Actuaries Summit

Think Differently

Actuaries Institute

21-23 May 2017 • Grand Hyatt Melbourne

Insuring Cyber Risk

A collaborative approach

Cyber Insurance Working Group

Presented by Susie Amos & Dean Marcus

Why Care?

Regulation

US experience

Growing

Agenda

Environment

Product and Pricing

Claims and Reserving

Aggregation

The Future

Environment

ebay

ASHLEY MADISON®.COM

NHS

Australian Red Cross BLOOD SERVICE

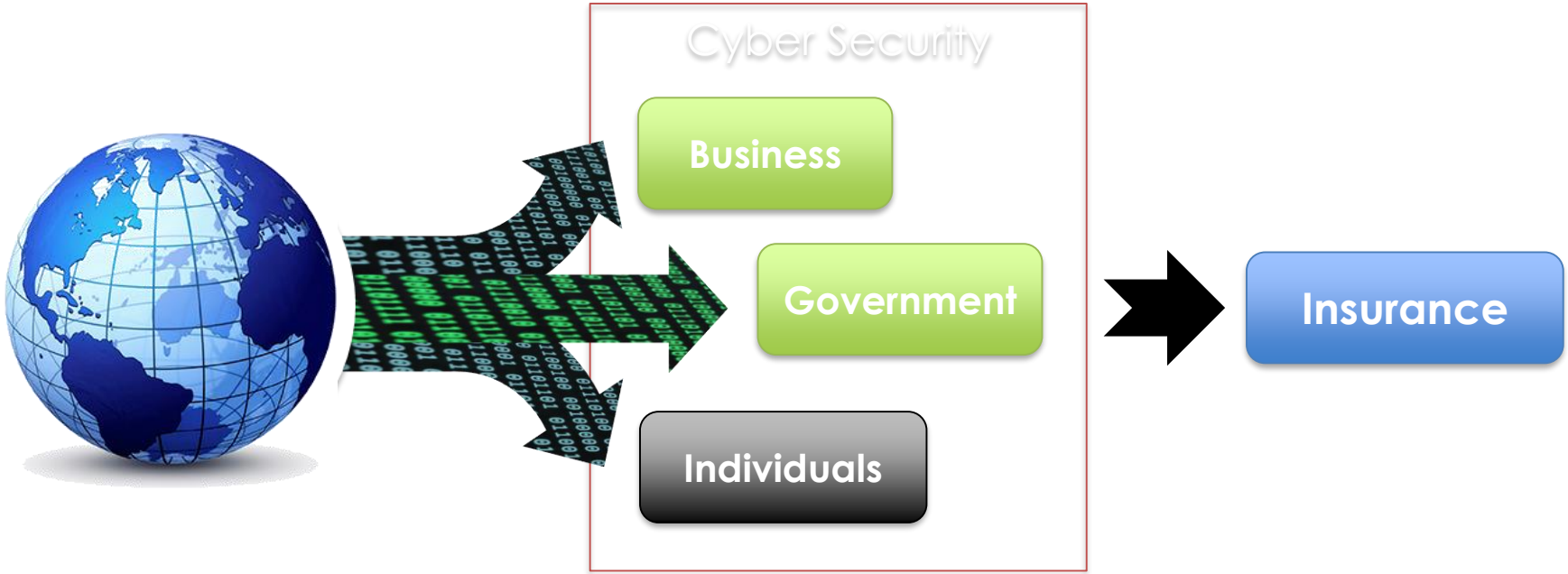
Census
abs.gov.au/census
For a brighter future

