place to comply with information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.



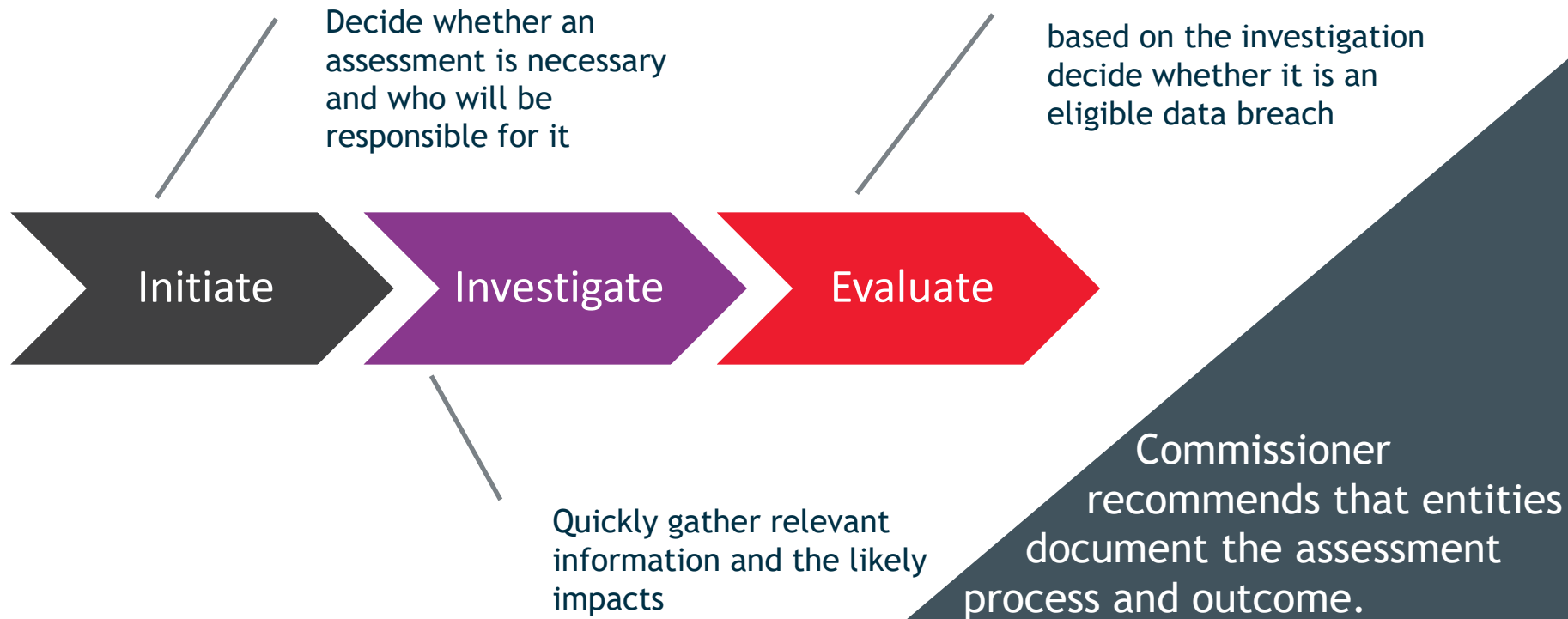
How quickly must an assessment be done?

- ✓ All reasonable steps to complete the assessment within **30 calendar days** after the day the entity became aware of the grounds that caused it to suspect an eligible data breach.
- ✓ Because the risk of serious harm to individuals often increases with time.
 - ✓ Where an entity cannot reasonably complete an assessment within 30 days, it should document this, so that it is able demonstrate:
 - that all reasonable steps have been taken to complete the assessment within 30 days
 - the reasons for the delay
 - that the assessment was reasonable and expeditious.

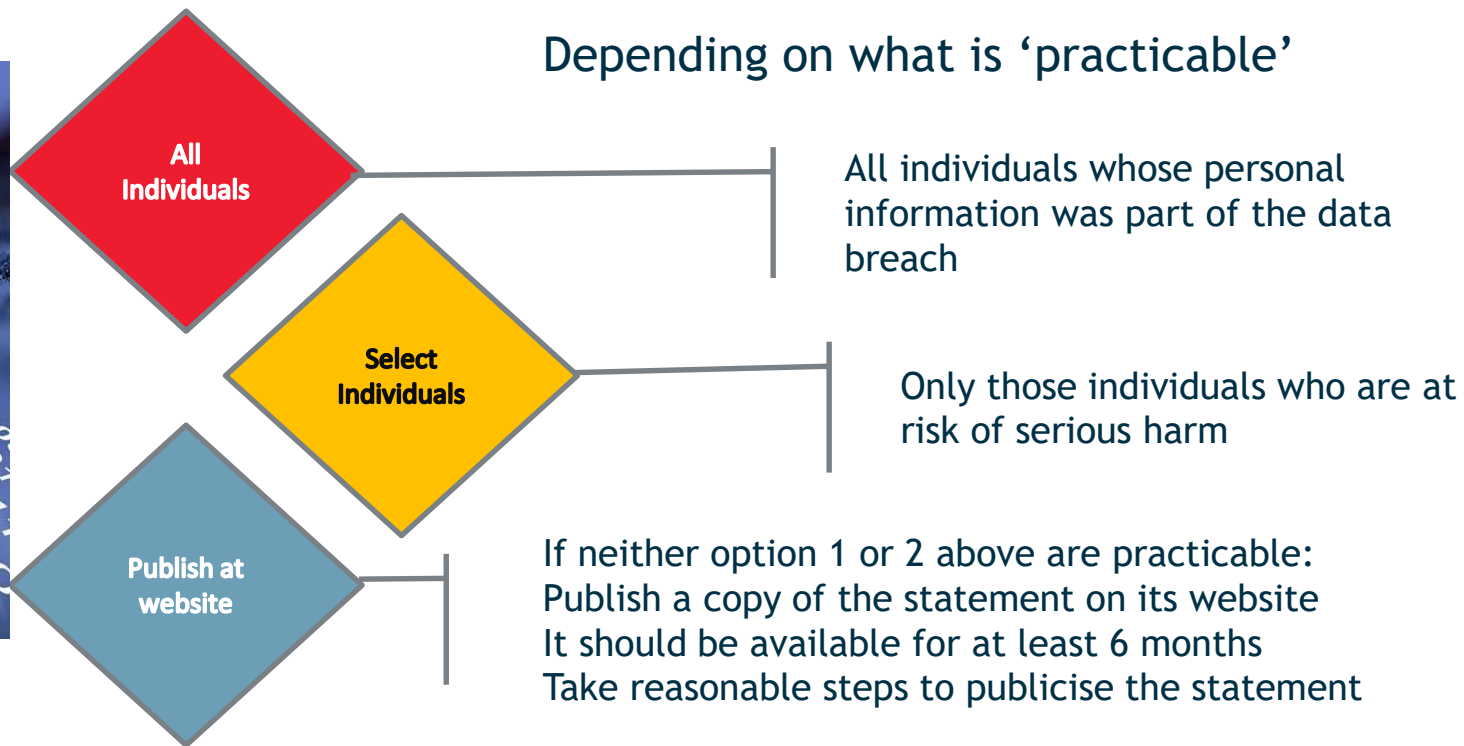
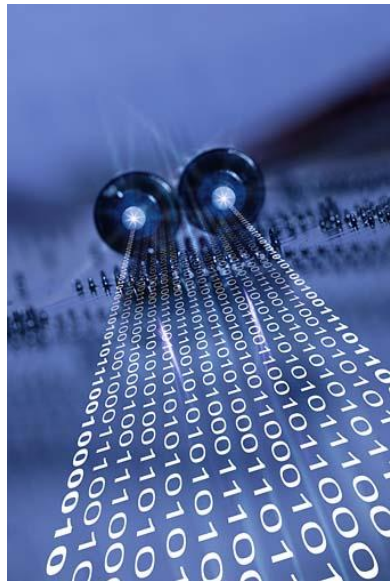


