ASTIN, AFIR/ERM and IACA Colloquia
Innovation & Invention
23-27 August 2015 | Amora Hotel Jamison Sydney
Actuaries Institute

Managing Cyber Risk through Insurance

Eric Lowenstein
Aon Risk Solutions


UNDERGROUND
tzmovies.net

Today's Agenda

- What are the key risks and exposures?
- Changing landscape including legislative reform
- Gaps in conventional insurances
- The breadth and limitations of cyber insurance policies

I left my laptop on the train

Our website has been vandalised

We lost confidential documents in transit

My cloud services provider has deleted my data

Someone is holding my data to ransom

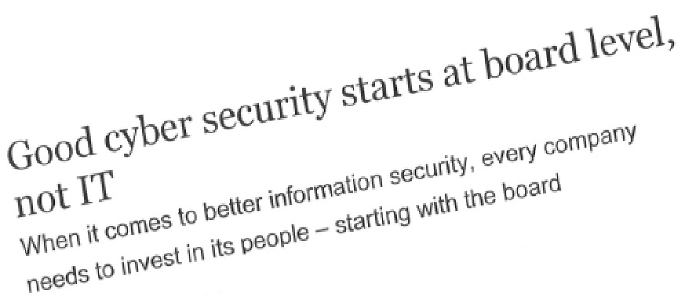
We've been hacked

A customer has posted misleading statements on our corporate Facebook page

Our access passwords have been compromised

Changing Landscape

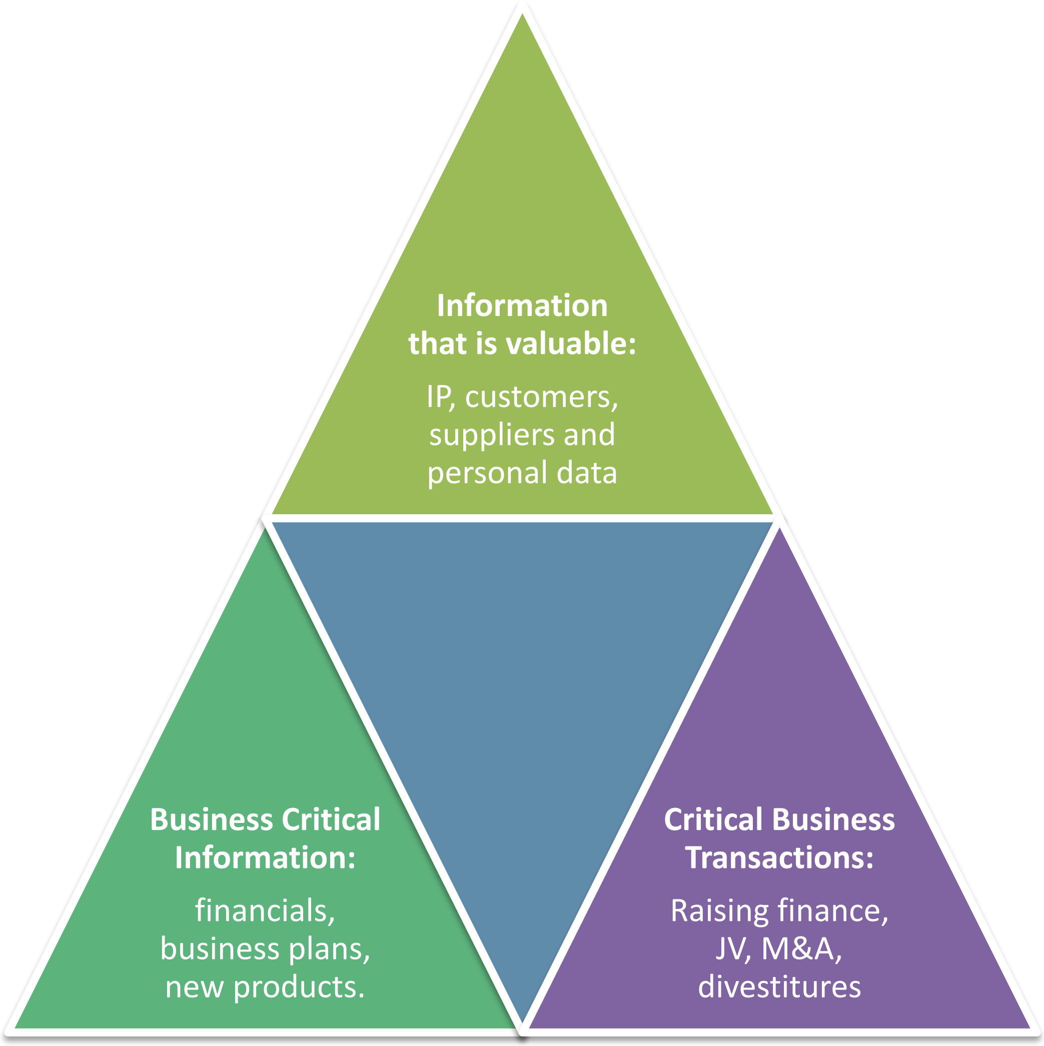
- Global cyber crime is on the rise
- Increased hacktivism
- Heightened media attention
- Laws and regulations creating new legal exposures
- Contractual requirements
- Increased awareness at Board level
- Cyber risk carve outs in conventional insurances