Target

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy

Cyber Risk

Our Focus is on Cyber Insurance

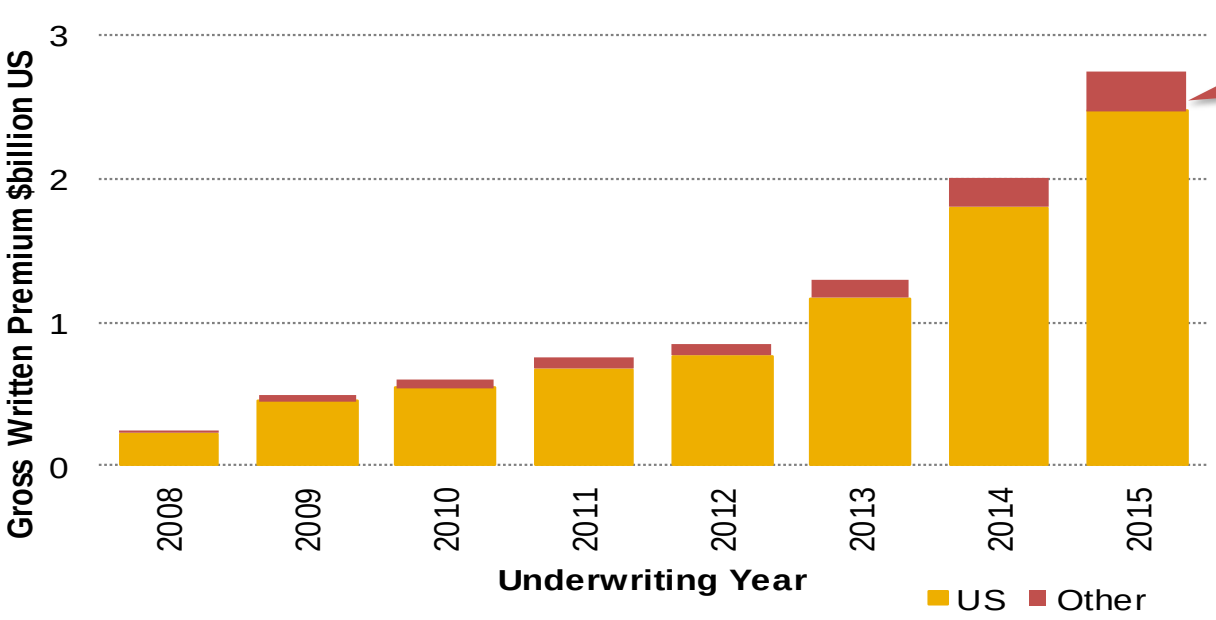


Where does insurance fit in?

Insurance is one piece of cyber risk management

Market Size

Global Cyber Premium is $2.5B



Australian GWP is estimated to be **20 million (AUD)**

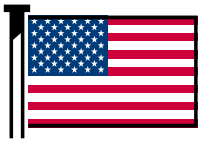
Annual growth over 30% over the last 3 years

Source: PWC

Global Regulation

HIPPA (Federal)
Health insurance breach notification

Mandatory Norification (California)