Source: <https://i1.wp.com/www.songsforyourspirit.com/wp-content/uploads/2017/09/LinkedInCalendar.jpg?zoom=2&resize=2000%2C1200>

How is an assessment done?



Notifying individuals about eligible data breach





- Receiving notifications of eligible data breaches
- Encouraging compliance with the scheme, including
 - by handling complaints,
 - conducting investigations, and
 - taking other regulatory action in response to instances of non-compliance
- Offering advice and guidance to regulated entities, and providing information to the community about the operation of the scheme.

Source: <http://gould.sydney/portfolio-item/office-of-the-australian-information-commissioner/>

Time for Lunch



TESTCASES



Source:

<https://static1.squarespace.com/static/56a5927b7086d7ad1b2b88f7/t/56ab5dfc76d99c66d1cf4d6d/1454071303188/training?format=750w>



Level of Cyber Incident
preparedness

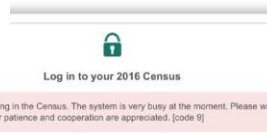
Level of protection of
customer data

Source: <https://irishtechnews.ie/171000-irish-firms-could-be-vulnerable-to-cyber-attacks-survey/>.

Source: <http://www.wealthengine.com/sites/default/files/styles/post/public/image/blog-customer-data-points.png?itok=-Td-wkzw>



Source: <https://static.scientificamerican.com/sciam/cache/file/4D644B93-81C5-4BE6-B0A49E726829967A.jpg?w=280&h=187&F733BA3B-A563-4FE0-82B86B9520339CED>



