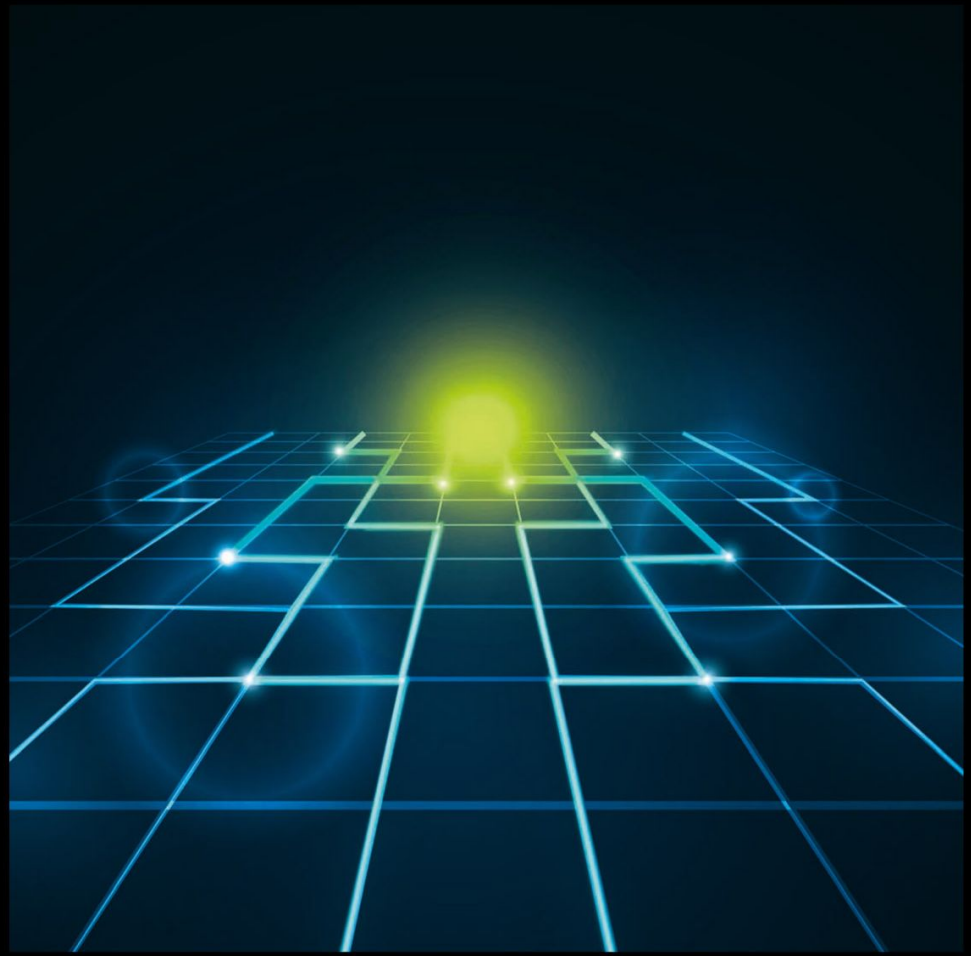
GI Glimpse

Actuaries Institute

3 August 2016 • Sydney



Cyber Security

Threats and Trends Today

Tony Vizza

sententia

a different way of thinking

Who are the hackers?

sententia
a different way of thinking

Cyber crime is huge

Symantec intel Security

$570 Billion

LLOYD'S

$380 Billion

Gross Domestic Product – Nominal - Billions USD

Source – World Bank 2015

20	Saudi Arabia	646,002
21	Argentina	548,055
22	Sweden	492,618
23	Nigeria	481,066
24	Poland	474,783
25	Belgium	454,039
26	Iran	425,326
27	Thailand	395,282
28	Norway	388,315
29	Austria	374,056

Huge issue globally

“Top Line Threat to National Security” - AG

Australian Cyber Security Strategy

Minister Assisting the PM for Cyber Security - Dan Tehan

Executive Order 13636

Cyber Security Framework 2014

Mandatory Breach Notification in most states

Data Protection Directive 1995

General Data Protection Regulation 2016

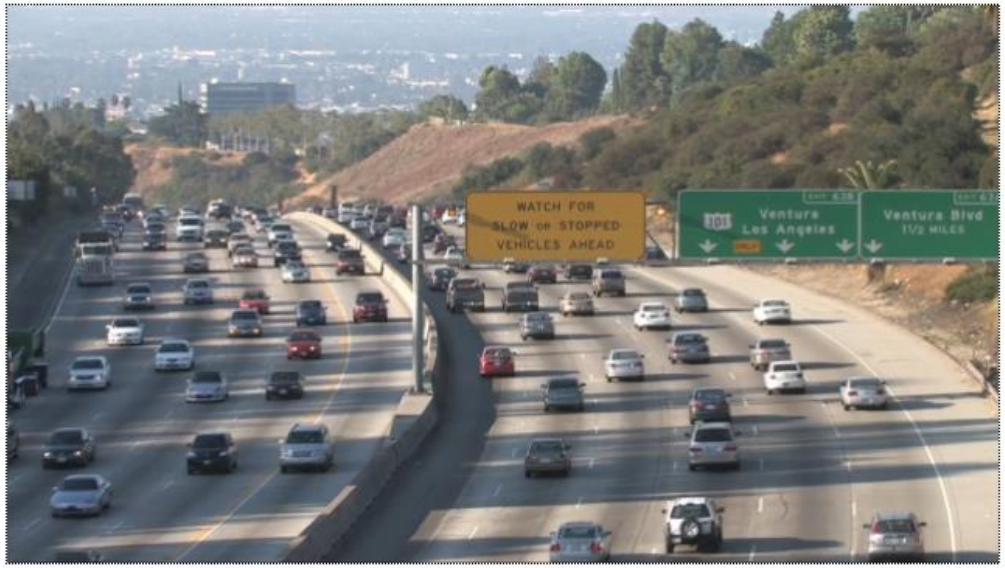
How easily can you personally be hacked?

FORTUNE SUBSCRIBE

TECH HACKING

Security Experts Say That Hacking Cars Is Easy

by Jonathan Vanian @JonathanVanian JANUARY 26, 2016, 6:47 PM EDT



New car features come at a cost

TRENDING: Siri takes control as Sierra beta arrives · Download: Best Places to Work in IT

COMPUTERWORLD INSIDER Sign In | Register

NEWS

Security researcher's hack caused airplane to climb, FBI asserts

Credit: flickr/francois schnell

The FBI said Chris Roberts hacked in-flight entertainment systems 15 to 20 times over three years

MORE LIKE THIS

Who's flying the plane? The latest reason to never ignore security holes

United launches bug bounty, but in-flight systems off limits

What third-party app crashed American Airlines pilots' iPads and caused flight...

on IDG **Answers**

How to prove an individual is stealing my data through smstracker he installed...