2003

2009 -2013

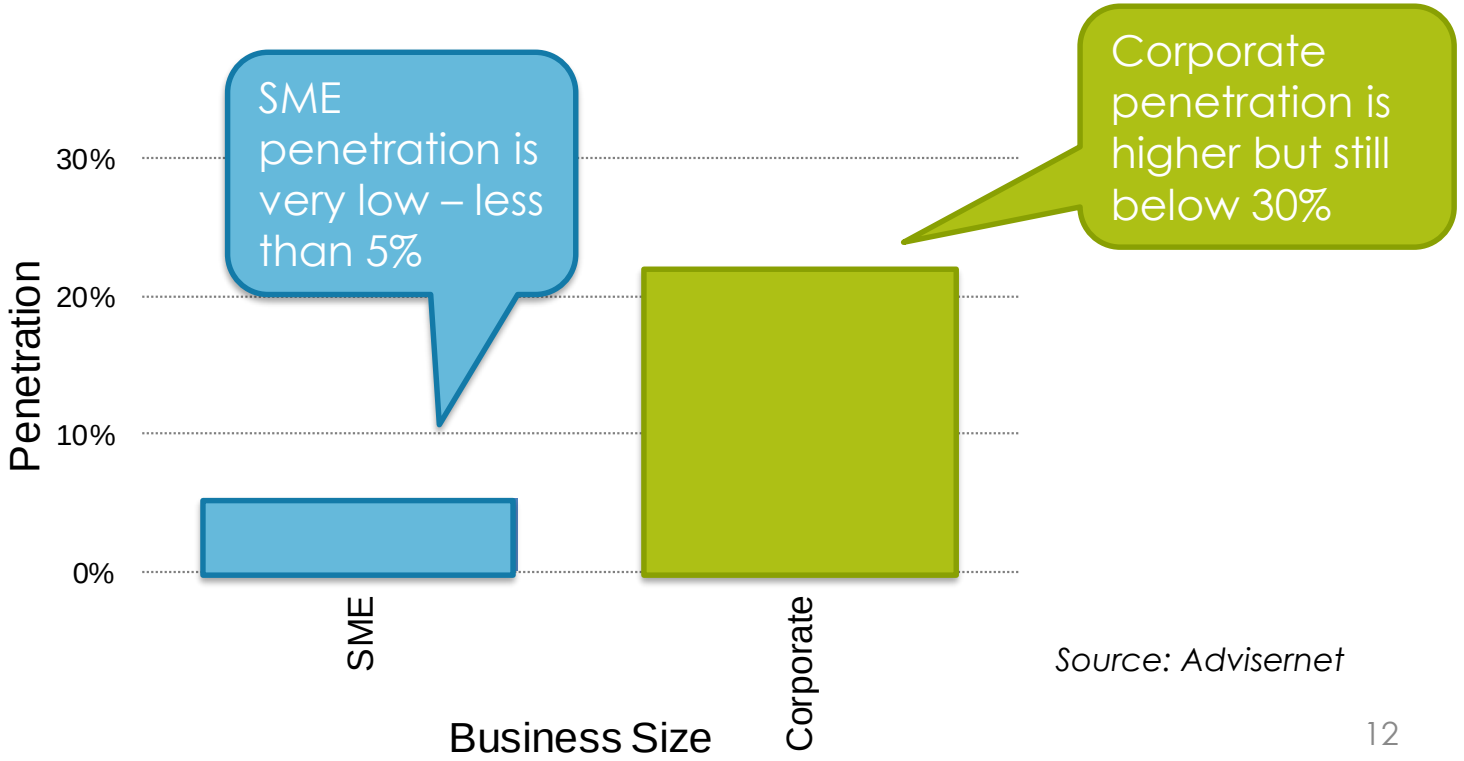
Federal & State
HIPPA enhanced. Similar requirements to California replicated in most other states

2016

GDPR (EU)
General Data Protection Regulation passed - comes into force in May 2018

Market Penetration – US

Opportunity for Growth



Source: Advisernet

Australian Regulation

Privacy Act
National Privacy Principles
OAIC

1998

My Health Records Act
Notifiable breaches

Privacy Act Enhancements
Australian Privacy Principles

2012

2015

Notification of Serious Data Breaches
Exposure draft for consultation

2018

Notifiable Data Breach Scheme
Commencing 22 Feb 2018

Product and Pricing

Insurance offerings in Australia

In its Infancy

- **~20** insurers offering cyber
- **No** standard policy wording
- **15-50+** underwriting questions
- **Variation** in premiums
- **Gaps** in coverage
- **Response** services provided