Cyber criminals are becoming successful - sophisticated, frequent



Not enough to **Defend**
but to **Mitigate**
consequences of
cyber attack



Effective Plan to be
developed to mitigate
the impact

Objective of an Incident Response Plan



Manage cybersecurity events to limit damages



Increase confidence of stakeholders



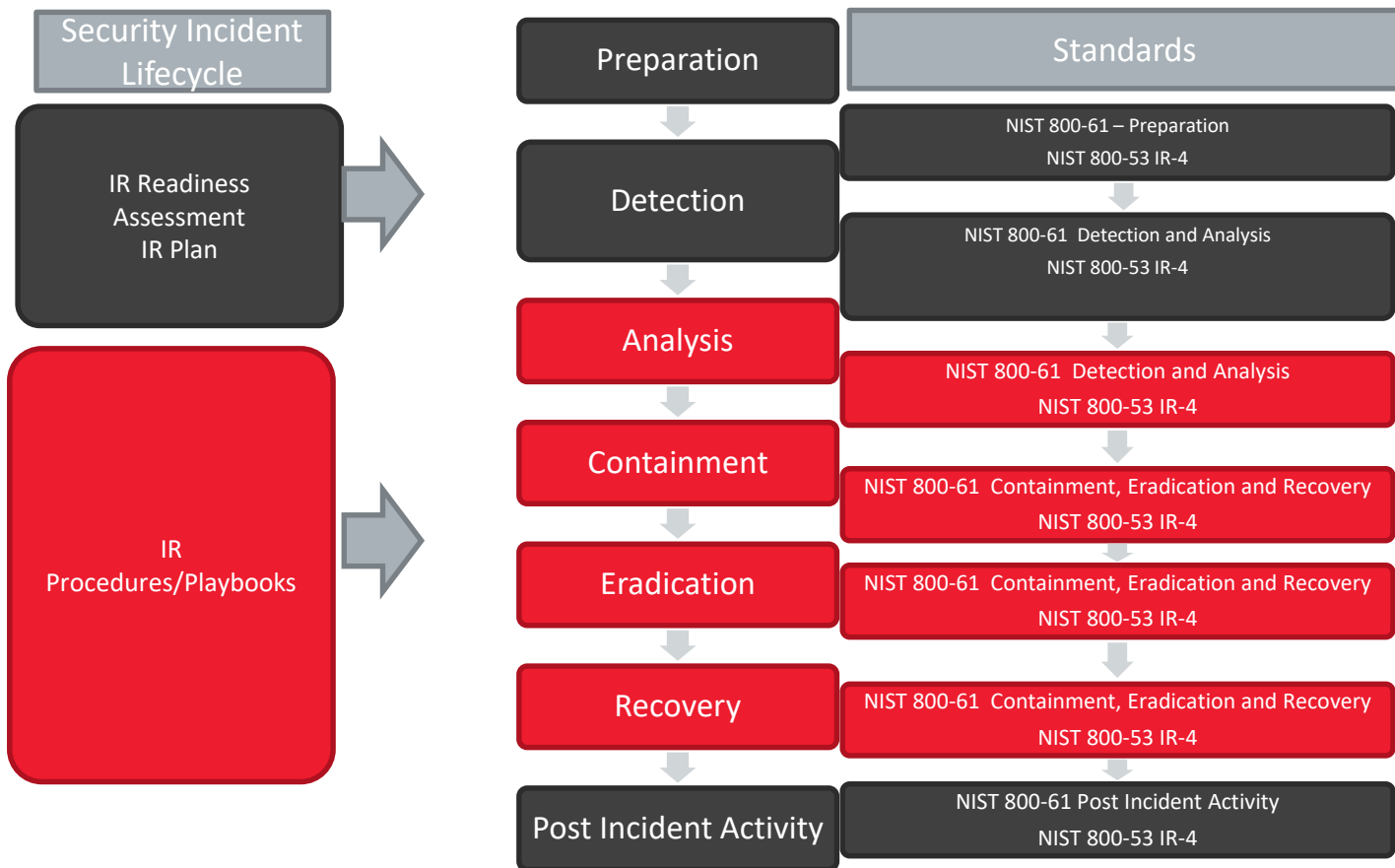
Reduce recovery time and cost

IR plans are not operationalized due to poor design or implementation

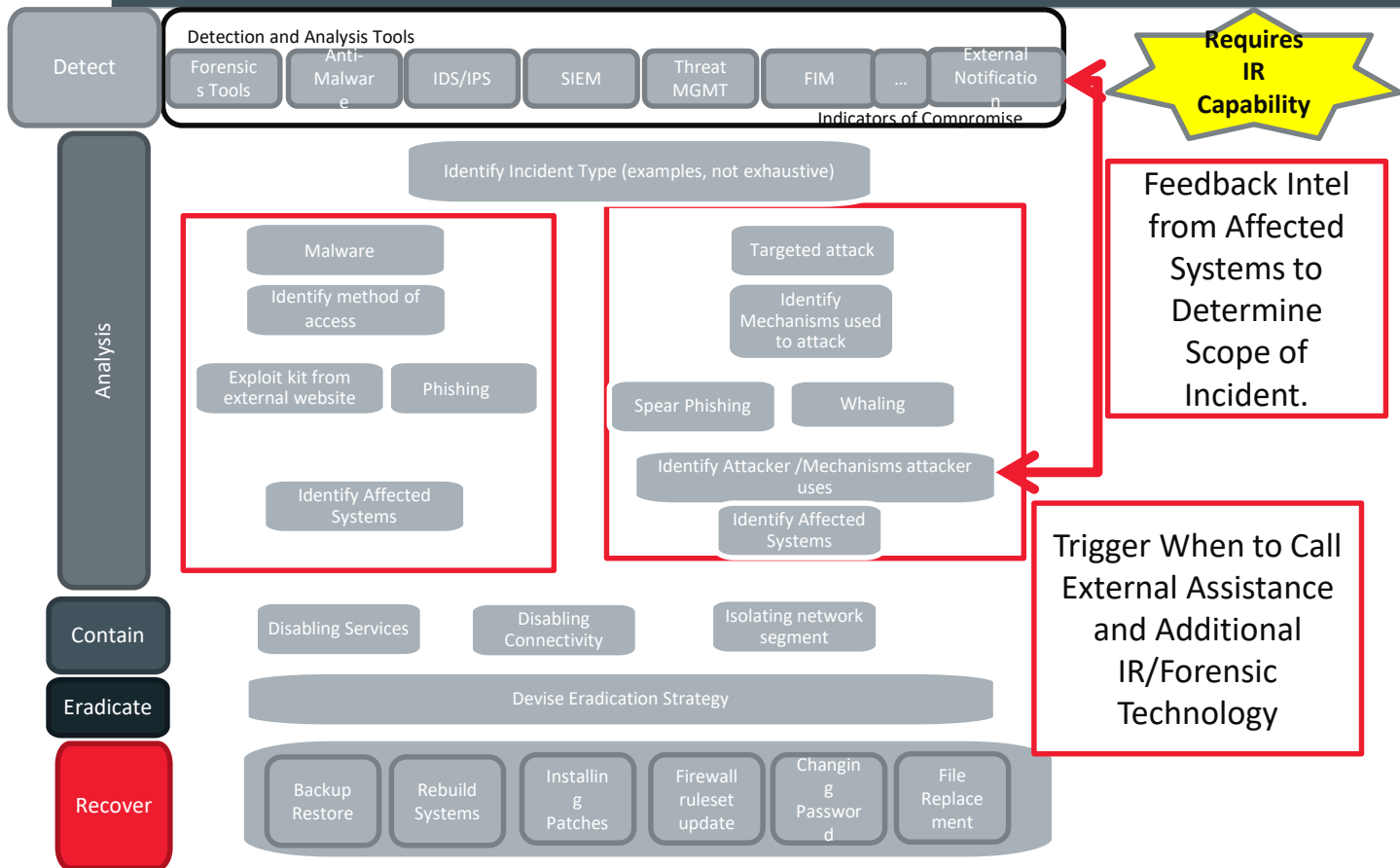
Generic and not specific for specific crisis

