Institute and Faculty of Actuaries

Cyber Risk Working Party

Understanding the impact of cyber risk on insurer capital

Dani Katz
Keat Ang
Paul Klumpes
Yves Colomb
Madhu Acharyya
Patrick Meghen
Ramiz Mohammed
Rory Egan
Ryan Rubin
Rishav Bajaj
Christopher Rhodes
Jasvir Grewal

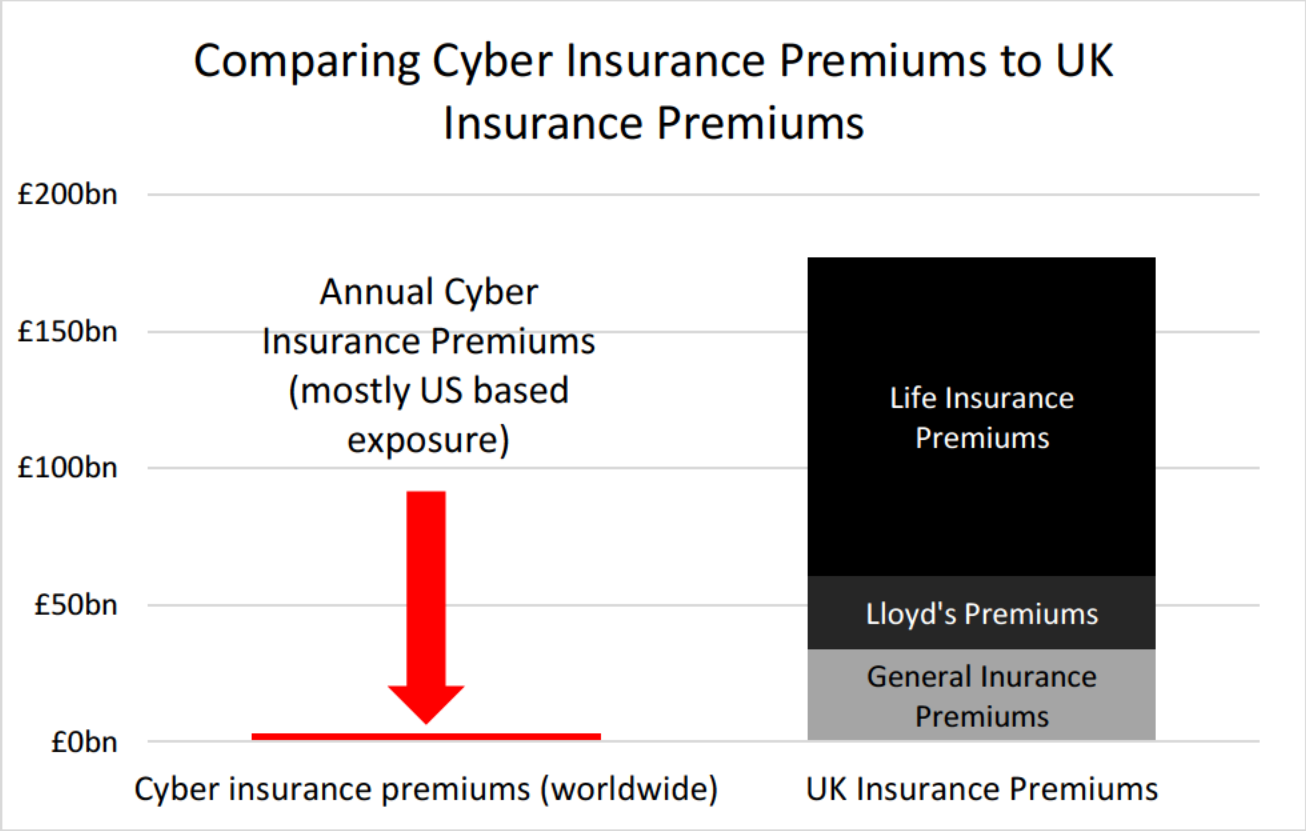
Introduction

- The IFoA Cyber Risk Working Party was set up the IFoA Enterprise Risk Management research committee to investigate operational cyber risk for insurers.
- Currently, cyber risk capital is held within insurers' operational risk capital as an implicit allowance. Given the growing size of the potential risk, it needs to be understood better.
- The aim of the Working Party is to:
  (1) Provide a resource base for actuaries to learn more about the operational risk faced by insurers, and the potential impact if a cyber event occurred in their company.
  (2) Create a better measure of capital required, and risk mitigation steps available.
  (3) Ensure the emerging threats and risk mitigation activities are understood by risk management actuaries.