sententia
a different way of thinking

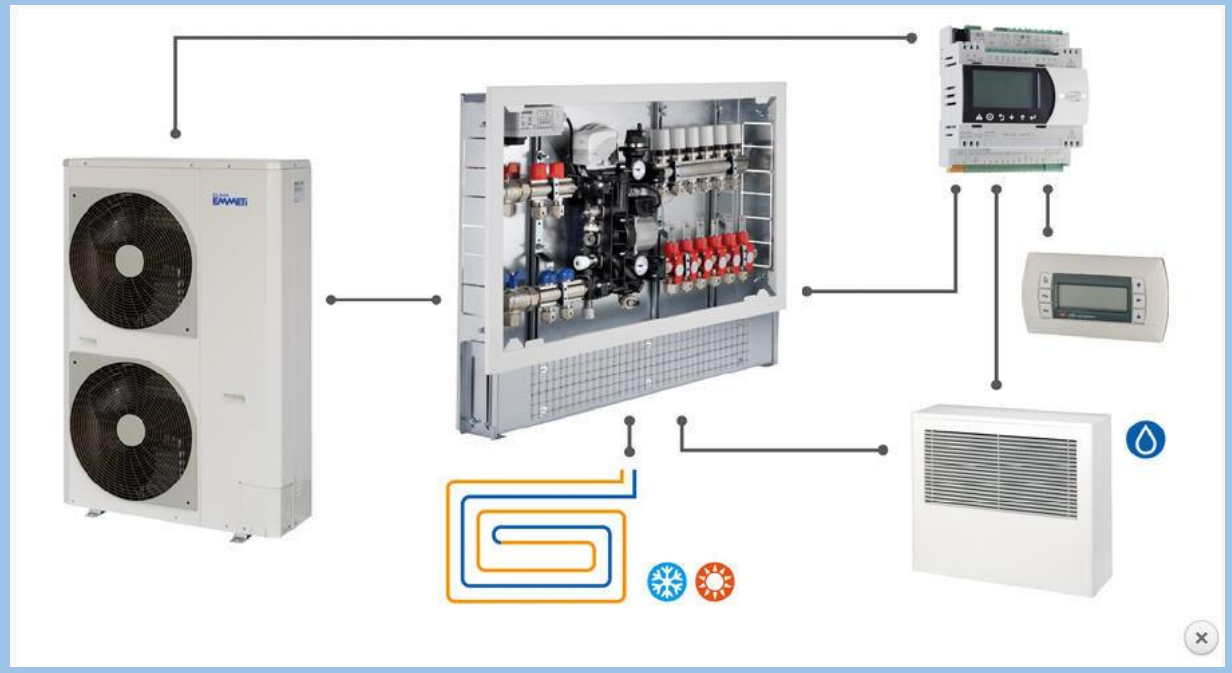
Poor cyber security is everywhere

Telstra Cable Gateway Max™

World's first AC Cable Gateway

The wild west of the IT world

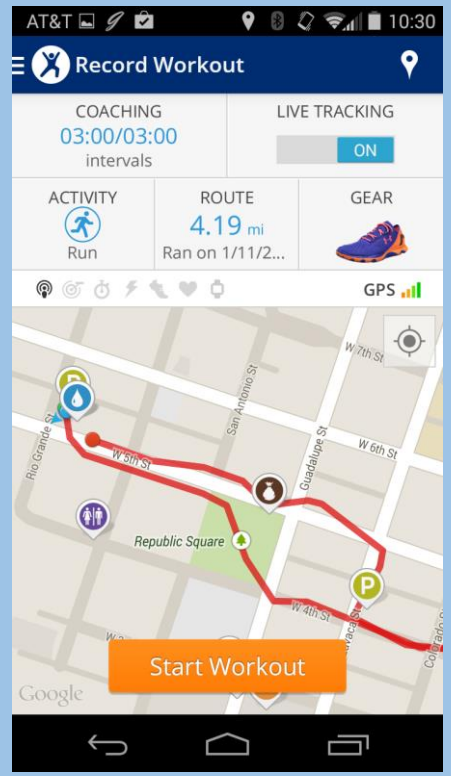
http://www.insecam.com

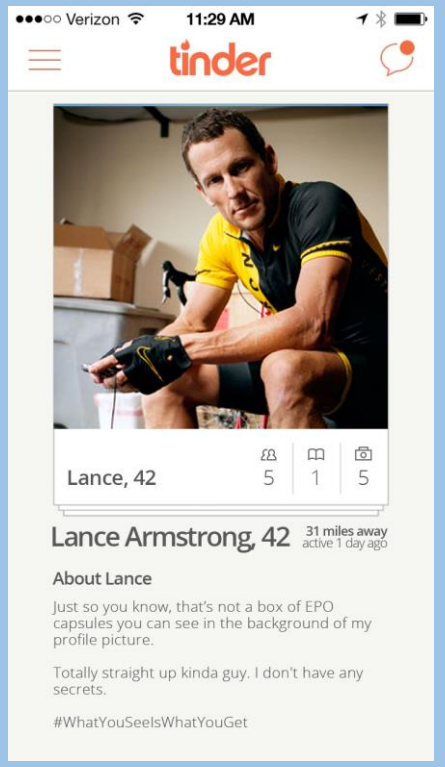


TARGET

Net cost of **$162 million** just in cyber breach related expenses.

And the Achilles heel – smartphones





sententia
a different way of thinking

Why bother?

The Codan Example

Codan posts record $26.5 million half-year profit on strong demand for its Minelab metal detectors

JULIAN SWALLOW THE ADVERTISER FEBRUARY 22, 2013 12:00AM

SHARE SAVE THIS STORY

Codan chief executive Donald McGurk with mine detectors made at Codan's Newton factory.

10 months later...

Codan halves profit forecast, shares down 39 per cent

VALERINA CHANGARATHIL THE ADVERTISER DECEMBER 12, 2013 11:40AM

SHARE SAVE THIS STORY

SOUTH Australian electronics manufacturer Codan has halved its first-half profit guidance and progressively cut jobs but says there is no reason to panic.

The company said volatility of its gold detector sales into Africa had resulted in sales for the first half being $50 million, or 80 per cent, less than the corresponding period in the previous financial year.

Civil unrest in Sudan over the control of gold fields had been one of the main factors behind the hit to its Minelab business.

Codan has now revised its first-half profit guidance to be in the range of $4 million to $5 million from an earlier "subdued" expectation of around $10 million.

Its share price fell 40 per cent in noon trading to 78 cents after it resumed trading.

Codan chief executive Donald McGurk with mine detectors made at Codan's Newton factory.

The Codan Example

Counterfeits are discovered

ABC “Four Corners” claims Chinese hackers have stolen Codan Blueprints

Net Profit collapse (down 80% in 12 months)

sententia
a different way of thinking

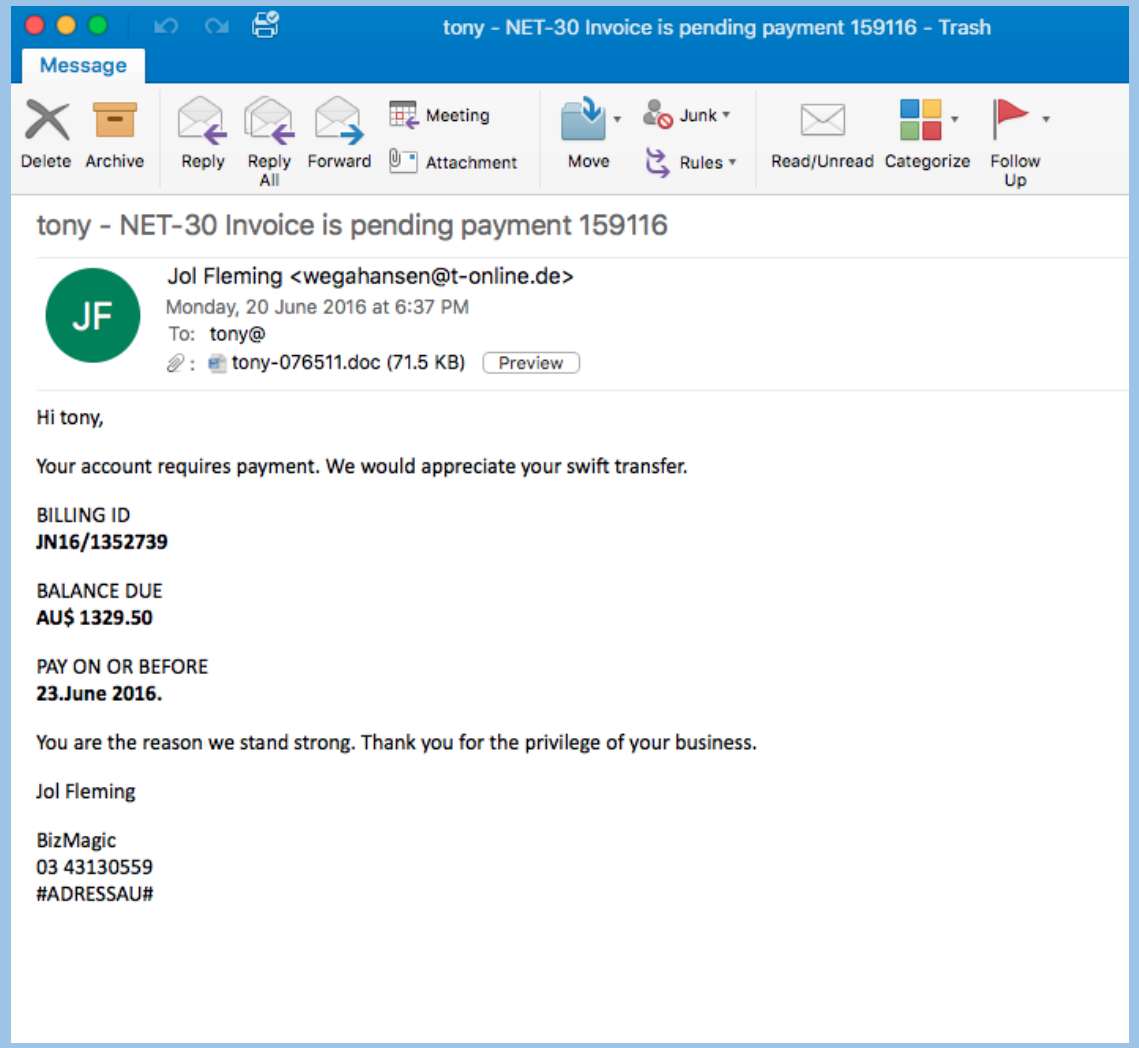
Hacking can take many forms …

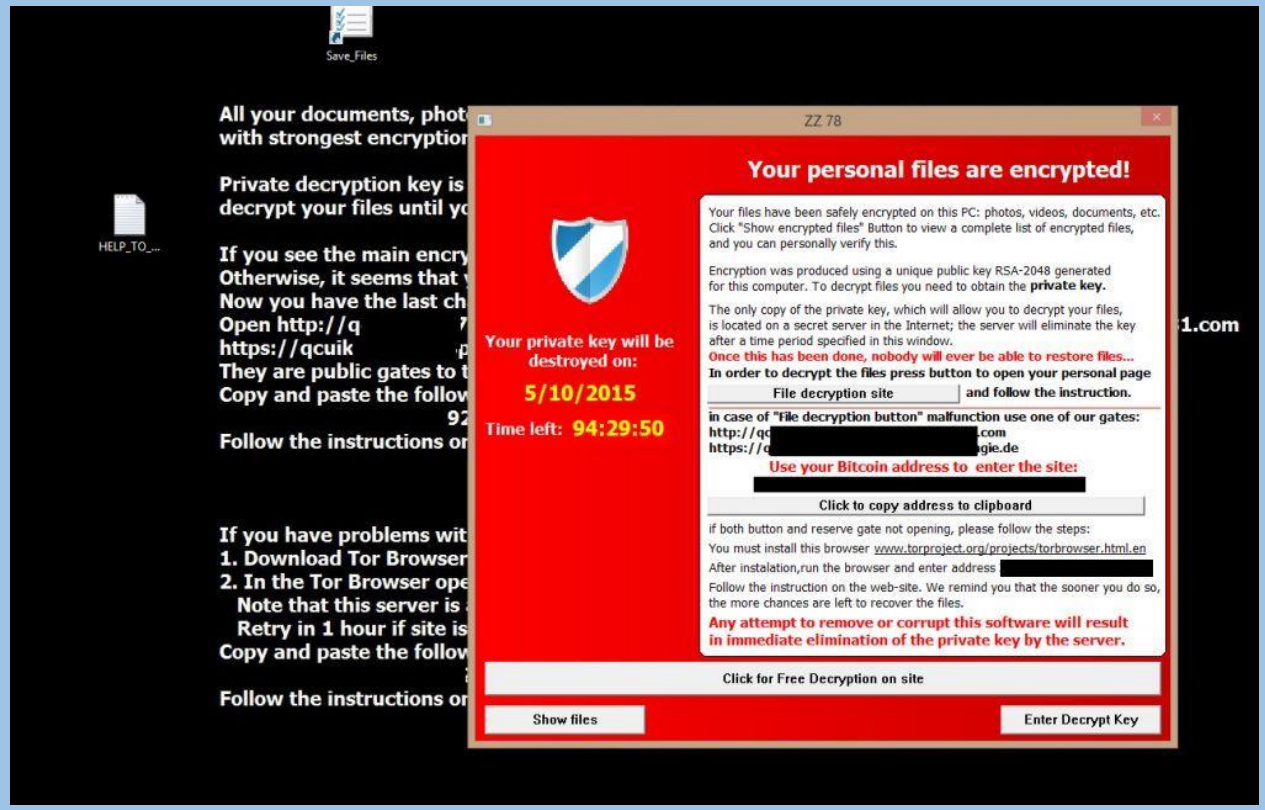
How to hack into a bank in 93 minutes – Less commercials!