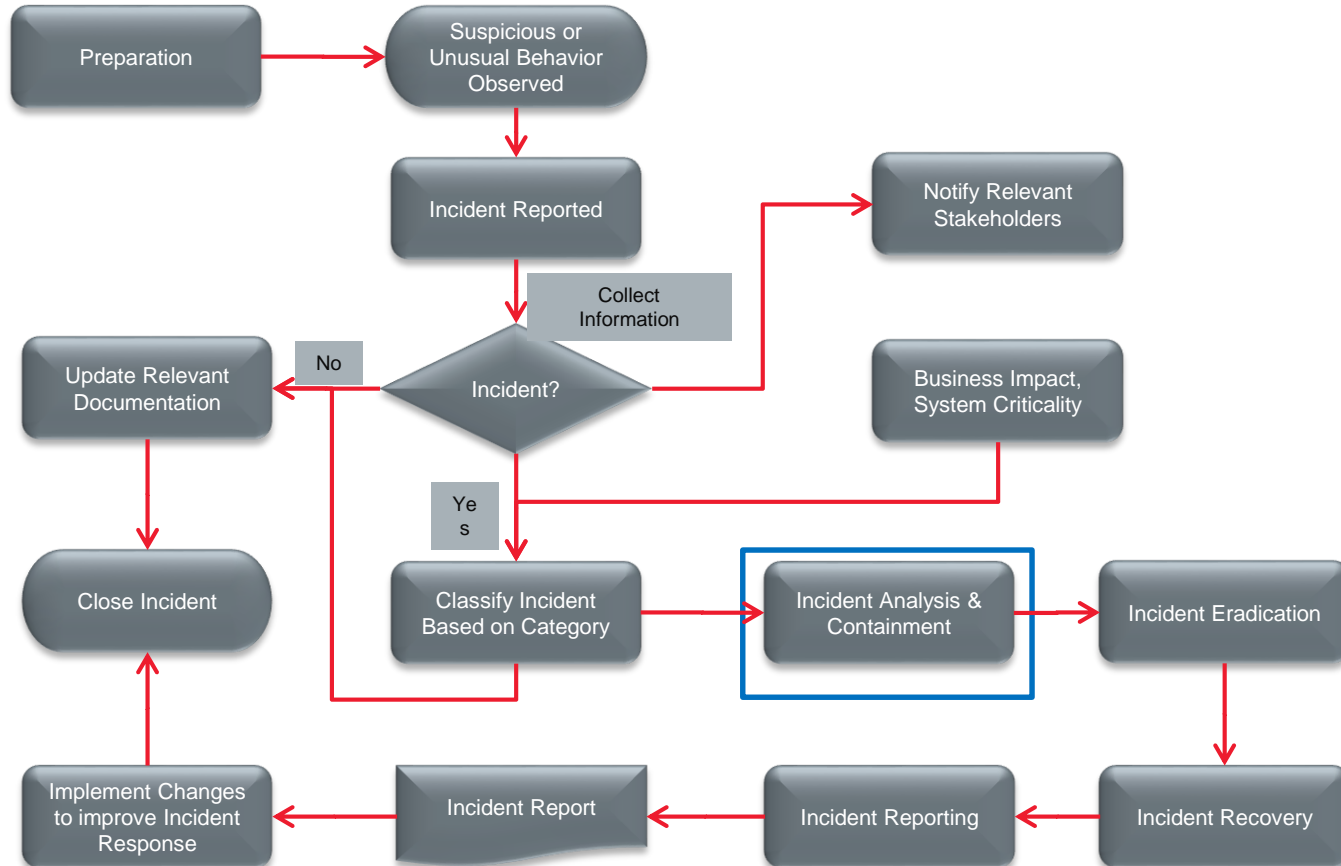
Integration across business units do not exists

Decision making is done by few people which results in single point of failure









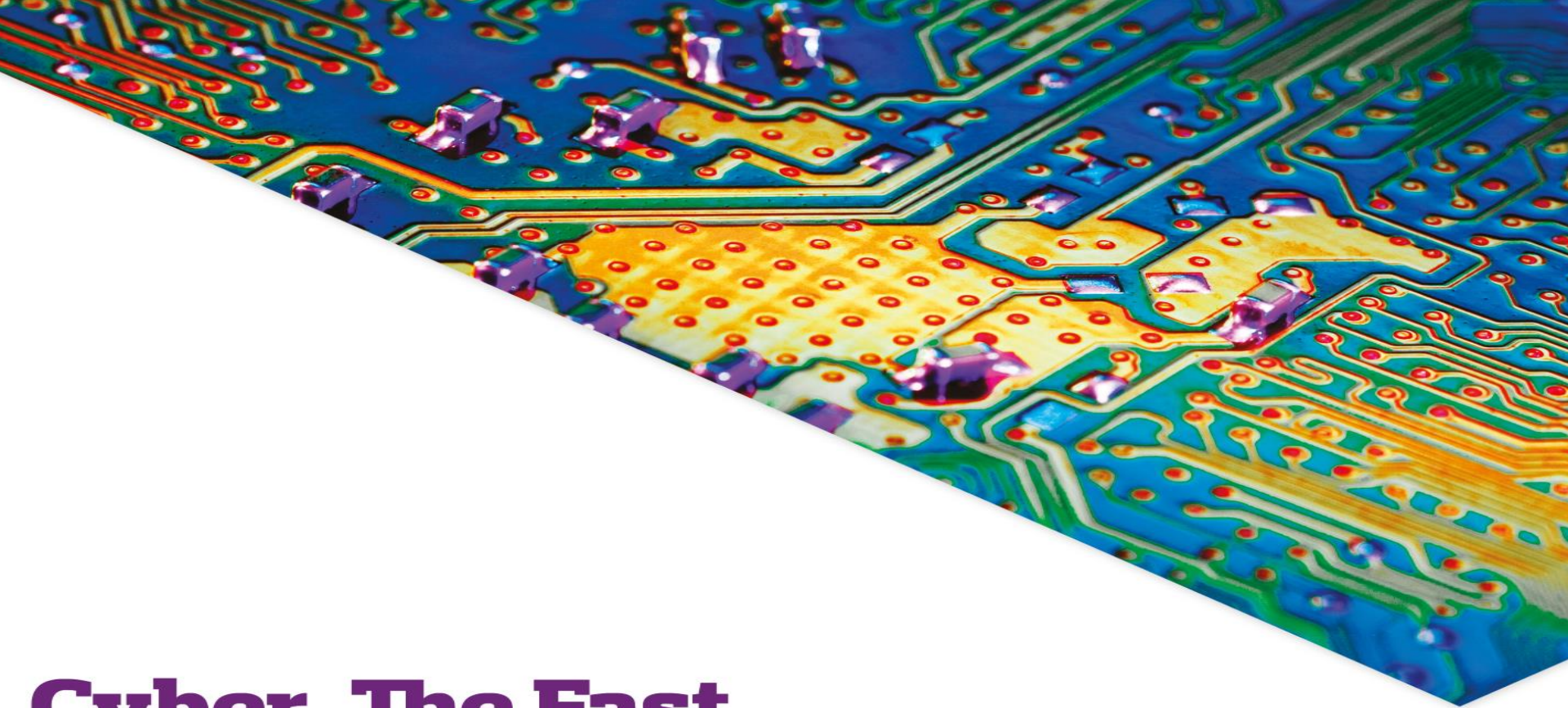


Incident Response and Data breach



Source:

[https://static.ffx.io/images/\\$zoom_1%2C\\$multiply_0.7619047619047619%2C\\$ratio_1.777778%2C\\$width_1008%2C\\$x_0%2C\\$y_61/t_crop_custom/t_sharpen%2Cq_auto%2Cf_auto/474052975e99159410c67f49acd61c85ba6df62e](https://static.ffx.io/images/$zoom_1%2C$multiply_0.7619047619047619%2C$ratio_1.777778%2C$width_1008%2C$x_0%2C$y_61/t_crop_custom/t_sharpen%2Cq_auto%2Cf_auto/474052975e99159410c67f49acd61c85ba6df62e)



Cyber, The Fast Moving Target

AON
Empower Results®

CYBER FUN FACTS

PUTTING CYBER INTO CONTEXT



THE EXTENT OF THE THREAT



“Organisations that are attacked once are three more times likely to be attacked again.”