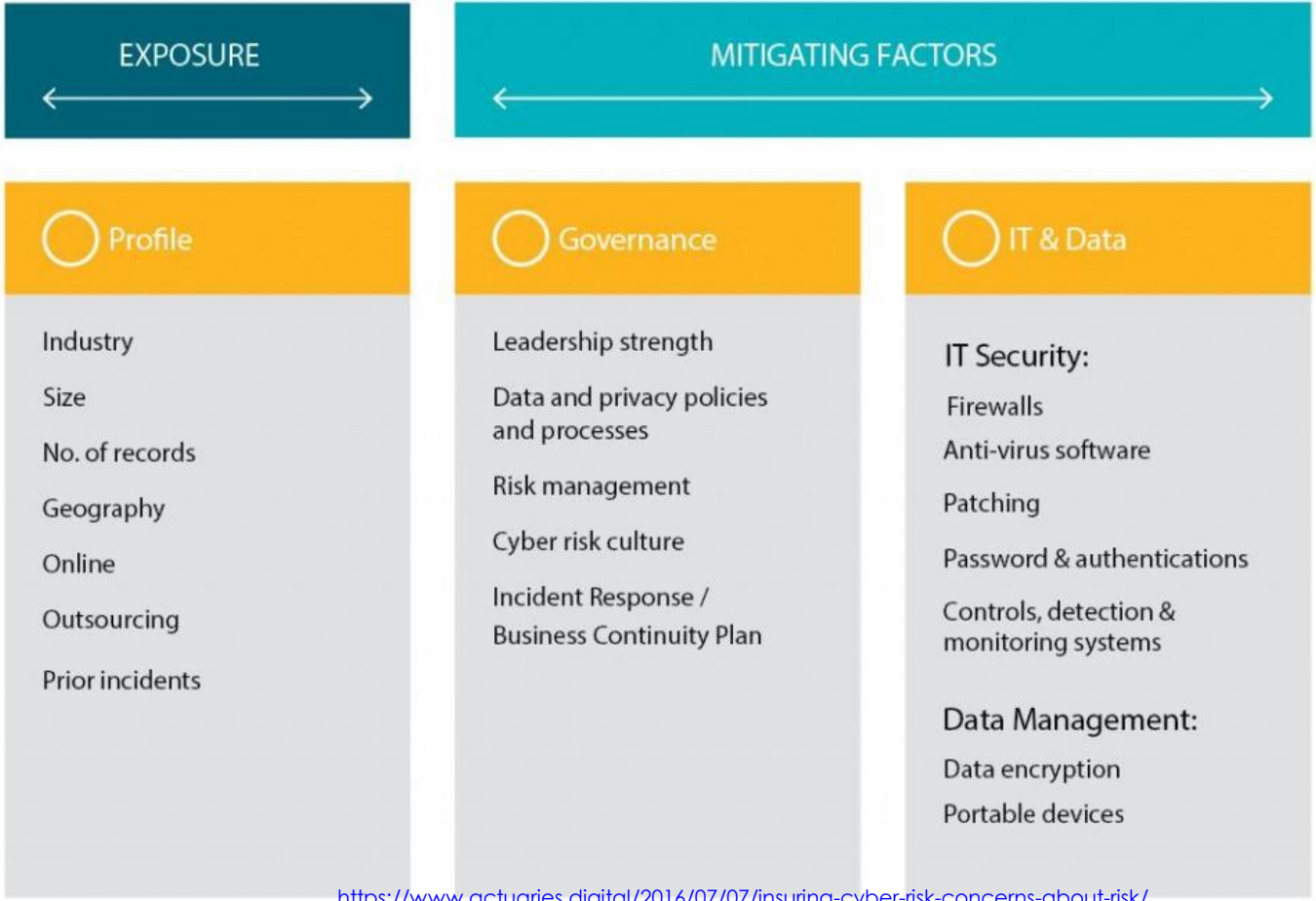
Cyber coverage

Cover	Property	General Liability	MGT Liability	PI / D&O	IT Liability	Crime	Cyber Security
1st Party							
Incidence Response	✗	✗	✗	✗	✗	?	✓
Information Asset Loss	✗	✗	✗	✗	✗	?	✓
Regulatory	✗	✗	✓	✗	✗	?	✓
Cyber Extortion Expenses	✗	✗	✗	✗	✗	?	✓
Loss of Income	✗	✗	✗	✗	✗	?	?
3rd Party							
Data Privacy Liability	✗	✗	?	?	?	✗	✓
Media Liability	✗	?	?	?	?	✗	✓
Network Security Liability	✗	✗	✗	✗	?	✗	✓