This presentation explores the frightening reality of what can be achieved by piecing together the jigsaw puzzle of our digital footprints.

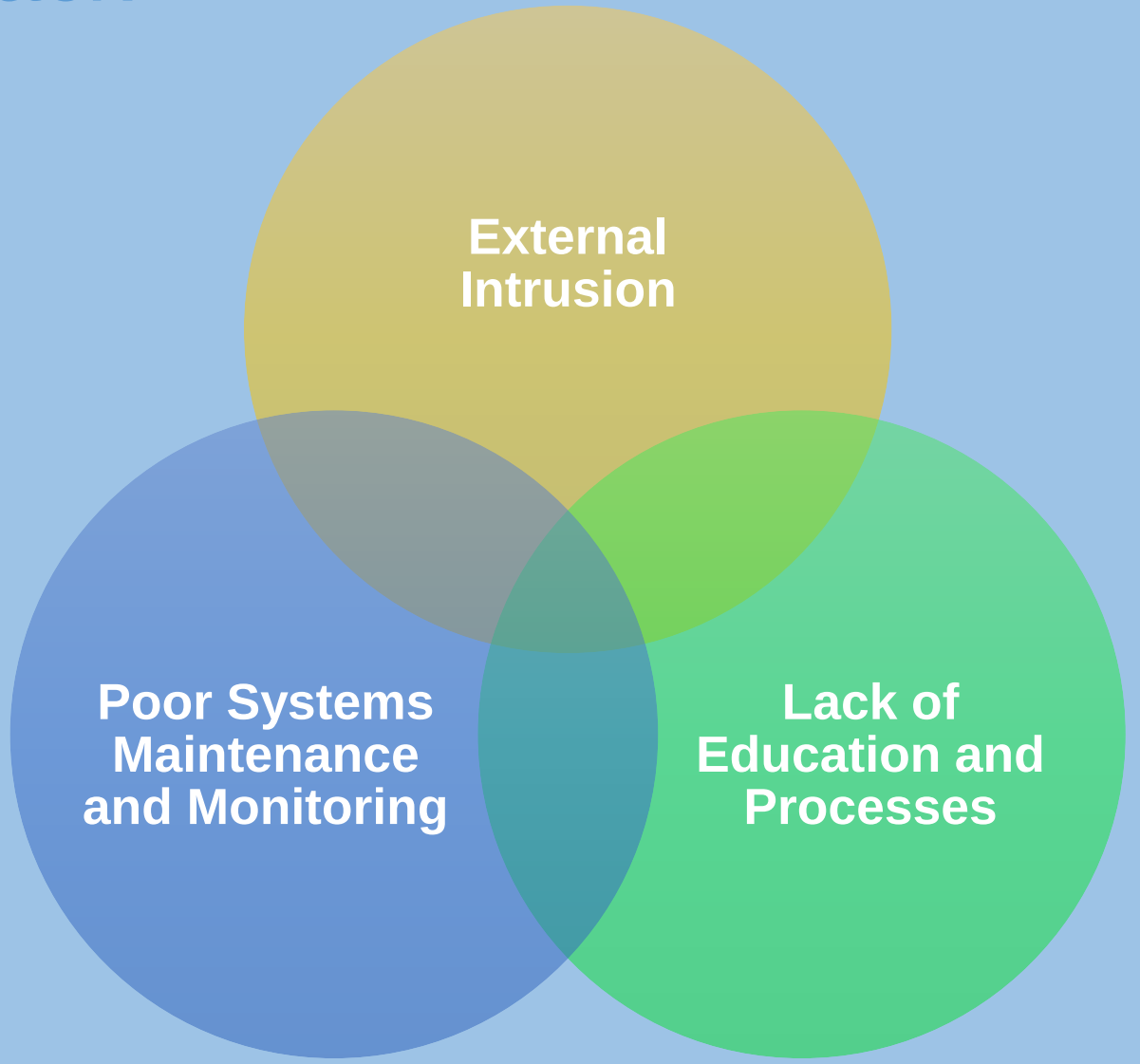
Inspector Matt McCarthy, NSWPOL Intel

Hackers are expert manipulators …





Anatomy of a hack

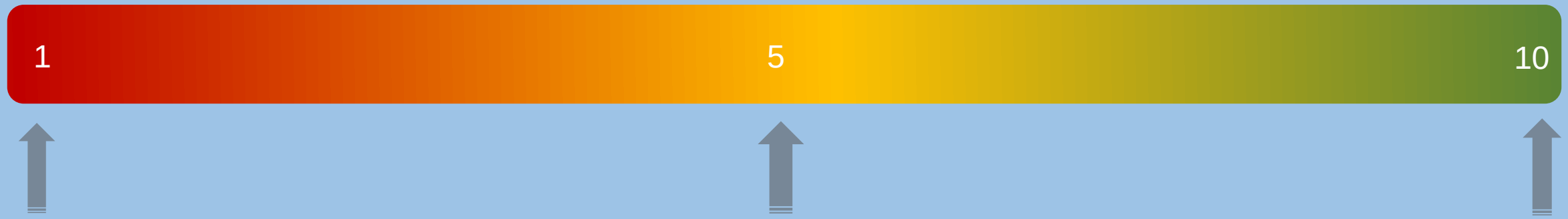


sententia
a different way of thinking

Cyber security from a risk perspective

Low Cost
High Risk

High Cost
Low Risk



"She'll be right, mate"

"Cyber Security is a necessary cost"

"We want to be ahead of the curve"

Cyber security professionals…

Make it as difficult as possible for a hacker to breach your organisation

Minimise your business risk and maximise your business resiliency

Recommend that risk managers pay close attention to cyber security and prepare

Thank You

Tony Vizza

Director of Sales and Marketing
Sententia

Phone: 0413 598 768
Email: tony.vizza@sententia.com.au

sententia
a different way of thinking

Cyber Attack Scenario
Insurance Response

Chris Mackinnon
General Representative
Lloyd's Australia

GI Glimpse

Actuaries Institute

3 August 2016 • Sydney

LLOYD'S

GI Glimpse

Actuaries Institute

Quantifying the Threat

- "Cyber crime is a bigger threat than drugs" *(UK Ex-Fraud Police Chief)*

- "There are two kinds of big companies in the US. There are those who've been hacked and those who don't know they've been hacked." *(2014 FBI director James Comey)*

- "We are in the midst of a crime wave unlike any since the 1920s and the age of gangsters" *(Tom Kellermann, Professor of cyber-security, American University)*

- There were 43 million global security incidents detected in 2014…..that's more than 100,000 attacks a day *(PWC Security Survey 2015)*

LLOYD'S

GI Glimpse

Actuaries Institute

Drivers of Future Growth

- 'The Internet of Things'
- Increasing Attacks
- Business Interruption / Supply Chain
- Industry and government sponsored information sharing of claims data and threat analysis, to aid Cyber Resilience
- Evolving Legislation: - EU regulations effective 2017

LLOYD'S

GI Glimpse

Actuaries Institute

Challenges

Matching Emerging Risks with Insurance Solutions

- Global interconnectedness
  - Cars, ships, aircraft, space, trains,
  - Logistics and supply chain – Food, water, sanitation
  - Smart devices
- Evolution of risk out pacing evolution of product
  - How viable will 12 month policies be in the future?
- Traditional lines of business unintentionally covering cyber risk
  - D&O exposures for failing to address risk
- Unanticipated aggregation of risk across multiple lines

Lloyd's Oversight

- Underwriting Performance monitoring: -
  - Establishment of common core data requirements
    - Consistent terminology and precise definitions
  - Establishment of specific Cyber Risk codes :-
    - Effective 2013: **CY** - Cyber security data and privacy breach
    - Effective 2015: **CZ** - Cyber security including property damage
- Underwriting Analysis and development of various 'Realistic Disaster Scenarios', with market returns required to monitor aggregation

SOCIETY & SECURITY

Business Blackout

LLOYD'S

Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE
Judge Business School

The insurance implications of a cyber attack on the US power grid

- We chose to investigate the economic and insurance costs of cyber attack against part of the US power grid:
  - Demand is emerging for insurance cover against the impacts of cyber attack against industrial control systems and operational technology in the critical infrastructure sector
  - Representative of the aggregate exposure management challenges that will emerge in the digitally connected economy
- The scenario was designed to be 'plausible but extreme' – that is, within solvency requirements and based upon threats and vulnerabilities known to exist
  - It is not a 'worst case scenario' – the attackers' capability and intent is limited to targeting a relatively small part of the US power grid