Good cyber security starts at board level, not IT

When it comes to better information security, every company needs to invest in its people – starting with the board

Who is being targeted?

What is being stolen?



Key Risks & Exposures

Fraud / Crime / Terrorism

- Malware attack / virus / phishing / hacking
- Cyber extortion
- Systems interruption / corruption
- Identify theft / disclosure of information

Social Media / Publishing

- Defamatory material
- Misleading content
- Privacy breaches
- Breach of intellectual property

Electronic data / devices / paper records

- Deliberate / malicious
- Negligence / human error (employee / supplier)
- Disclosure of information
- Loss or destruction of data / information

Technology Services

- Cloud computing
- Data storage / hosting
- Hardware / software maintenance

Regulatory & Compliance

- Licence suspension or cancellation
- Privacy Act violations
- Duties of directors and trustees

Brand & Reputation Damage

Loss of Revenue

Impact on Share price

Legal Liability

Forensic Consultant Costs

Breach Notification Costs

Regulatory Scrutiny

Fines & Penalties

System Disruptions

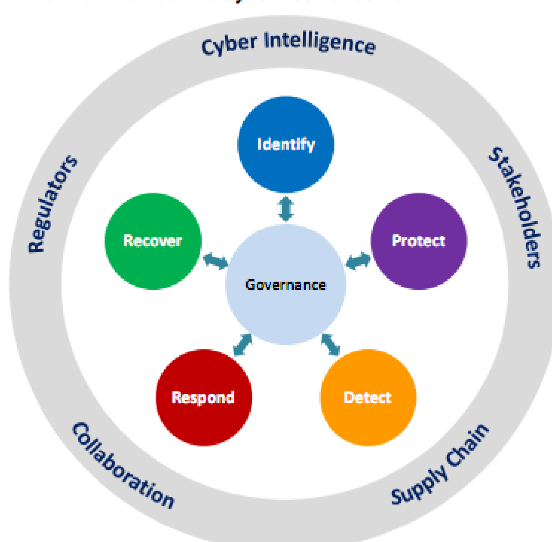
Increased Compliance Costs

Damage to Digital Assets

ASIC Guidance & Requirements
Report 429 - "Cyber resilience: Health check"

- ASIC defines cyber resilience as "*the ability to prepare for, respond to and recover from a cyber attack*".
- The Report emphasises the importance of cyber resilience in protecting the integrity of global markets and supporting consumer trust and confidence.
- ASIC noted that corporates must consider how and when a cyber attack may need to be disclosed as market-sensitive information in accordance with continuous disclosure obligations
- Directors' obligations to take cyber risks into account including cyber insurance when discharging their duties in considering risk management issues