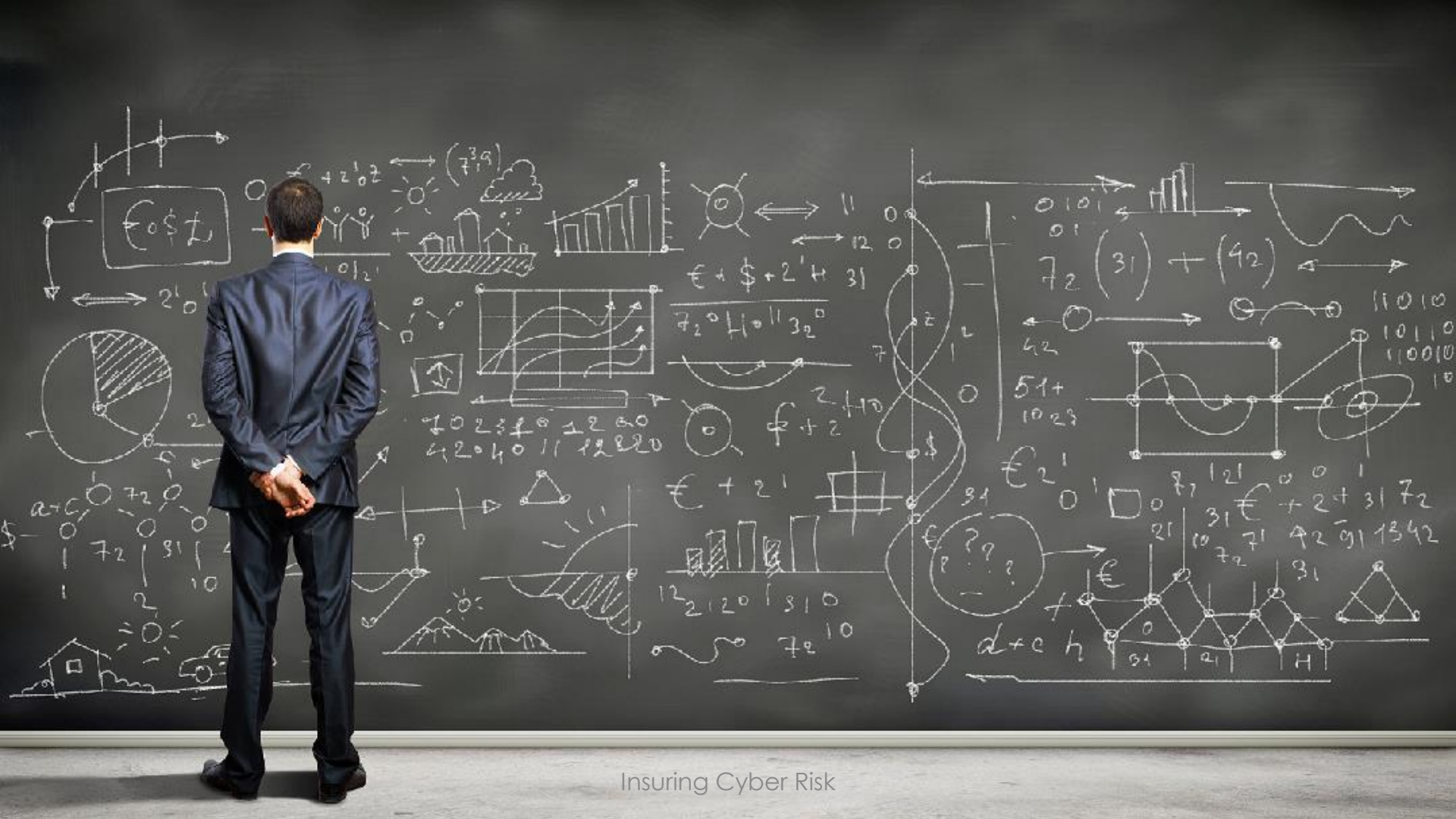
✗ Not generally covered ✓ Covered ? Uncertain or varied coverage

http://www.actuaries.digital/2016/06/29/insuring-cyber-risk-concerns-about-coverage/

Drivers of Risk



https://www.actuaries.digital/2016/07/07/insuring-cyber-risk-concerns-about-risk/



Insuring Cyber Risk

Show me the Data!

NetDiligence®
2015 CYBER CLAIMS STUDY

Ponemon INSTITUTE

IT security
Threats
DDoS attacks
Breaches
Cyber losses
Paid cyber insurance losses?

Show me the Data!

Available data*

- Surveys: Breaches reported by a few large US companies.
- Mandatory breach notification may lead to better data, but is an underlying driver of higher claims.