www.lloyds.com/businessblackout

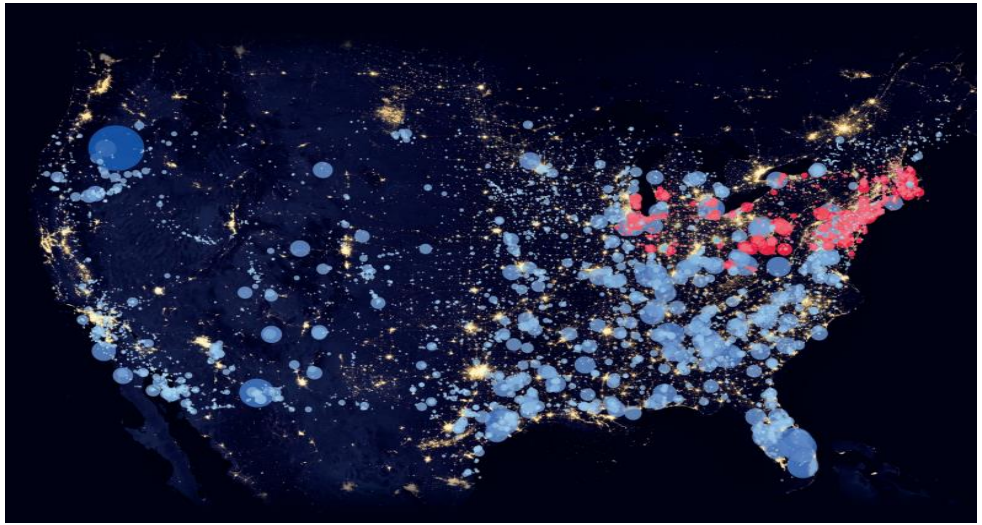
Business Blackout

LLOYD'S
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

Scenario

Year 1 | Year 2 | Year 3+

Research → Dormancy → Activation → Blackout → Aftermath



SOCIETY & SECURITY

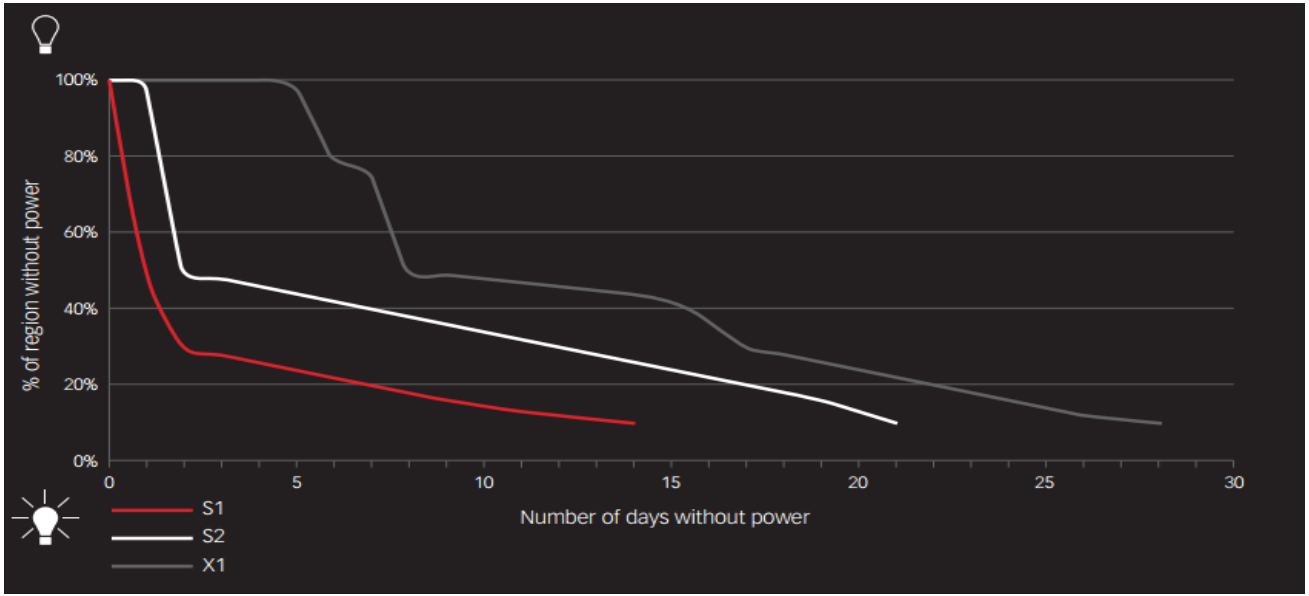
Business Blackout

LLOYD'S

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Scenario	Outage duration, weeks (to 90% restoration)	City-Days	Number of damaged generators	Percentage of generators vulnerable to contagion
S1	2	3.78	50	10%
S2	3	8.08	50	10%
X1	4	13.83	100	20%



Business Blackout

LLOYD'S
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

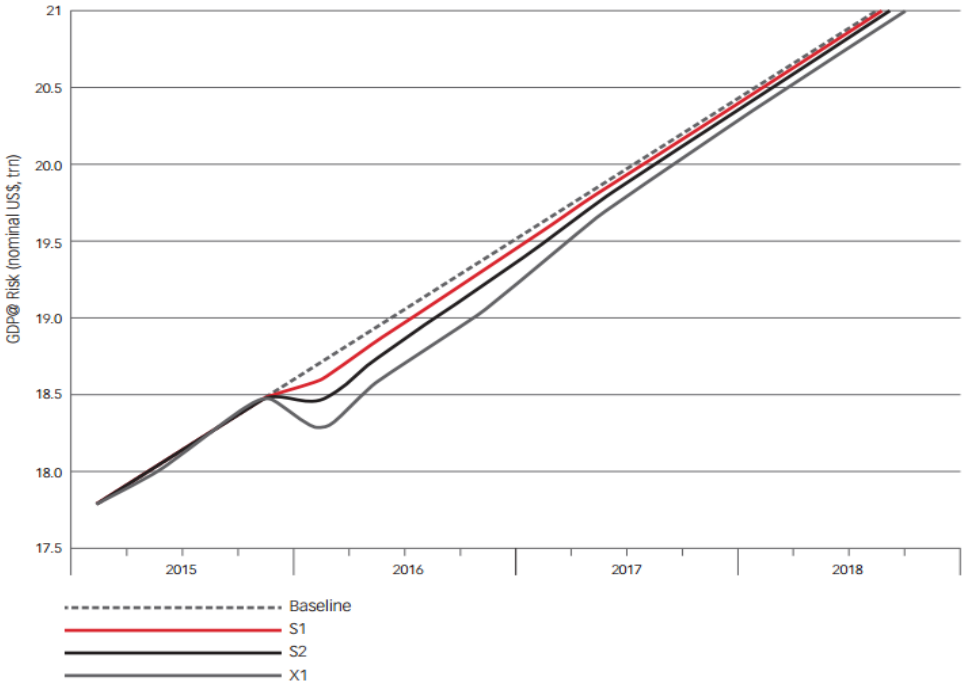
Direct cost of electricity interruption:

- **S1**: $61 billion
- **S2**: $130 billion
- **X1**: $223 billion

Total economic cost:

- **S1**: $243 billion
- **S2**: $544 billion
- **X1**: $1,024 billion

Figure 3: Domestic USA GDP@Risk under each variant of the Erebos Cyber Blackout Scenario



Insurance claimants

Power Generation Companies		$ millions
	Property Damage (Generators)	633
	Business Interruption (Generator Damage)	3,817
	Incident Response Costs	3
	Fines - FERC/NERC	4
	Other liabilities	-
Defendant Companies		
	Liability	2,253
Companies that Lose Power		
	Perishable Contents	595
	Contingent Business Interruption - Suppliers Extension	6,769
	Liability	3,120
Companies Indirectly Affected		
	Contingent Business Interruption - Critical Vendor	2,928
	Liability	749
Homeowners		
	Household Contents	465
Specialty		
	Event Cancellation	63
Total		**$ 21,398**

For variant S1

Estimated insurance industry loss:

- **S1**: $21 billion
- **S2**: $40 billion
- **X1**: $71 billion

Business Blackout

LLOYD'S
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

Property	
Personal Lines/Homeowner	0
Personal Contents	2
Commercial Combined	5
Construction & Engineering	1
Commercial Facultative	4
Binding Authorities	0

Casualty	
Workers' Compensation	1
Directors & Officers	3
Errors & Omissions	3
Financial Lines	3
General Liability	4
Healthcare Liability	0
Professional Lines	1
Professional Liability	2

Auto	
Personal Lines	-1
Commercial & Fleet	-2

Marine & Specie	
Cargo	0
Marine Hull	0
Marine Liability	1
Specie	1

Aerospace	
Airline	2
Airport	3
Aviation Products	1
General Aviation	1
Space	0

Energy	
Downstream	5
Energy Liability	5
Onshore Energy & Power	0
Upstream	0

Specialty	
Accident & Health	1
Aquaculture Insurance	0
Contingency – Film & Event	4
Equine Insurance	2
Excess & Surplus	1
Surety	0

Cyber Cover	
Standard Data Breaches	1
Advanced Property	5

Life & Health	
Life Insurance	0
Health Insurance	2
Income Protection	2
Death & Disability	0
Hospital Cover	-3

Pension and Annuities	
Standard Annuities	0
Variable Annuities	0
Enhanced Annuities	0
Life Settlements	0

War & Political Risk	
Kidnap & Ransom	0
Political Risk	2
Political Violence & Terrorism	1
Product Recall	3
Trade Credit	4

Agriculture	
Multi-peril Crop	0
Crop Hail	0
Livestock	0
Forestry	0
Agriculture	1

KEY TO CHANGE IN INSURANCE CLAIMS

Major decrease in claims — No change in claims — Major increase in claims

-5 -4 -3 -2 -1 0 1 2 3 4 5

Business Blackout

LLOYD'S
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

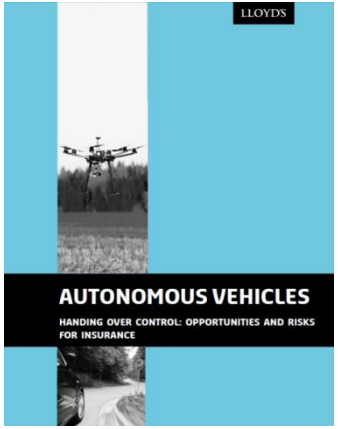
Date	Event name	Detailed description	Actors	Motivation	Methodology	Outcome
April 1999 (Milhorn, 2007)	**Gazprom – Russian gas supplier**	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorised Access
July 1999 (National Safety Transport Board, 2002) (Wilshusen, 2007)	**Bellingham**	Over 250,000 gallons of gasoline leaked into nearby creeks and caught on fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb. and April 2000 (Jill Slay, 2008) (Wilshusen, 2007)	**Maroochyshire**	A recently fired employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers and the grounds of a hotel.	Insider attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001 (US House of Representatives, 2005 (SCADA)[29] Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems, 2005	**California**	A hacking incident at California Independent System Operator (CASO) lasted two weeks, but did not cause any damage.	External attack	Unknown and contained	Deliberate	Thwarted
August 2005 (GAO Report, 2007)	**Daimler-Chrysler**	Thirteen Daimler-Chrysler US auto manufacturing plants were taken offline for about an hour by an internet worm. An estimated $14m in downtime costs.		Spyware Installation	Zotob Worm and MS05-039 Plug-n-Play	Infection

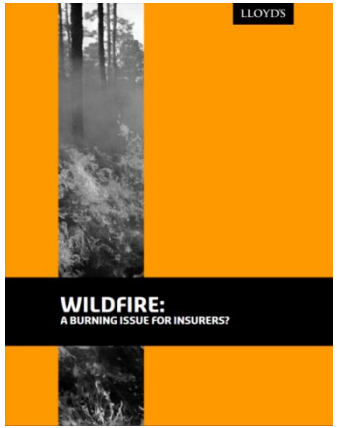
Business Blackout

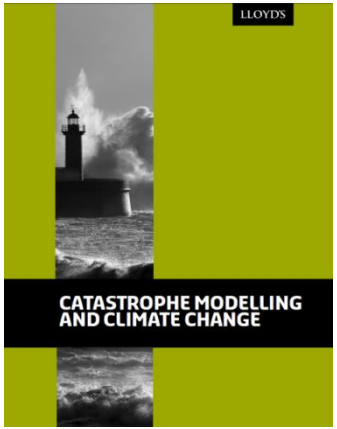
LLOYD'S
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