Institute and Faculty of Actuaries

Cyber Operational Risk, not Cyber Insurance Risk

- The working party is focused on the operational risk carried by insurers as operational capital in their Solvency II capital calculations.



Institute and Faculty of Actuaries

What contribution can actuaries make?

- The subject of cyber exposure and protection is seen as IT led. However, this often ignores the financial component, resulting in misallocated spend.
- Actuaries can provide a financial approach to this problem and are doing this already by (1) allocating insurers' operational capital and (2) developing cyber insurance products.
- There are many areas where actuaries can help:
  - Identify where risk exposure is highest.
  - Help insurers model cyber risk capital, enabling better measures of the benefits and return from cyber risk mitigation spend.
  - They can advise on the benefits of cyber insurance products.
  - Focus spend on mitigation measures where the capital and exposure capital are outside of risk appetite.

Institute and Faculty of Actuaries

Setting the questions to be answered

We felt there were four questions that needed to be investigated by the working party:

1. What make an insurer more exposed to a cyber risk event?
2. What type of cyber events are possible?
3. What is the potential size of the loss for an insurer from a cyber risk event?
4. What can be done to prevent or mitigate the effects of a cyber risk event?

We will be arranging cyber risk sessions at upcoming IFoA events.

Institute and Faculty of Actuaries

1. What make an insurer more (or less) exposed to a cyber risk event?

Institute and Faculty of Actuaries

Insurers have been exposed to cyber attacks

Security

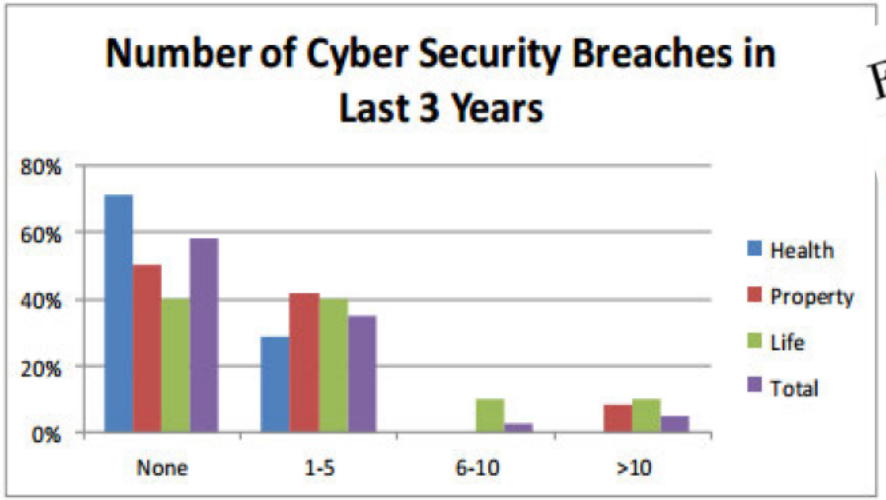
Quotemehappy? No, I'm furious: Insurance site loses customer details

And one-time TalkTalk victims are really unhappy with the help on offer

16 Feb 2016 at 17:00, Alex...

16

SCAN Health Plan notifies 87,000 after cyber attack



http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf

Institute and Faculty of Actuaries

Cyber risk exposure can be highly uncertain

- Mostly personal data breaches
  - *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service"* [Source: Information Commisioner's Office]
- For the UK
  - Estimated £27 billion yearly for all UK companies [Detica 2011]
  - £8.5m "average annualized cost of cyber crime" in the UK Financial Industry in 2015 [Ponemon Institute] up from £3m in 2012
- Globally, speculative estimates up to 5+ times known events of $100+ billion [Centre for Strategic and International Studies, June 2014]