Tim Fitzgerald, Symantec Global Chief Security Officer



Cybercrime is now the
NUMBER ONE ECONOMIC CRIME
in Australia, according to PWC.



In one of the
**BIGGEST DATA
BREACHES OF ALL TIME,**

the criminals accessed the company's point-of-sale database via their Air con system.



IN APRIL 2016
US President Barack Obama has for
the second year declared a national
emergency in cyberspace.

CYBER FUN FACTS

PUTTING CYBER INTO CONTEXT



IMPACT OF A CYBER EVENT

85%

OF AUSTRALIANS

said they would stop dealing with an organisation if their data was breached.



Cyber policies are most evolved in the healthcare, retail, and finance sectors – eight claims of over \$US75 million were paid out in those sectors.



The new mandatory data breach notification law requires organisations to report the compromise of as little as **ONE DATA RECORD.**



Many analysts believe that in mid-2016 total costs from the Target breach had exceeded

1 BILLION DOLLARS US.

2017 Cyber top 5 Exposure Trends



Cyber Liability – Top Facts

- 1** Data is one of your most important assets yet it is not covered by standard property insurance policies
- 2** Systems are critical to operating your day to day business but their downtime is not covered by standard business interruption insurance
- 3** Cybercrime is the fastest growing crime in the world and there are gaps in conventional Crime insurance
- 4** Reliance upon Cloud and other providers does not eliminate your exposure to Cyber risk
- 5** Third party data is valuable and you can be held liable and face penalties if you lose it



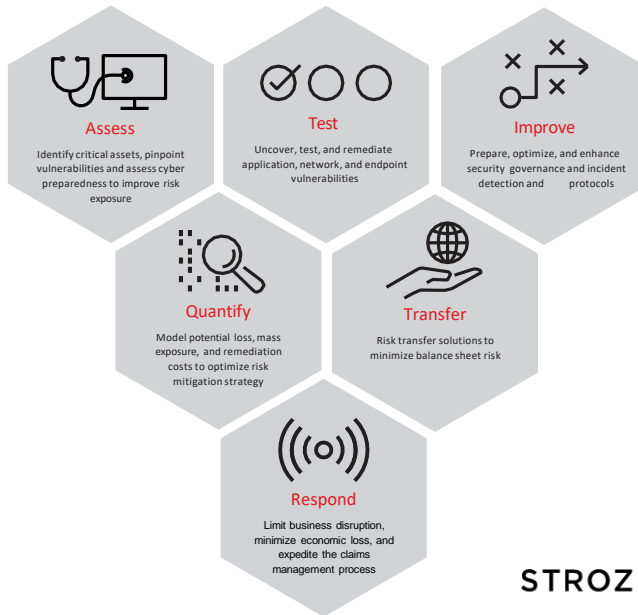
Cyber Liability – Top Facts

- 6 Complying with data breach notification and privacy laws costs time and money
- 7 Your reputation is your number one asset: how will you manage the fall out of a Cyber event?
- 8 Flexible working and BYOD increase the risk of hacking, loss and theft
- 9 Social media and Internet of Things (IOT) usage is at an all-time high
- 10 Cyber criminals are targeting organisations of all sizes and across all industries



Cyber Resilience Solutions Framework

- Identifying and protecting your critical assets by aligning your cybersecurity strategy with your corporate culture and risk tolerance.



Our Approach

We collaborate to understand both your near- and long-term business priorities, how we can add value to your organisation, and help you respond to changing market dynamics.

We jointly author a plan to define how we will work together, outline our commitments to you, and define how we will measure our success.

We seek your input on how we are doing both through informal feedback sessions and annual surveys.

We follow through on our plan, executing with excellence and tracking outcomes.

STROZ FRIEDBERG
an Aon company

Cyber Insurance: setting the scene

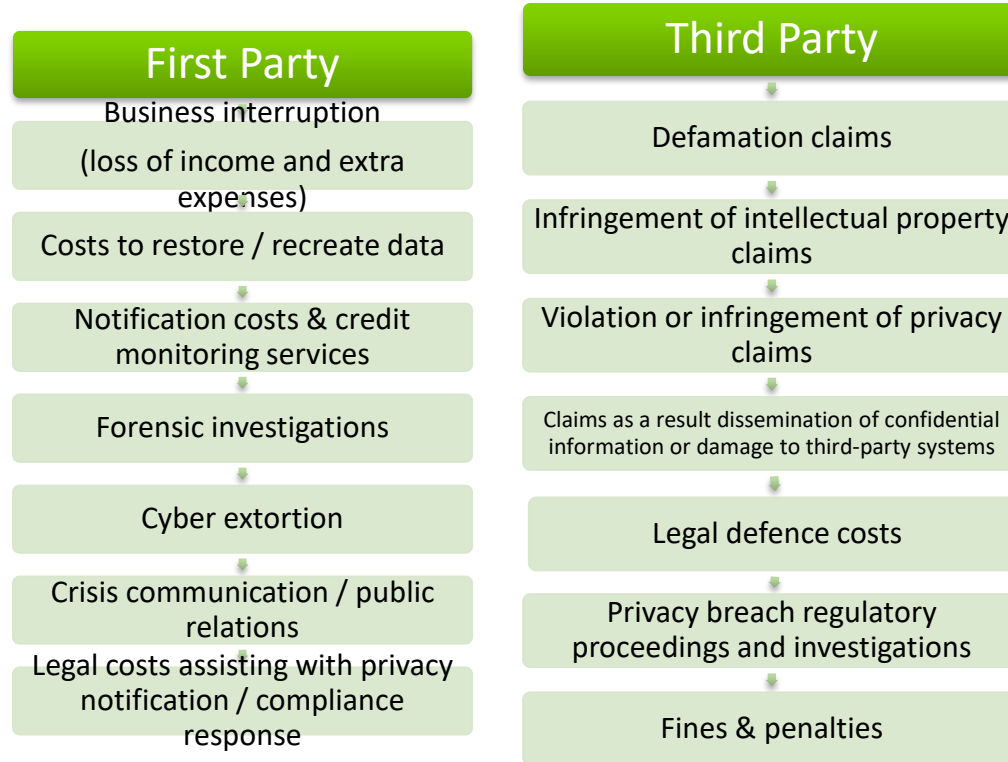


- **GWP** of circa. \$60m
- Substantial **growth** in the number of policyholders
- Underwriting **appetite mixed** e.g. Education / Govt. / Financial Institutions / Healthcare / On-Line Retail
- Circa. **\$100m of capacity** without off-shore support
- **Bifurcated market**: 1) SME (commoditised) and 2) “Corporates” / “more complex risks”
- **<5% of companies buy cyber insurance**