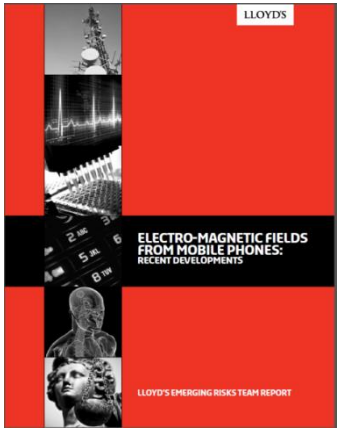
Infection	**Brown's Ferry**	Loss of recirculation flow on a US nuclear reactor down for maintenance caused a manual scram. A worm exploited a buffer overflow flaw in the widely used MSSQL server during the scram.		Unknown	Slammer Worm and Buffer Overflow	Non-industrial control systems targets
Oct 2006 (Wilshusen, 2007)	**Harrisburg**	Hackers gained access to a water treatment plant through an infected laptop.	Targeted Threat Agent	Mischief	Compromised Laptop	Server used to run online games
Jan 2008 (Maras, 2012)	**Lodz**	Attacker built a remote control device to control trains and tracks through distributed field devices. Four trains were derailed with zero deaths. A disgruntled employee installed malicious code on a canal control system.	Targeted Threat Actor, Accident or Insider Attack	Mischief	Altered Universal Remote	Mayhem, Criminal Damage
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the E.ON Kingsnorth power station which caused a 500MW turbine to take an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Protest
Nov 2008 (Kravets, 2009)	**Pacific Energy**	A recently fired employee disarmed safety alarms on three offshore platforms.	Insider Attack	Disgruntled Employee	Disabling alarm systems	Revenge & Sabotage
June 2009 to 2010 (Zetter, 2014)	**Stuxnet**	Malicious code targeted ICS at an Iranian nuclear plant. A recently fired employee disarmed safety alarms on three offshore platforms.	Virus	Unknown Presumed Nation State	Destroying centrifuges and thwarting uranium enrichment	Revenge & Sabotage
2010 to Aug 2014 (Symantec, 2014) (Kaspersky, 2014)	**Dragonfly/Havex/ Energetic Bear campaign**	A campaign against defence, aviation and energy companies	Remote access trojan (RAT)	Espionage	Malware infection and remote access	Malware clean-up
August 2012 (Bronk, 2013)	**Shamoon/ Wiper**	A Saudi Arabian oil company, Saudi Aramco, has over 30,000 workstations knocked out	RAT	Unknown Presumed Hacking group	Wiping 30,000 machines of their data	Unknown
April 2013	**California Power Station**	Snipers fired at a California substation, knocking out 17 transformers.	Physical	Unknown	Destruction of substation oil tanks	Unknown

Lloyd's – Thought Leadership









http://www.lloyds.com/news-and-insight/risk-insight/library

GI Glimpse

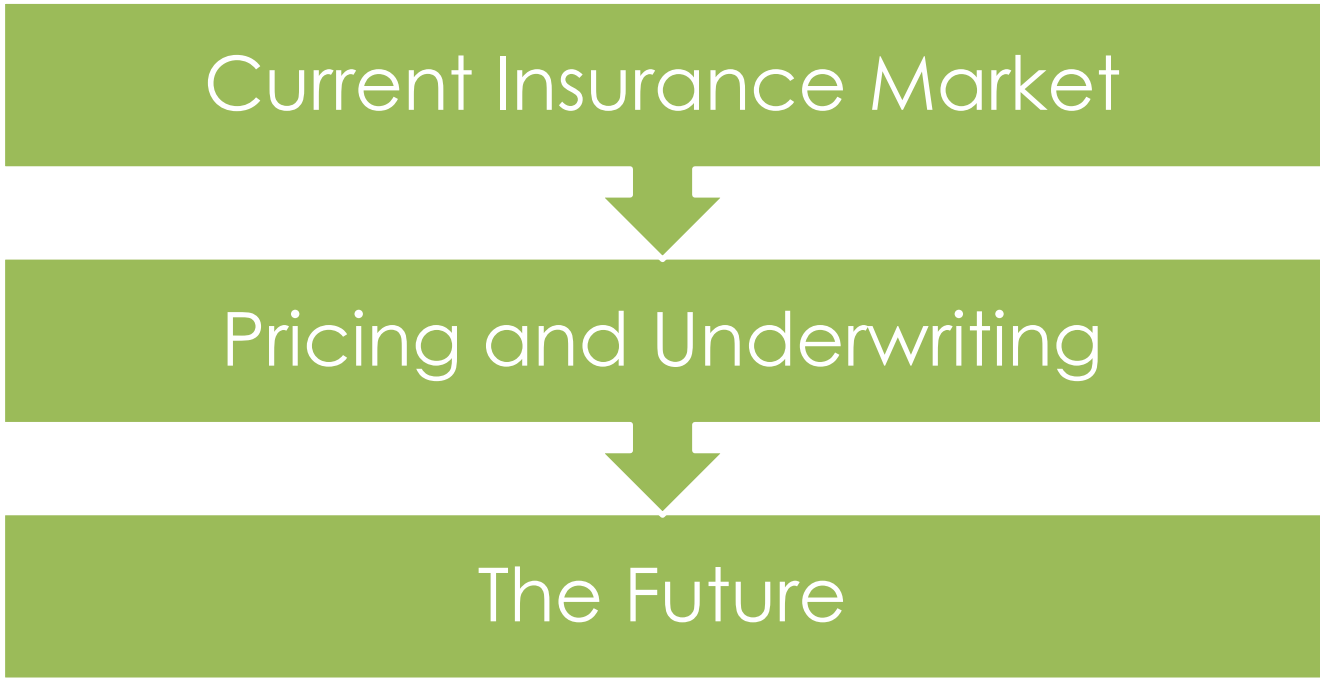
3 August 2016 • Sydney

Actuaries Institute

Cyber Insurance – Risk and Opportunities

Susie Amos

Agenda


Current Insurance Market
Pricing and Underwriting
The Future

Where does insurance fit in?

Insurance is one piece of cyber risk management

GI Glimpse

Actuaries Institute

Russian hackers hold Gold Coast doctors to ransom

By Sara Hicks

Updated 11 Dec 2012, 8:47am

China blamed after ASIO blueprints stolen in major cyber attack on Canberra HQ

Updated 28 May 2013, 7:51amTue 28 May 2013, 7:51am

Hobart airport website hacked with 'pro-Islamic militant messages'