General caveats

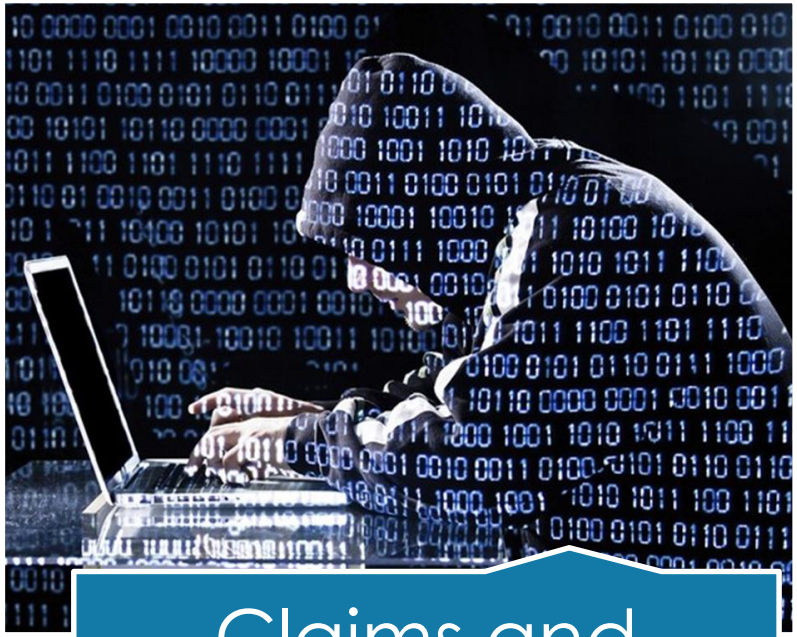
- Events are breaches rather than insurance claims.
- Doesn't cover all perils.
- How useful is historical data?
- Very few breaches are reported.

*See Appendix A

Limitations/Biases in Data*

- Small samples
- Reporting bias
- Lacking detail
- Not insurance Data

*See Appendix A



Claims and Reserving

Timeline of a Claim

- Notify Insurer
- Response Team

- Qualify
- Legal
- Crisis management

- PR
- Notify regulator
- Insurance investigation
- Rectification Plan

- Rebuild/replace systems
- Improve security
- Monitoring of impacted data
- Liaise with investigators
- Finalise claims cost

Claims Handling

Support responding to attack

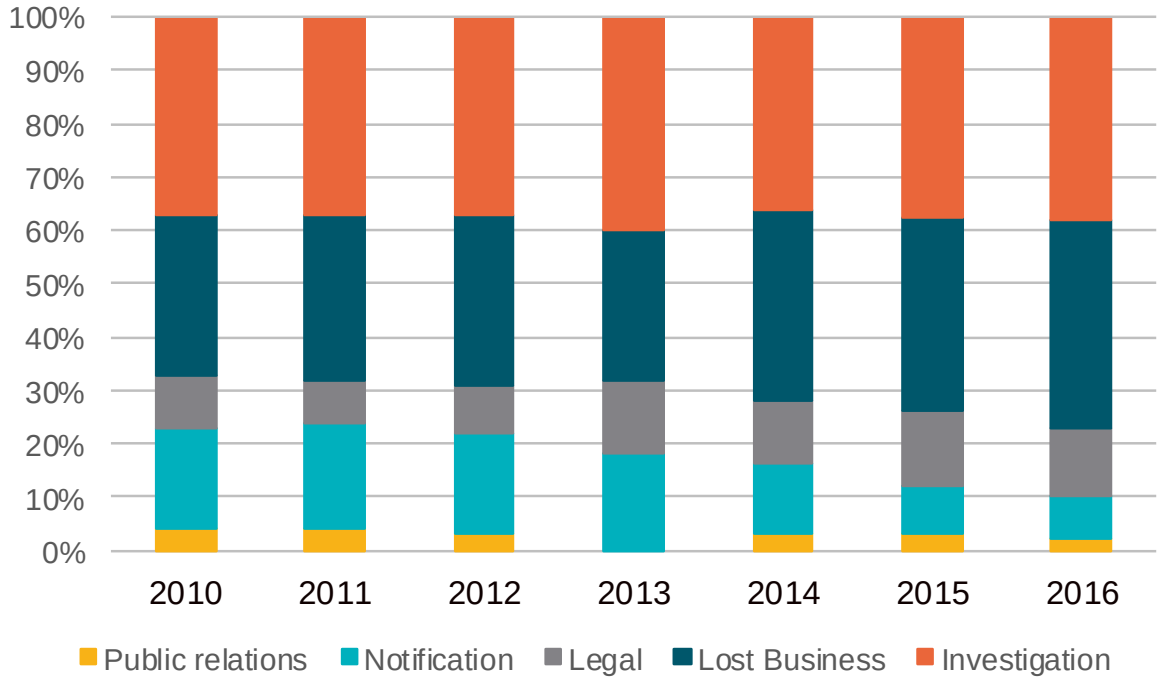
- Fast response times
- Analogous to kidnap and ransom policies
- 3rd party support for crisis, mitigation, IT forensics and legal