Need to manage exposure besides estimating potential losses

Institute and Faculty of Actuaries

Possible basic metrics to assess exposure level & vulnerabilities

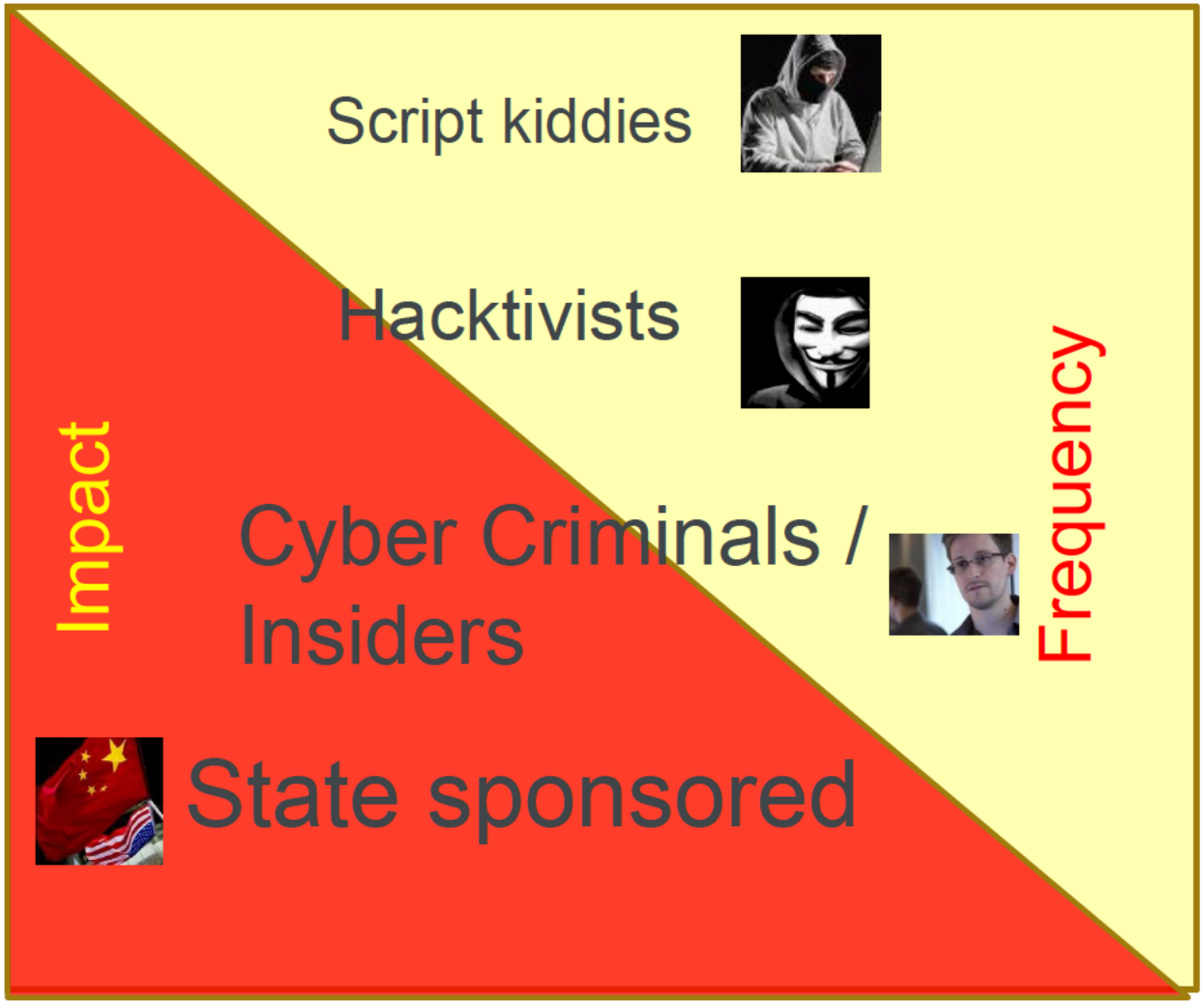
Category	# Authorised Insurers	Volume	Assets under Mgt
General Insurance	903 (incl. 563 passporting)	£34 bn NWP (2014)	~ £100 bn
Lloyd's	84 syndicates	£27 bn GWP (2015)	£25 bn capital, reserves and subordinated debt, and securities
Life Insurers	379 (incl. 179 passporting)		~ £1.8 trn

