Actuaries Summit

Think Differently

Actuaries Institute

21-23 May 2017 • Grand Hyatt Melbourne

Insuring Cyber Risk
Insuring Cyber Risk
A collaborative approach

Cyber Insurance Working Group
Presented by Susie Amos & Dean Marcus
Why Care?

- Regulation
- US experience
- Growing

Insuring Cyber Risk
Insuring Cyber Risk

WannaCry

Ransomware

- Self-replicating software
- Vulnerabilities in Microsoft
- Files on a computer are locked (encrypted), with decryption upon payment (in Bitcoin!).

- Not a data breach, but often covered by cyber insurance.

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

Our Focus is on Cyber Insurance

Cyber Security

- Business
- Government
- Individuals

Insurance
Where does insurance fit in?
Insurance is one piece of cyber risk management
Market Size
Global Cyber Premium is $2.5B

Source: PWC

Australian GWP is estimated to be 20 million (AUD)

Annual growth over 30% over the last 3 years

Insuring Cyber Risk
Global Regulation

**HIPPA (Federal)**
Health insurance breach notification

**Mandatory Notification (California)**

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

**GDPR (EU)**
General Data Protection Regulation passed - comes into force in May 2018
Corporate penetration is higher but still below 30%

SME penetration is very low – less than 5%

Source: Advisernet
Australian Regulation

Privacy Act
National Privacy Principles
OAIC

My Health Records Act
Notifiable breaches

Privacy Act Enhancements
Australian Privacy Principles

1998

Notification of Serious Data Breaches
Exposure draft for consultation

2012

2015

2018

Notifiable Data Breach Scheme
Commencing 22 Feb 2018

Insuring Cyber Risk
Product and Pricing

Insuring Cyber Risk
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

<table>
<thead>
<tr>
<th>Cover</th>
<th>Property</th>
<th>General Liability</th>
<th>MGT Liability</th>
<th>PL / D&amp;O</th>
<th>IT Liability</th>
<th>Crime</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st Party</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incidence Response</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Information Asset Loss</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Regulatory</td>
<td>X</td>
<td></td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Extortion Expenses</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Loss of Income</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td><strong>3rd Party</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Liability</td>
<td>X</td>
<td></td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Network Security Liability</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **X** Not generally covered
- **✓** Covered
- **?** Uncertain or varied coverage

Drivers of Risk

EXPOSURE

MITIGATING FACTORS

Profile

- Industry
- Size
- No. of records
- Geography
- Online
- Outsourcing
- Prior incidents

Governance

- Leadership strength
- Data and privacy policies and processes
- Risk management
- Cyber risk culture
- Incident Response / Business Continuity Plan

IT & Data

IT Security:

- Firewalls
- Anti-virus software
- Patching
- Password & authentications
- Controls, detection & monitoring systems

Data Management:

- Data encryption
- Portable devices

Insuring Cyber Risk
Show me the Data!

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
Timeline of a Claim

First Days
- Notify Insurer
- Response Team

First Week
- Qualify
- Legal
- Crisis management

First Month
- PR
- Notify regulator
- Insurance investigation
- Rectification Plan

3-6+ Months
- Rebuild/replace systems
- Improve security
- Monitoring of impacted data
- Liaise with investigators
- Finalise claims cost
Support responding to attack

• Fast response times

• Analogous to kidnap and ransom policies

• 3\textsuperscript{rd} 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

Insuring Cyber Risk
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 × cost per record?

Aggregation

Insuring Cyber Risk
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

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

For more discussion on scenarios, see http://www.actuaries.digital/2016/02/22/insuring-emerging-cyber-risks-2/
The Future

Insuring Cyber Risk
# The Future

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Environment</th>
<th>Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>➔ Mandatory reporting of cyber events will be introduced, and losses are likely to increase.</td>
<td>➔ Evolution of cyber threats as hackers become more sophisticated.</td>
<td>➔ Understanding and take up of cyber insurance will increase.</td>
</tr>
<tr>
<td>➔ 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.</td>
<td>➔ High profile cyber breaches are likely to impact Australian businesses - increasing the appetite for cyber insurance.</td>
<td>➔ Streamlining of cyber products across markets to better meet businesses’ needs.</td>
</tr>
</tbody>
</table>
Questions?

Our paper is will be released soon...
Appendix

Data
## Appendix: Data

### Key available datasets

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |

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