Core functions and factors involved in a cyber-resilience framework



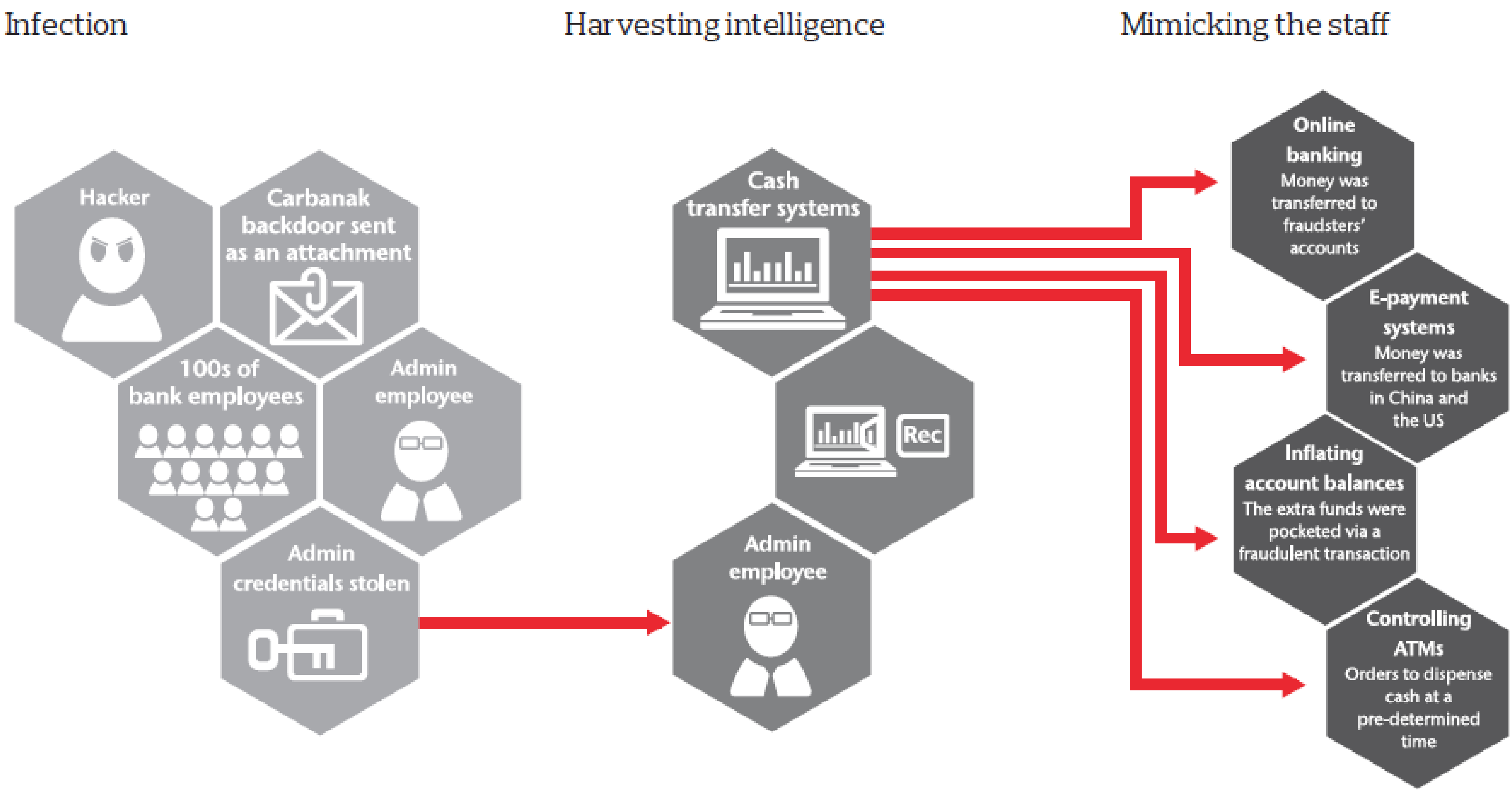
Are you aware of your obligations?