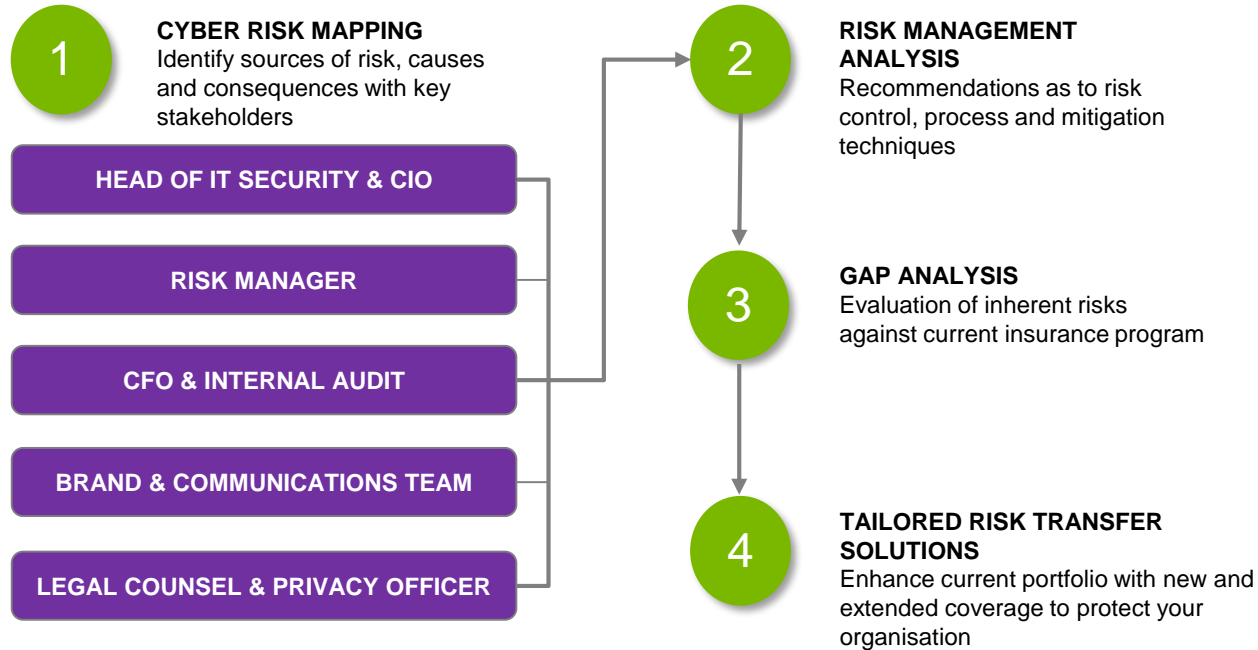


- **GWP** of circa. US\$4 billion (PWC estimate US\$5.6 billion – US only - by 2018)
- **Split**: North America 88%, 7% EMEA, 4% APAC & 1% LATAM
- **Global capacity** circa. US\$1b+ (direct)
- **Aon-sponsored Ponemon Institute study**:
 - >2000 respondents, 37 countries
 - Organisations buy insurance to cover just over half (51%) of the MPL of Tangible Property risks but only 12% of the probable maximum loss of Information Assets = **underinsurance**
- **>45% of companies buy cyber insurance**

What does a cyber policy **typically** cover?



Cyber risk analysis: what are your key vulnerabilities?



Privacy Act February 2018 – Mandatory data breach notification

- Organisations are required, as of the 22nd February 2017 to notify the OAIC (Privacy Commissioner) and those affected by any data loss/breach
- This is within 30 days after the entity has become aware that there are reasonable grounds to believe that there has been an eligible data breach
- The information that must be included in the notification:
 - the identity and contact details of the entity
 - a description of the serious data breach
 - the kinds of information concerned
 - recommendations about the steps that individuals should take in response to the serious data breach
- Minimum threshold for eligibility under the Privacy Act is AUD 3 million annual revenue (with certain exceptions, e.g. healthcare)
- Fines are decided case-by-case but maximum is 2.1 million / breach!



The New Data Breach Notification Laws



Unauthorised
access or
disclosure of
personal
information held
by an entity



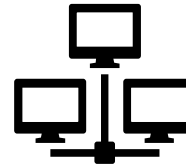
Serious harm to
individuals



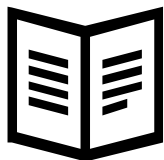
Notification to OAIC
and affected
individuals



Containment of
breach



Review of systems
and processes



Updated fact
sheets

Areas of updated guidance

- ✓ Identifying eligible data breaches
- ✓ Information held jointly
- ✓ Notification
- ✓ Eligible data breach statements
- ✓ OAIC role in NDB scheme



What entities are covered?

APP Entities who have obligations under the Privacy Act including:



**Federal
Government
agencies**



**Businesses and NFP
organisations with
annual turnover
>\$3m**



**Certain other
organisations**

- Private sector health service providers
- Credit reporting bodies
- Credit providers
- Entities that trade in personal information
- TFN Recipients



Powers of the Office of the Australia Information Commissioner





Litigation Risk



- **Class Actions**
- **Interest from plaintiff law firms following US experience**



- **D&O Risks**
- **Oversight from the board in relation to compliance**



Useful Resources

- *Privacy Amendment (Notifiable Data Breaches) Act 2017*: <https://www.legislation.gov.au/Details/C2017A00012>
- OAIC Notifiable Data Breaches Scheme website: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
- Data breach response plan: <https://www.oaic.gov.au/about-us/corporate-information/key-documents/data-breach-response-plan>
- Entities covered by the NDB Scheme: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/entities-covered-by-the-ndb-scheme>
- Assessing a suspected data breach: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach>
- OAIC's role in the NDB Scheme: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/australian-information-commissioner-s-role-in-the-ndb-scheme>
- Notifying individuals about an eligible data breach: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach>

New versions of old threats – WannaCry, Adylkuzz & NotPetya

- Ransomware and digital currency mining attached to a self-propagating worm
- Does not require human intervention/assistance to infect vulnerable systems
- Massive attack footprint, 300k+ WannaCry and reputed 500k+ Adylkuzz, that we know about
- The exploit used to spread the worm was developed buy the NSA for surveillance and stolen by a hacking Group called the Shadow Brokers
- There are reputedly 149 tools from the NSA hoard that are for sale on the dark web
- Security researchers anticipate that there will be many more and varied cyber incidents (e.g. IoT, IIoT) on the way.
- Very high vigilance is suggested, especially around patch management
- NotPetya – “Destruction of Service”

<http://aon.com.au/cyber>



OAIC Guide - Data breach preparation & response



“Your actions in the first 24 hours after discovering a data breach are often critical to the success of your response...”