Insurer perspective

- Wide range of services and skills
- Scaling claims handling down to smaller businesses/losses?
- Is an "all perils" cover more appropriate in some cases?

Claim Trends

Investigations and Lost Business Drive Costs



Reserving

Initial challenges

- No standard policy wordings, coverage and exclusions
- Best data is out of date
- Claims coverage conflicts: coverages can conflict with other policies!

Similar classes

- PI and Medical Malpractice
- D&O
- Liability

➢ Common learnings: dealing with new &evolving policy wordings, lack of case law and precedents

Reserving – What do We Know?

- Average time to identify a breach: 163 days*.
- Once a breach is identified:
  - First party heads of damage are *relatively* easy to estimate
  - Benchmarking surveys can assist for data breach compensation
  - Regulatory penalties evolve over time
- Reserving methodology: Initially will be very simple

*IBM/Ponemon 2016

Reserving – WARNING

$$Cost = number\ of\ records\ breached \times cost\ per\ record?^{*}$$

* https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf

Aggregation

Sandy Blackout: erin m

Aggregation & Scenarios

Statistical data for Cat-style modelling?

Scenarios?

Scenarios*

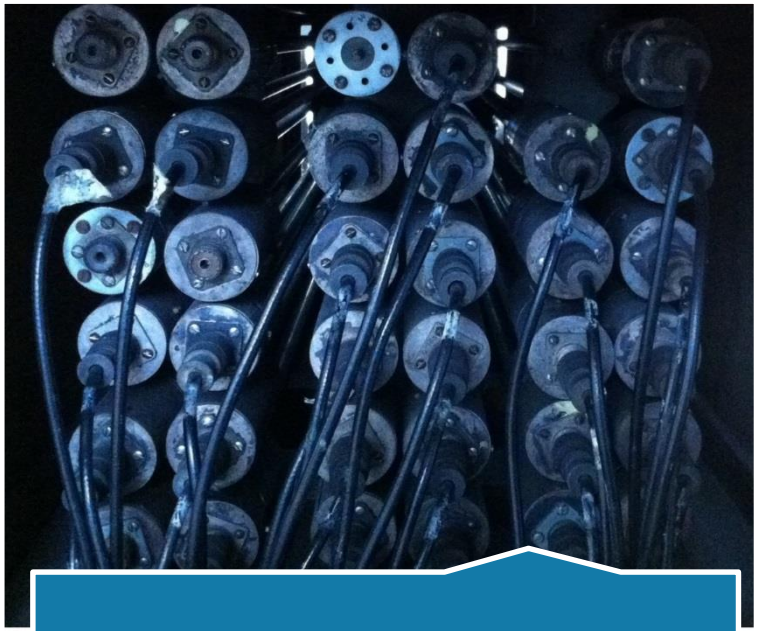
- Business Blackout – US/UK electricity grid
- Database corruption
- Data breach at major retailers (PRA)
- Data breach
- Ransomware
- Cloud breach
- Payment provider breach
- Denial of service attack
- Building management system breach

*Business blackout https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout
UK Grid http://www.lockheedmartin.com/us/news/press-releases/2016/april/collaboration-on-critical-national-infrastructure-cybersecurity.html
FSA Retailers: http://www.bankofengland.co.uk/pra/Documents/supervision/activities/generalinsurancestresstestingjuly2015.pdf
Others see RMS: http://forms2.rms.com/rs/729-DJX-565/images/RMS-Managing-Cyber-Insurance-Accumulation-Risk-05142016.pdf