Updated 13 Apr 2015, 12:08pm

Private health insurer nib leaks customers' private details

June 22, 2015

Comments 10

Read later

Cyber attacks: pharmacies, patient records targeted 'ransomware' attacks

By technology reporter Jake Sturmer and Alison McClymont

Updated January 17, 2014 17:27:49

Dominos data hacked, ransom demanded

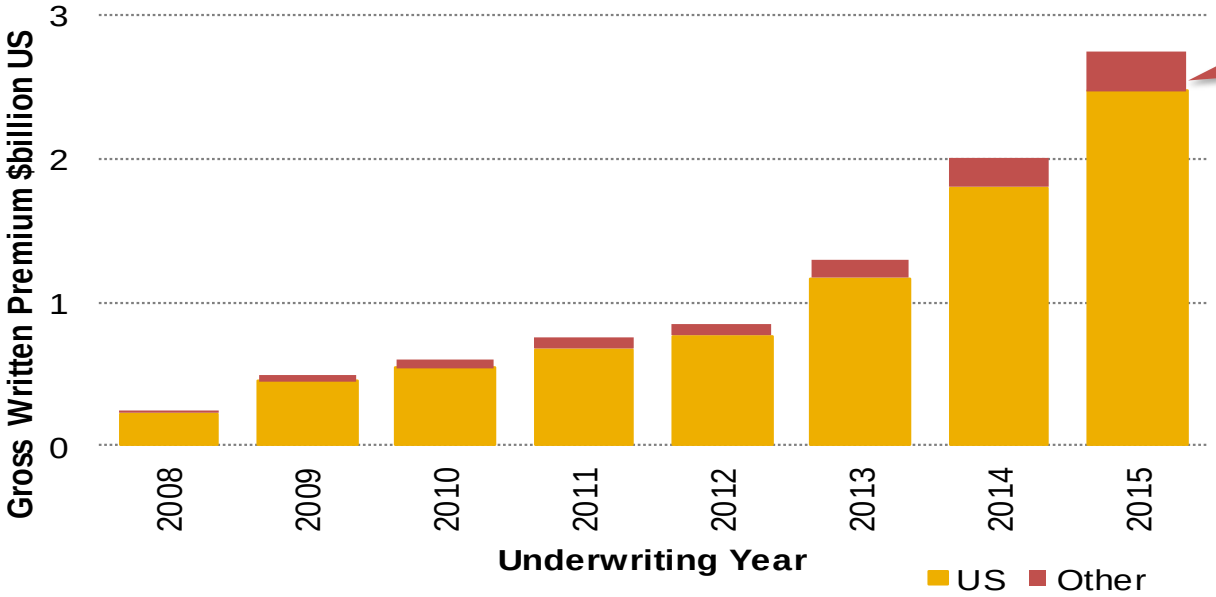
June 17, 2014

Comments 1

Current Insurance Market

Market Size

Global Cyber Premium is $2.5 billion

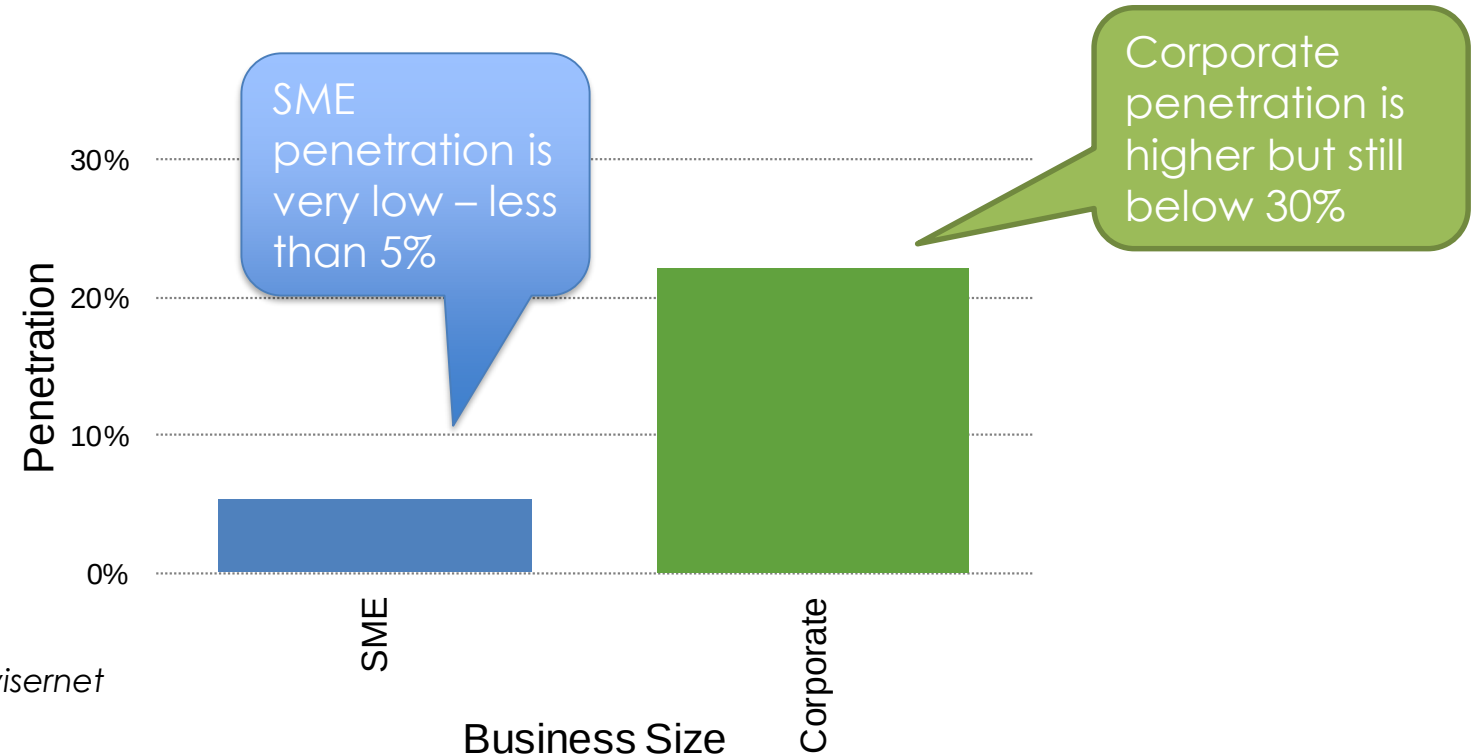


Australian GWP is estimated to be **10 million (AUD)**

Annual growth over 30% over the last 3 years

Market Penetration – US

Lots of opportunity for more growth

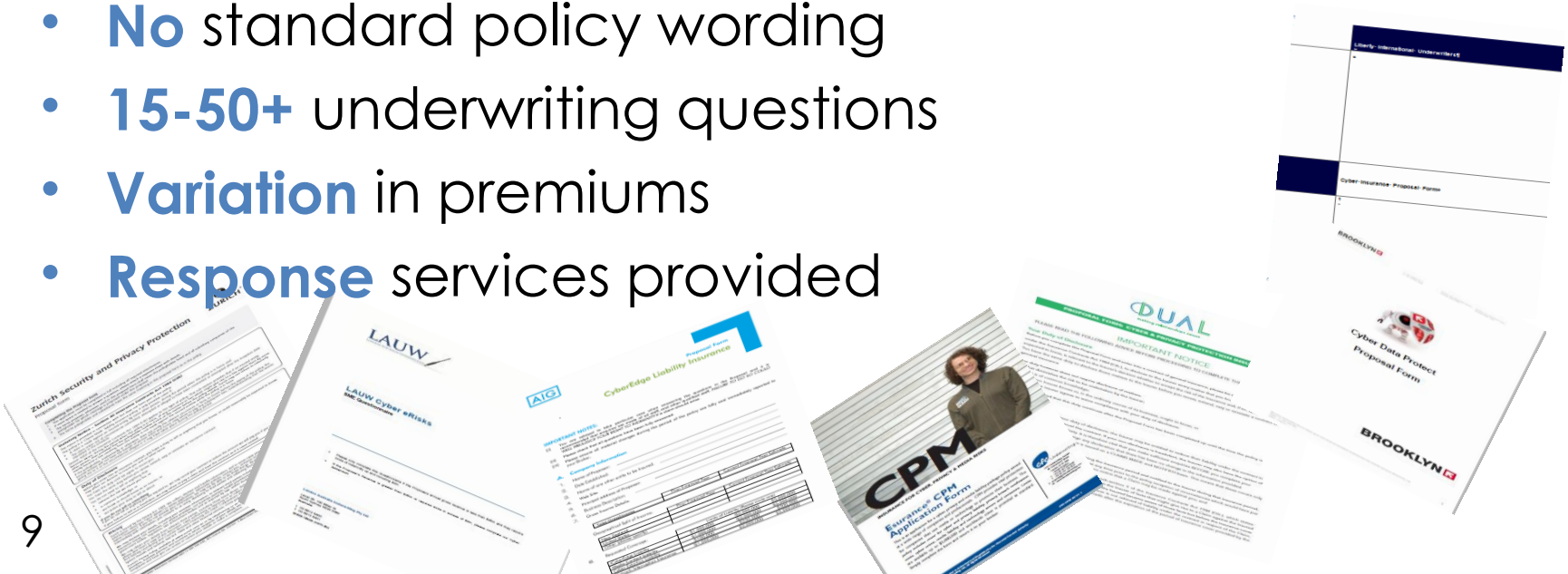


Source: Advisernet

Insurance Offerings in Australia

still in its infancy …

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



Cyber Coverage

Cyber fills some gaps

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	✗	✗	✗	✗	✗	?	✓
Property Damage	✗	✗	✗	✗	✗	?	?
Third Party							
Data Privacy Liability	✗	✗	?	?	?	✗	✓
Media Liability	✗	?	?	?	?	✗	✓
Network Security Liability	✗	✗	✗	✗	?	✗	✓

Legend

✗ Not generally covered

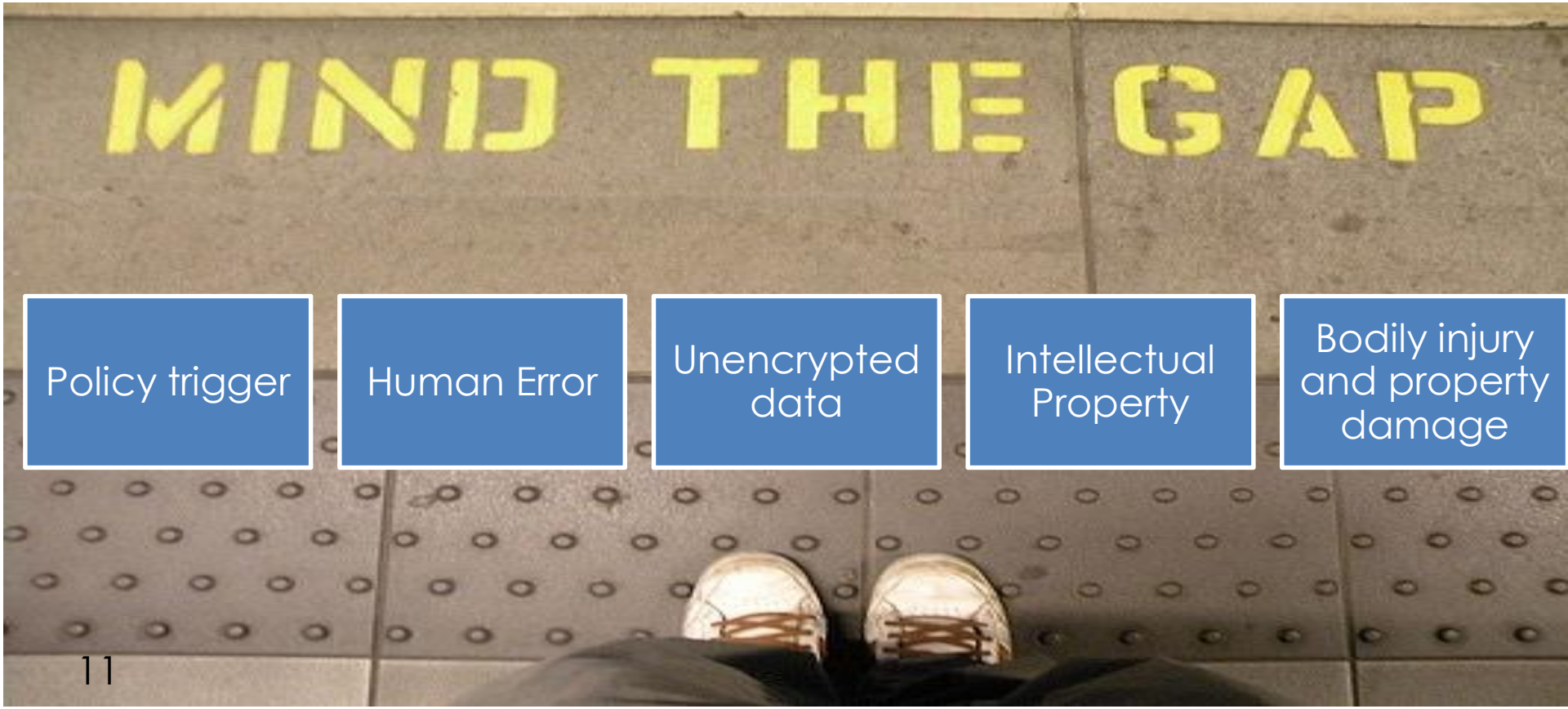
✓ Covered

? Uncertain or varied coverage

* *Some policies do not have cyber exclusions*

Cyber Coverage Gaps

Some Gaps Remain



- Policy trigger
- Human Error
- Unencrypted data
- Intellectual Property
- Bodily injury and property damage