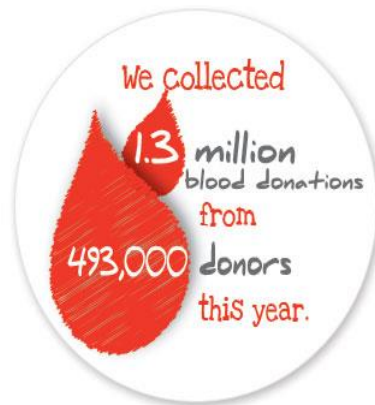
“You should create and test your plan before a data breach occurs...”

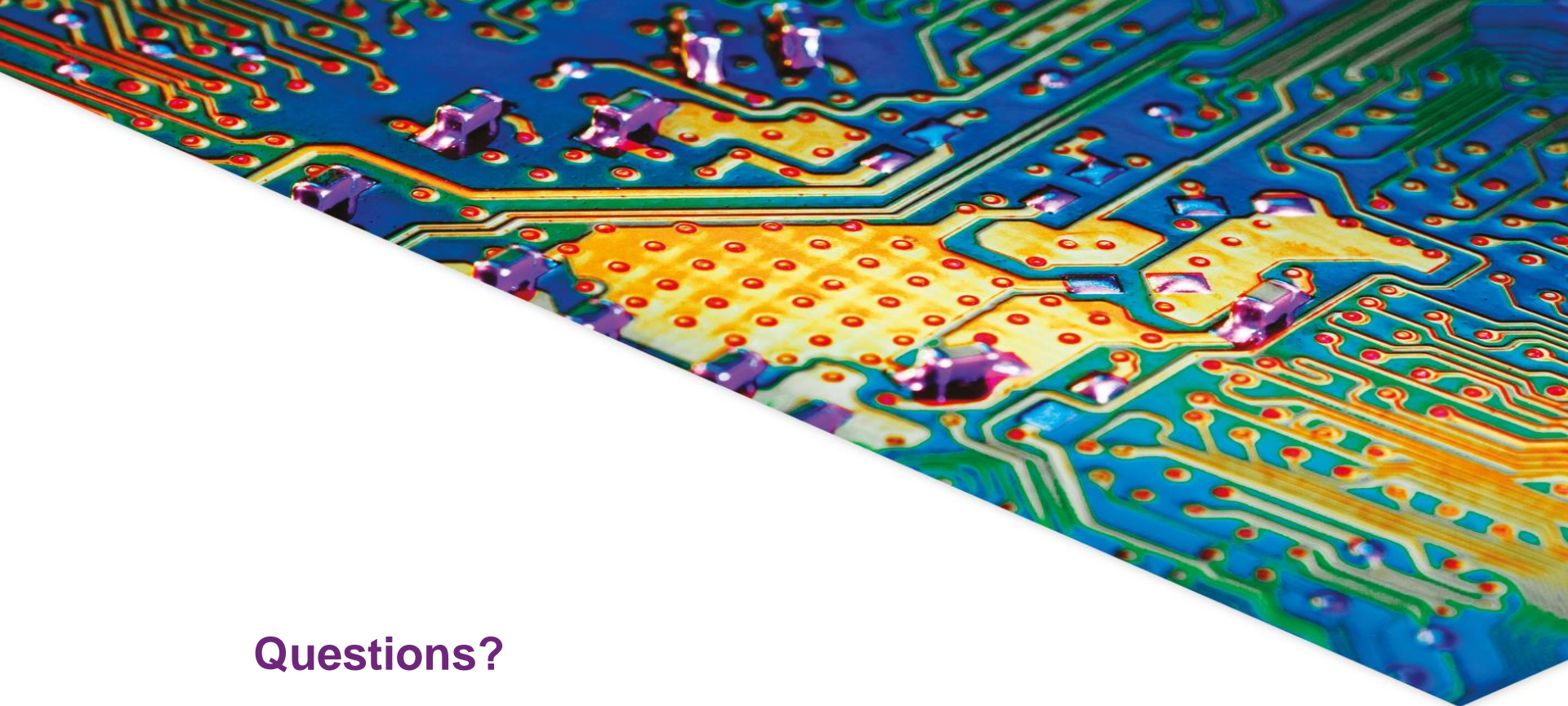


“Response team membership: ensure that the relevant staff, roles and responsibilities are identified and documented...”

Case Studies – Red Cross Blood Service – Well Handled

- Largest Australian potential data breach ever recorded
- >550,000 personal data records - >2% of Australian population
- Records were obtained from a vulnerable third party web server where the last 6 years of online applications were stored
- The ARCBS had an incident response plan linked to cyber insurance
- General consensus is the incident was handled exceptionally well
- A solid & tested incident response plan is the only way to reduce the reputational damage that can be caused by a cyber incident





Questions?



Source: <http://timothykurek.com/wp-content/uploads/2017/10/automatic-deductions-for-meal-breaks-and-the-law-what-you-need-on-images-for-lunch-break.jpg>

Increased cost of non compliance

Everchanging laws

Diversified sources

Growing saturation of technology



Reduced boundaries

Continuous innovation – cloud, IOT

Immature processes

Corner cutting to meet speed targets

Inadequate tools

Failure to upgrade technology

Unaware users

Lack of training



Data breach on product or services may be perceived by customers as not being secure. Users and customer may stop using the product or services



Inability to protect the intellectual property rights could reduce the value of the product, service and the brand



Reputational damage due to privacy concern related to the technology.

Source: <https://blog.ipleaders.in/wp-content/uploads/2016/09/metal-plating-effect-patented-696x696.jpg>.