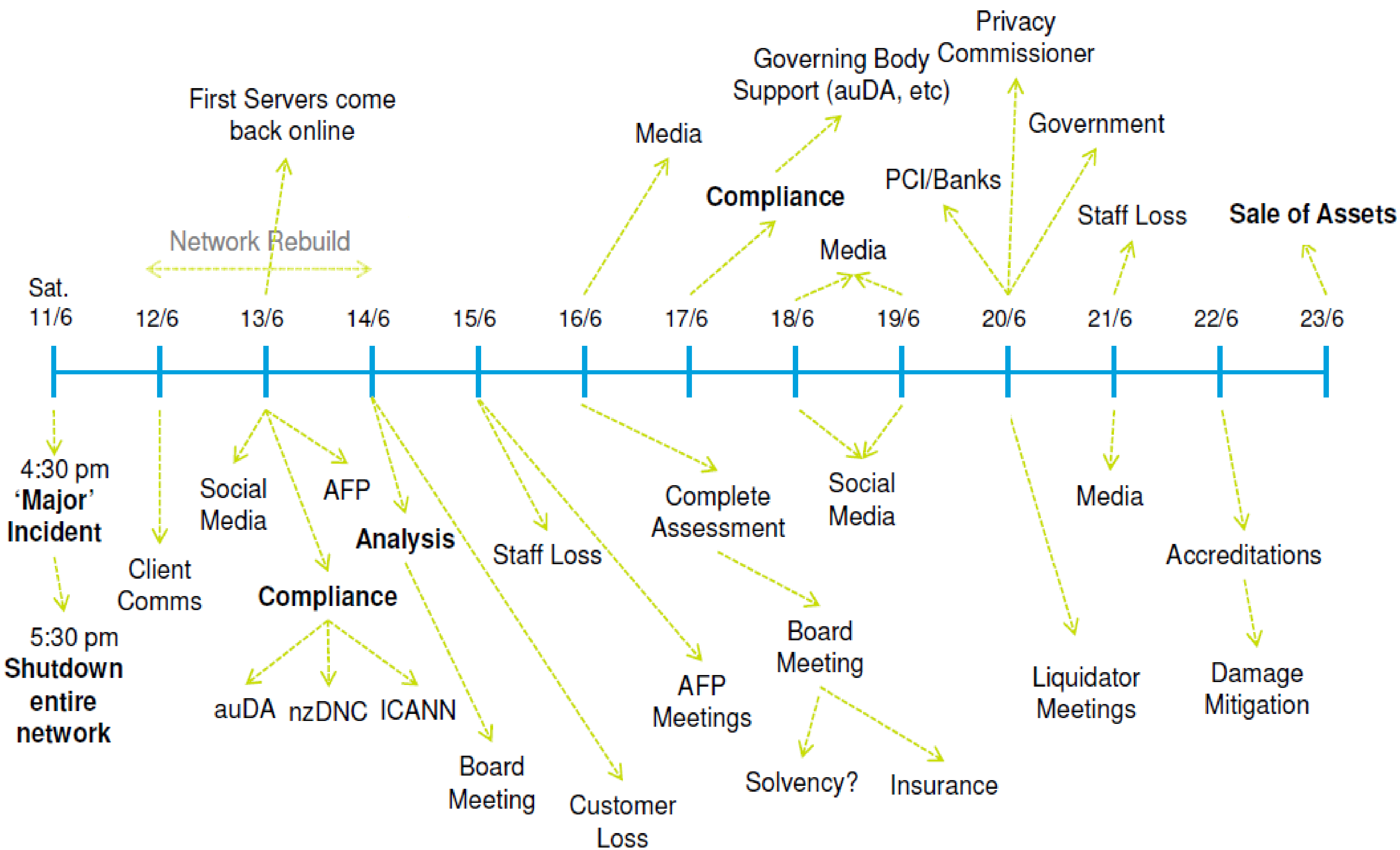
Are you aware of your obligations?	
If as a director, are you meeting your legal obligations?	You may not have considered how cyber risks may affect your directors' duties and annual director report disclosure requirements. Consider reviewing your board-level oversight of cyber risks and cyber resilience strategy, and consider if you need to incorporate greater consideration of cyber risks into your governance and risk management practices.
Have you considered disclosure of cyber risks in a prospectus?	Cyber risks may need to be disclosed if they are a significant factor that would form part of information that investors and their professional advisers would reasonably require to make an informed assessment of any offer.
If you are a listed entity have you considered your continuous disclosure obligations?	A cyber attack may need to be disclosed as market-sensitive information.
If you are an AFS licensee have you considered how cyber risks affect your general licensing obligations?	Your risk management plans, policies and procedures may need to take cyber risks into account. Inadequacies in your risk management systems may amount to a significant breach of your obligations that may need to be reported to ASIC. Cyber risks may need to be disclosed as a significant risk associated with holding the product.
If you are a responsible entity is your compliance plan is up to date?	A compliance plan must reflect, among other things, the major compliance risks that investors face. This may include cyber risks.
If you are a market participant, how do you identify and deal with unauthorised transactions on client accounts?	It is useful to pay particular attention to client accounts that appear to be trading unprofitably and take action to verify the origin of such orders, and address complaints of unauthorised transactions from clients. You could also encourage your clients to monitor their accounts and change passwords regularly.
Is your board and senior management are aware of your cyber risks?	You are encouraged to review the level of board and senior management oversight of your cyber risks, including how frequently risks are updated. Oversight should take into account your legal and compliance obligations and be proportionate to the cyber risks you face and the nature, scale and complexity of your business.
If you are a credit licensee How cyber risks affect your general licensing obligations?	Your risk management plans, policies and procedures may need to take cyber risks into account.