Pricing and Underwriting

Sorry

No Data Available

Underwriting Questions

3 main sources of risk

Profile

Activities

Prior Incident History

Quality

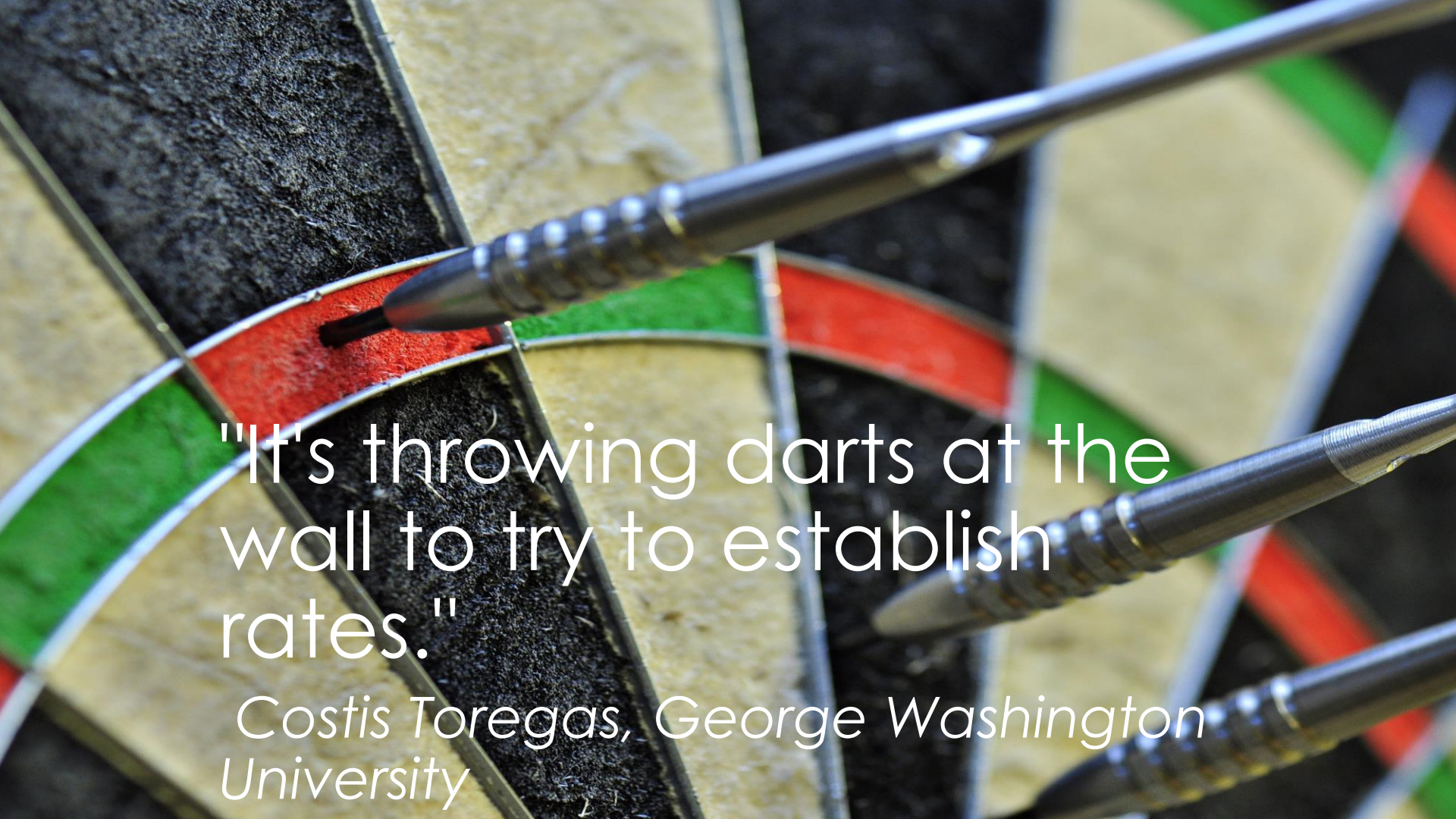
Leadership, Culture and Governance

Incidence Response / Business Continuity Plan

IT

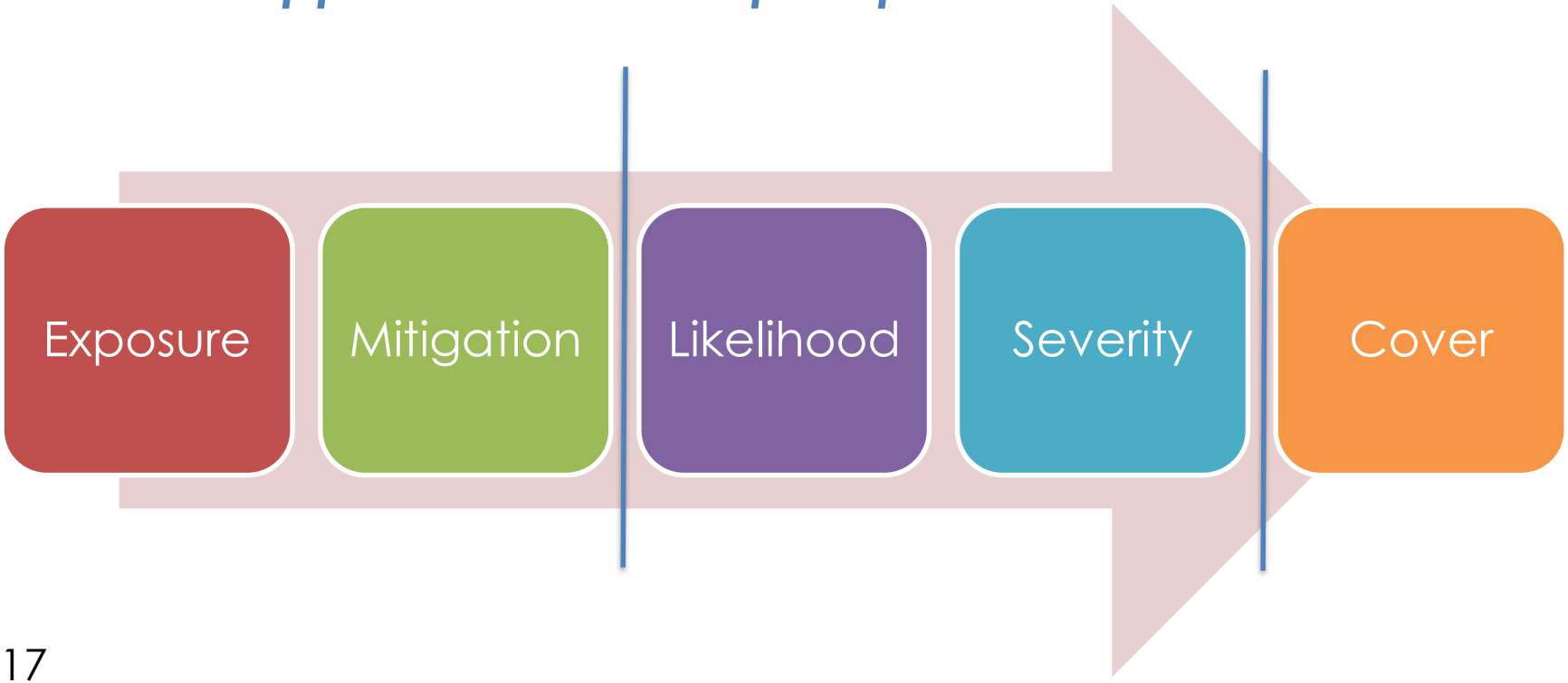
Network Security

Data Management


"It's throwing darts at the wall to try to establish rates."
Costis Toregas, George Washington University

Underwriting and Pricing Framework

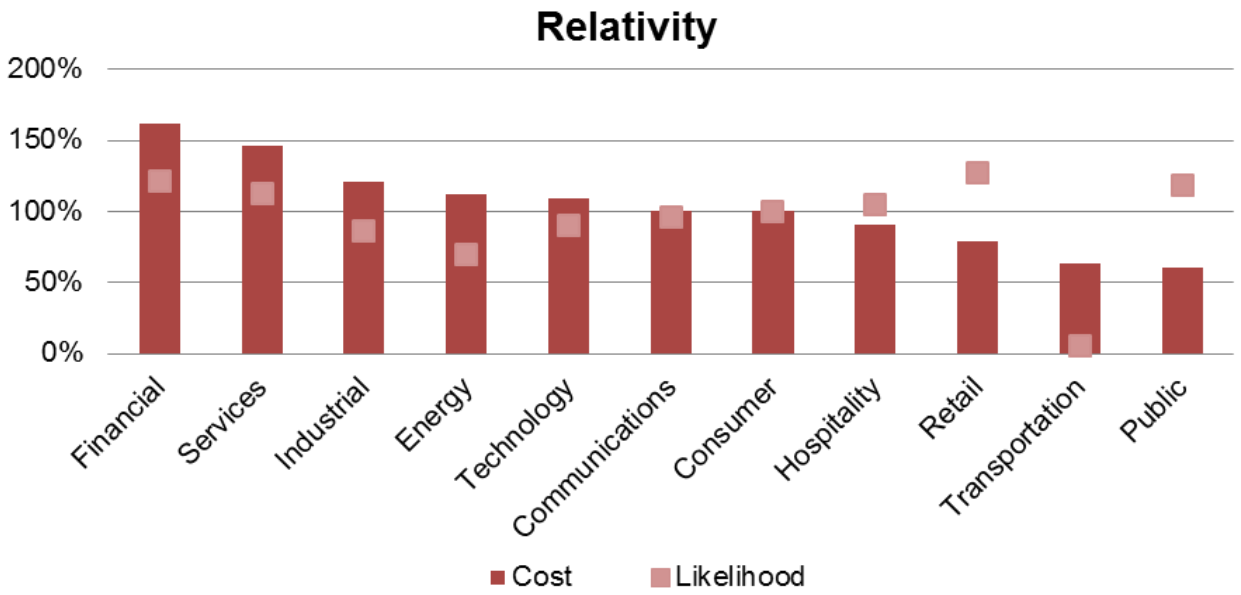
Traditional approach to a complex problem