Source: <https://www.negocio.me/img-contenido/img-789/comu.jpg>

CLASSIFICATION

Prevention

Encryption

AWARENESS

ACCESS

log in

MALWARE

Firewall



Source:
<https://i1.wp.com/www.fryborg.com/fryborg/wp-content/uploads/2014/08/hands.png?w=480>

Audited to detect shadow data and shadow IT

Scan all files that are uploaded and downloaded from the cloud

Content inspection of data in cloud apps

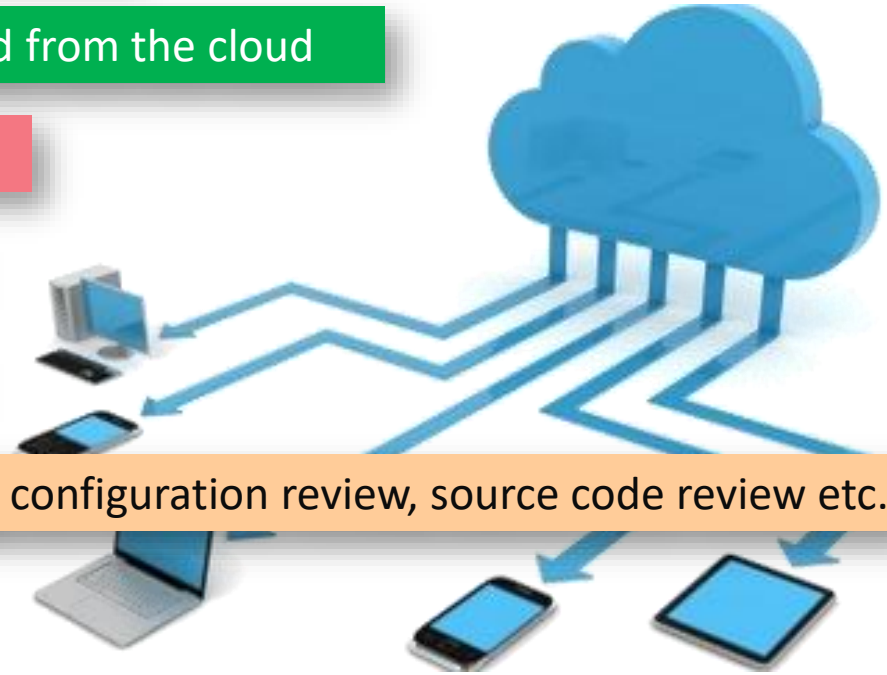
Sharing and access right of cloud apps

User behaviour monitoring and analysis

Security assessments-Pen testing, Vul scanning, configuration review, source code review etc.

Compliance auditing

Automated Self healing



Source: https://qtxasset.com/styles/breakpoint_l_640px_w/s3fs/2016-07/Cloud%20computing%20use%20sparingly.jpg?IU7wULk5hwY_wcTnUhSwV1W.gfdf1425&itok=gWsXwAMd

European Union General Data Protection Regulation (GDPR)



Primary objective: Assurance to EU citizens that their personal data are processed in a secure environment

Does not require any enabling legislation to the passed by national governments; thus it is directly binding and applicable

Apply to organisations that are not part of EU but collect and/or process personal data of EU residents

Will take into effect in May 2018

Non-compliance can result in severe penalties of up to 4 percent of worldwide turnover or upper limit of 20 million euro whichever is higher

Source: <http://hlb-poland.com/hlb-poland-news/important-data-protection-act-2018-amendment-are-you-aware/>

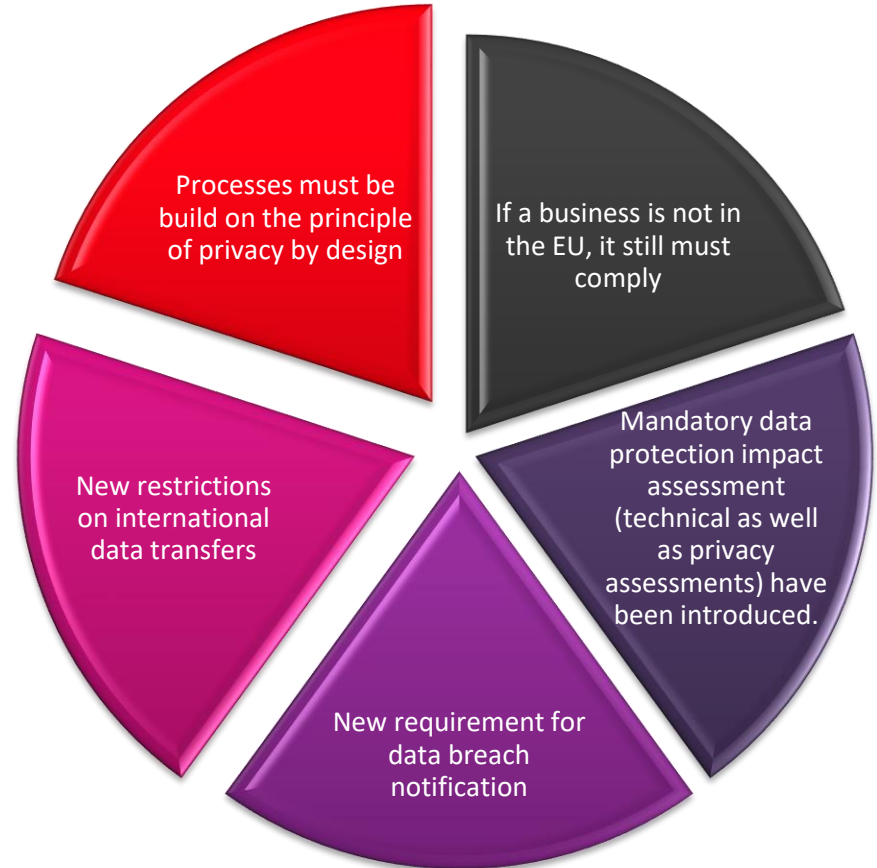
Data subjects have the following rights

Right to be forgotten/erasure

Right to access

Right to rectification

Right to object





Thank You!

Contact details:

DAVIS PULIKOTTIL

National Practice Manager

GRC, Sense of Security

Level 8, 66 King Street, Sydney NSW 2000, AUSTRALIA

T : +61 (02) 9290 4451 | M : +61 (0) 490147654 |

davis@senseofsecurity.com.au

© 2002 – 2017 Sense of Security Pty Limited. All rights reserved.

Some images used under license from Shutterstock.com or with permission from respective trademark owners. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

Security, it's all we do. Knowledge, Experience & Trust.

Sense of Security Pty Ltd
ABN 14 098 237 908

Sydney
Level 8, 66 King Street
Sydney NSW 2000

Melbourne
Level 15, 401 Docklands Drive
Docklands VIC 3008

Tel. 1300 922 923
Intl. +61 2 9290 4444
www.senseofsecurity.com.au


@ITSecurityAU