APRA Requirements

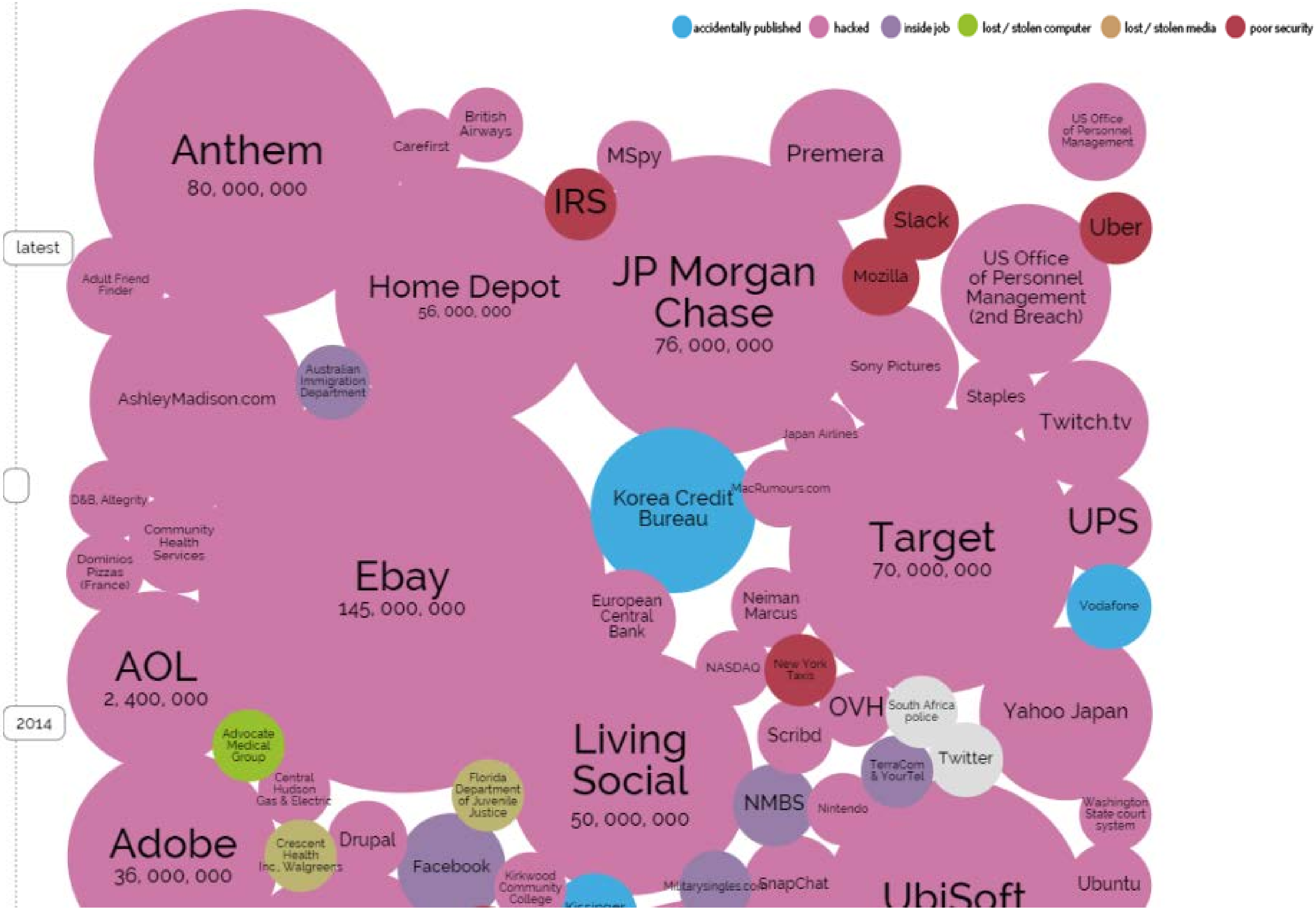
CPS 220 – Risk Management	• Submit a Risk Management Strategy to APRA • Submit a 3-year Business Plan to APRA (& re-submit annually or if material changes) • Submit a Risk Management Declaration & Financial Information Declaration to APRA (annually) • Dedicated risk management function (or role)
CPG 235 – Managing Data Risk	• Assess, classify & manage data at each stage • Adopt a systematic & formalised approach • Staff awareness • Auditability, desensitisation, end-user computing, outsourcing / offshoring responsibilities • Identify and develop processes to managed potential data issues • Test data risk management assurance programs frequently
CPG 234 - Management of Security Risk in Information and Information Technology	• Develop, implement & maintain a hierarchy of policies, standards and procedures • Adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework • User awareness • Regular assessments • Access control, asset management, physical security, monitoring and management