Industry Frequency and Severity

Exposure

- **Industry**
- Size
- # Records
- Geography
- Online
- Outsourcing

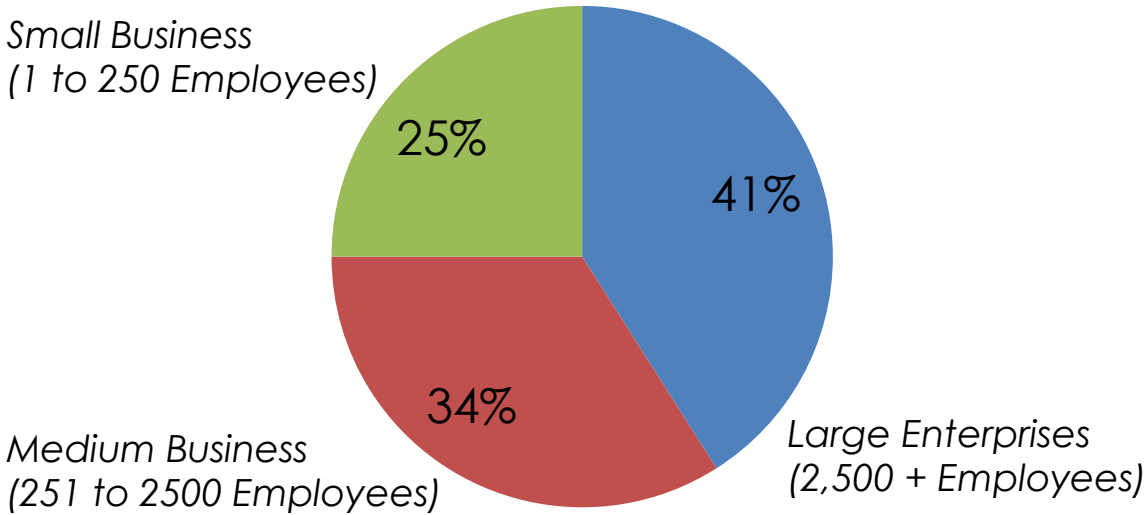


Ponemon Institute 2015 Cost of data Breach Study: Australia

Size

Exposure

- Industry
- **Size**
- # Records
- Geography
- Online
- Outsourcing

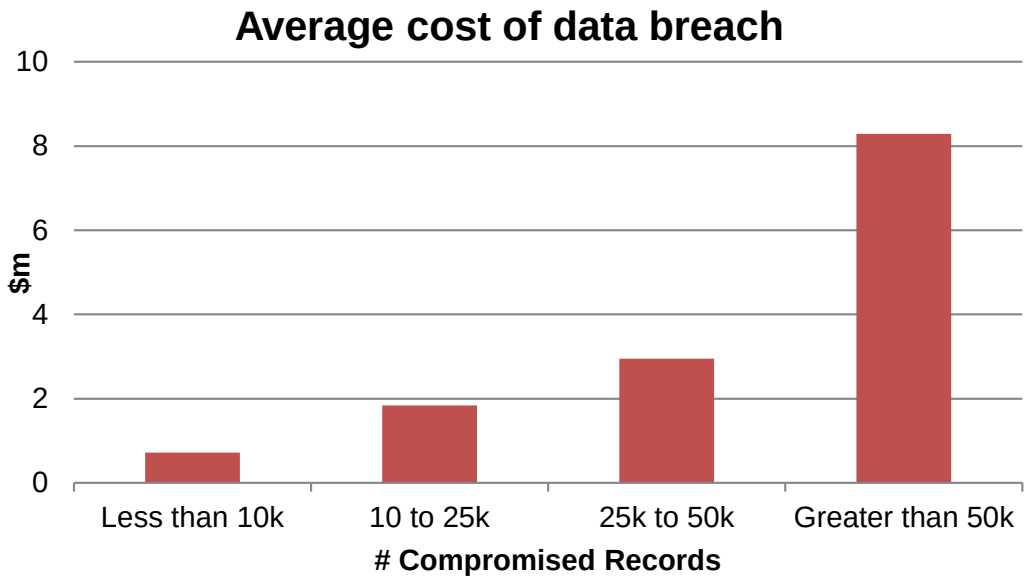


Source: Internet Security Threat Report 2015

Number of records

Exposure

- Industry
- Size
- **# Records**
- Geography
- Online
- Outsourcing



Ponemon Institute 2015 Cost of data Breach Study: Australia

Exposure

- Industry
- Size
- # Records
- **Geography**
- **Online**
- **Outsourcing**

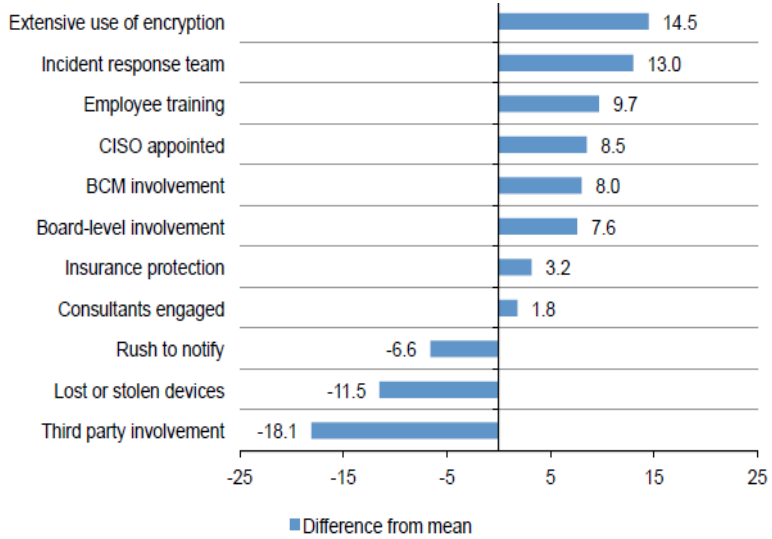
Mitigation

Mitigation

- Leadership, Culture and Governance
- Incidence Response / Business Continuity Plan
- Network Security
- Data management

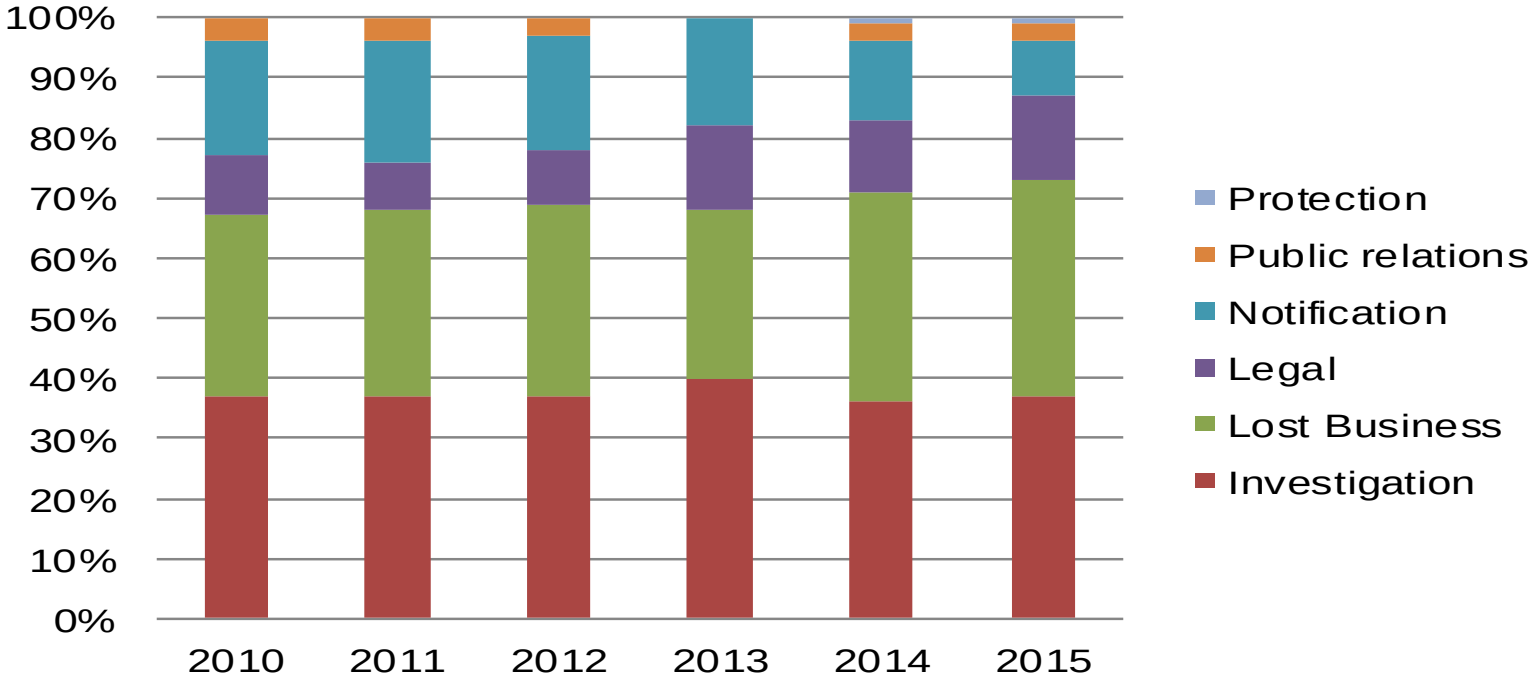
Qualitative assessment

External provider 'Security vulnerability' score



Cover

Investigations and Lost Business are key



Large losses & Accumulations

Cyber Large Losses & Accumulations

Important but difficult to assess

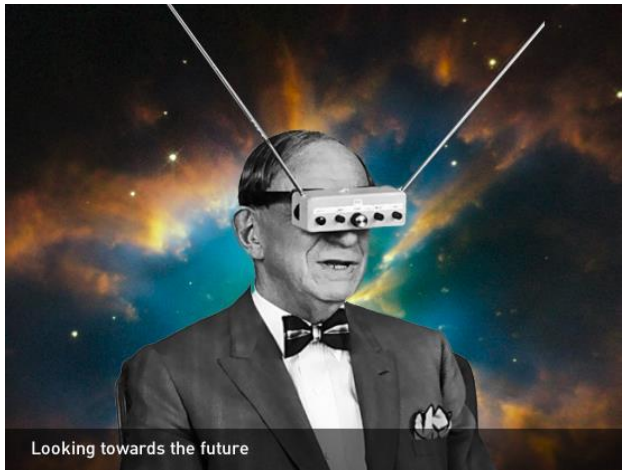
Single large loss

- Power grid outage
- GPS System of a major airline
- Major investment firm is hacked

Accumulation

- Cloud service provider
- Software
- Denial-of-Service Attack
- Cyber extortion

The Future



The Future


Mandatory Reporting
Constantly new threats
Take-up
Streamlining
Mainstream coverage