Electrical Grid Scenarios

- Available data based on historical grid reliability:
  - Loss extent
  - Return period
- Credible threat:
  - December 2015 Ukrainian attack*
  - Demonstrations of attacks on specific pieces of equipment
- **Key message: bear in mind proximate cause**

*https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyber_attack
For more discussion on scenarios, see http://www.actuaries.digital/2016/02/22/insuring-emerging-cyber-risks-2/



The Future

CSIRAC Australia's first computer with 768 words of memory: photo SCIS (CC)

The Future

Regulation
Mandatory reporting of cyber events will be introduced, and losses are likely to increase.
Tightening of privacy laws is being considered in Australia, to give more protection in relation to use of personal information. This has already happened in the US.
Environment
Evolution of cyber threats as hackers become more sophisticated.
High profile cyber breaches are likely to impact Australian businesses - increasing the appetite for cyber insurance.
Insurance
Understanding and take up of cyber insurance will increase.
Streamlining of cyber products across markets to better meet businesses' needs.

Questions?

Our paper is will be released soon…

Appendix

Data

Appendix: Data

Key available datasets

Ponemon Survey (Australia)	• Benchmarks the cost of data breach incidents internationally and in Australia (separate reports) • Covers 26 companies in 11 sectors • Attack details and identification/reporting stats by industry, business size, cause • Preventative measures being used • Lost business costs
Verizon Data Breach Investigation Report	• Uses 64,199 incidents and 2,260 breaches to produce stats on breaches • Attack details and identification/reporting stats split by industry, agent, method, intention • Software vulnerability comparisons, phishing stats, etc.
NetDiligence Cyber Claims Study	• Uses 160 data breach insurance claims submitted by underwriters, usually relating to smaller organisations. They estimate that this covers "approximately 5% of the total number of cyber claims handled by all markets" with event dates between 2012-2015. • Attack details and identification/reporting stats split by claim/HoD type (first vs. third party, crisis services, legal defence, legal settlement, regulatory defence, regulatory fines), type of lost data, cause, industry, size of business.

- Congressional Research Service Cybersecurity: Data, Statistics, and Glossaries, Rita Tehan (2015): https://www.fas.org/sgp/crs/misc/R43310.pdf
- IBM/Ponemon: http://www-03.ibm.com/security/au/data-breach/index.html
- Verizon: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
- NetDiligence: https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

Appendix: Data

Survey biases

Sampling-frame bias and non-statistical results: The participants in the surveys aren't statistically representative of all companies in Australia, and the problem worsens when looking at particular industries/sizes. As a result, the surveys don't display statistical measures like confidence intervals.

Reporting bias: Firms are often reluctant to divulge accurate data or even record some events. This casts doubt on the reliability of the data, but might change over time depending on mandatory reporting.

Non-response bias: Companies that didn't participate may have significantly different data breach cost histories, and may have opted out of surveys in part because of this difference.

Unmeasured factors: Various important variables, including detailed security measures and other features of companies, are omitted from surveys.

Basis risk: The surveys typically measure losses from a business perspective, not from an insurance perspective

Makes You WannaCry

Ransomware

- **Files on a computer are locked** (encrypted), with decryption upon payment (in Bitcoin!).
- **Not guaranteed that decryption will occur** after payment, but hacker assumes reputation risk if not paying up!
- ***Not* a data breach**, but often covered by cyber insurance.

WannaCry

- **Global impact**.
- Total economic costs from interruption to business estimated up to **$4 billion USD***.

Case study – Cyber Insurance Process

1. **Insured:** See screen (left), consult internal IT then notify insurer.
   Insurer: Send response team to investigate and assist security.

2. **Insured:** Pay / don't pay, but restore backup.
   Insurer: Determine coverage under Ransomware payments, business interruption, and information asset loss; and incident response cost.

3. **Insured:** Improve security.
   Insurer: Potentially assist the insured in improving security, finalise claims cost and pay.

*http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18B00H