The Carbanak attack - patient and problematic




Sat. 11/6
12/6
13/6
14/6
15/6
16/6
17/6
18/6
19/6
20/6
21/6
22/6
23/6
Network Rebuild
First Servers come back online
Media
Compliance
Governing Body Support (auDA, etc)
Media
PCI/Banks
Privacy Commissioner
Government
Staff Loss
Sale of Assets
4:30 pm 'Major' Incident
5:30 pm Shutdown entire network
Client Comms
Social Media
AFP
Compliance
auDA
nzDNC
ICANN
Analysis
Board Meeting
Customer Loss
Staff Loss
AFP Meetings
Complete Assessment
Board Meeting
Solvency?
Insurance
Social Media
Liquidator Meetings
Media
Accreditations
Damage Mitigation

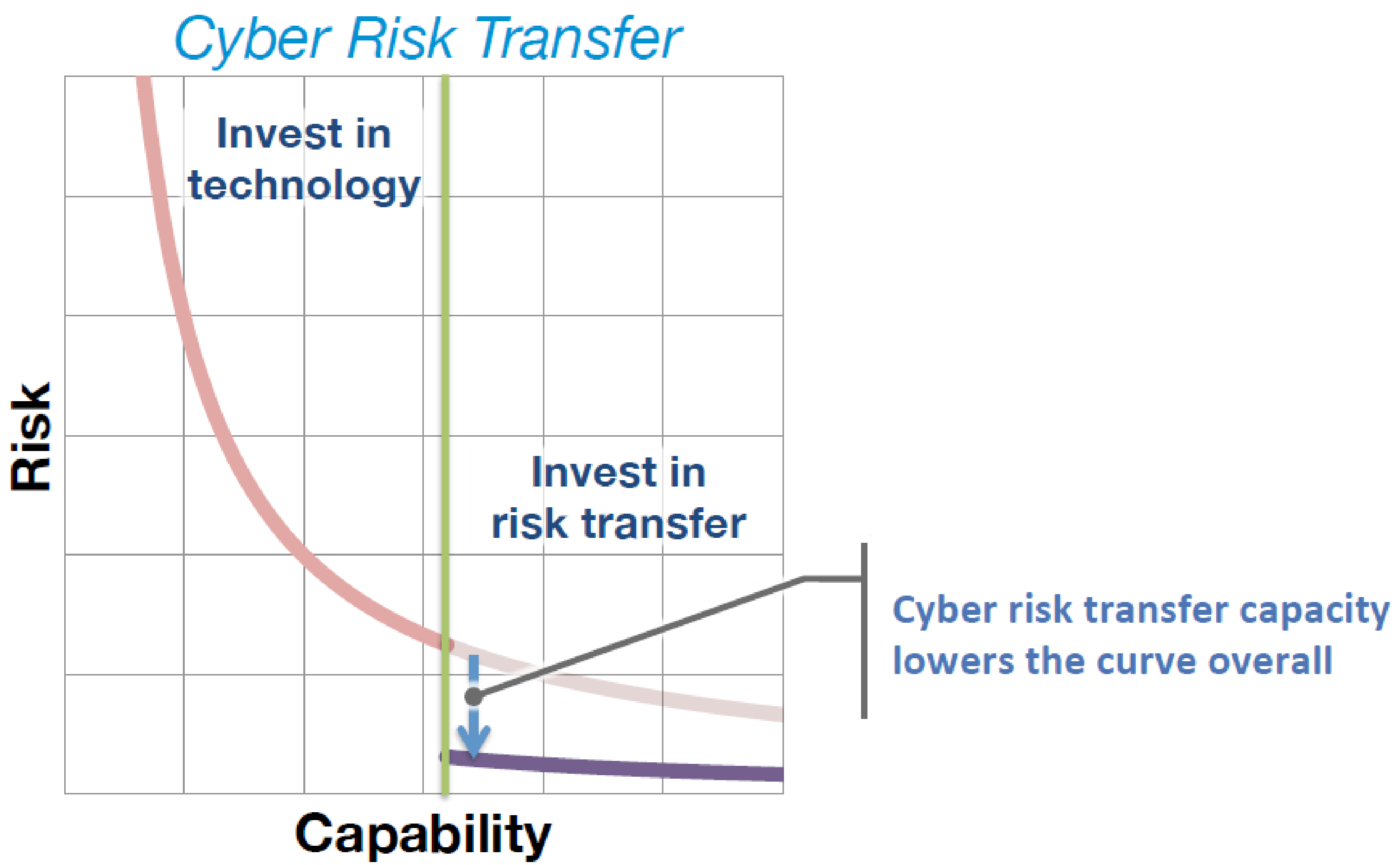
World's Biggest Data Breaches



What Does a Policy Usually Cover?

First Party	Third Party
Business interruption (loss of income and extra expenses)	Defamation claims
Costs to restore / recreate data	Infringement of intellectual property claims
Notification costs & credit monitoring services	Violation or infringement of privacy claims
Forensic investigations	Claims as a result dissemination of confidential information or damage to third-party systems
Cyber extortion	Legal defence costs
Crisis communication / public relations	Privacy breach regulatory proceedings and investigations
Legal costs assisting with privacy notification / compliance response	Fines & penalties

Cyber Risk Transfer



Gaps in Traditional Insurance Programme

	Property	General Liability	Crime/ Bond	K&R	PI	Cyber
1st Party Data Protection Privacy Risks						
Network Interruption						
Cyber Extortion						
Data Restoration, Recollection, Recreation (Determination and Action)						
Employee sabotage of Data						
Virus/ Hacker damage to Data						
Denial of Service attack						
Physical damage to Data Only						
3rd Party Data Protection Privacy Risks						
Breach of Personal Information						
Breach of Corporate Information						
Outsourcing Liability / Vicarious Liability						
Contamination of Third Party Data by any unauthorised software, computer code or virus						
Denial of access to third party data						
Theft of an access code from the Company's premises						
Destruction, modification, corruption, damage or deletion of Data						
Physical theft of the Company's hardware						
Data disclosure due to a Breach of Data Security						
Costs and expenses for legal advice and representation in connection with an Investigation						
Data Administrative Fines						
Repair of Company / Individuals Reputation						
Media Content Liability (IP, Plagiarism, defamation, trespassing)						
Notification Costs						
Monitoring Costs (with identity theft education and credit file or identity monitoring						

Coverage Provided

Coverage Possible

No Coverage

For reference and discussion only: policy language and facts of claim will require further analysis