Firm attributes	General insurance	Life & Pensions	Health
Intellectual property	Insurer vs insurer corporate espionage		
Policyholder information	Multi-billion dollar corporates, High net worth individuals, Fraud on firm	Personal financial information	Personal health and financial information
Processes	Low-key and sustained claims "skimming"	Massive asset portfolio	Low-key and sustained claims "skimming"

Sources:
https://www.abi.org.uk/~/media/Files/Documents/Publications/Public/2015/Statistics/Key%20Facts%202015.pdf
http://www.lloyds.com/annualreport2015/assets/pdf/lloyds_annual_report_2015.pdf

Institute and Faculty of Actuaries

What is the source of the threats?



- This is for all industry sectors combined…can an insurer predict its own threat vectors?
- Are third parties incentivised to tighten security?
- Rely increasingly on IT - double-edged sword
- Op risk capital gives false sense of security?

Institute and Faculty of Actuaries

Useful to consider various control frameworks & checks

NIST Cybersecurity Framework	Cyber Resilience Review	Checks on firm resilience against Cyber Risk

• Identify
• Protect
• Detect
• Respond
• Recover
	• Asset Management
	• Controls Management
	• Config and Change Management
	• Vulnerability Management
	• Incident Management
	Service Continuity Management
	• Risk Management
	• External Dependencies Management
	• Training and Awareness
	• Situational Awareness
		• Acknowledge threats exist
		  • WHEN not IF
		• Holistic risk management
		  • Context & Data intelligence
		  • Not just policy & penetration tests
		• Are insurers willing and able to share relevant information?
		  • How can losses be modelled?
		• Regulatory risk
		  • Solvency 2 ORSA
		  • GDPR

NIST National Institute of Standards and Technology

COSO

2. What type of cyber events are insurers exposed to?

Institute and Faculty of Actuaries

Cyber events due to organisation failures

Event type	Description	Evidence	Examples
Actions of people	Intentional – fraud, theft, unauthorised activity Unintentional – human error	Causes 62% of all incidents ICO Q1 2016	Anthem data breach 2015
Systems and technology failures	Insufficient investment IT Over-reliance legacy Deficiencies in data loss protection controls	ICO increase fines for IT systems failure	Staysure fine £175 for IT failure ICO 2015
Failed internal processes	Deficient governance Incompetence Non-compliance Business continuity plan	AP insurers x6 exposed to malware (Cisco 2015)	Accendo Insurance error 2011

Institute and Faculty of Actuaries

Cyber events due to frictional risks

Event type	Description	Evidence	Examples
External events	Untargeted attacks Targeted attacks	Causes 8% of all incidents ICO Q1 2016 (vs 58% TL)	Han Hai Shu Trojan attack FT 2016
Clients, business practices	Privacy issues Over-reliance big data Financial intermediaries	EU NIS Directive implemented 2016	Quotemehappy data breach 2016
Outsourcing, 3rd party sharing	Systemic share systems Over-reliance 3rd parties Deficiency legal docs	FCA investigates GI market 2015	Quinn Insurance collapse and its aftermath IE 2015-16

Institute and Faculty of Actuaries

3. What is the potential size/extent of losses that could result for an insurer from a cyber risk event?

Institute and Faculty of Actuaries

How do you calculate the cost of cyber crime?

Direct expenses result from the direct expense outlay to accomplish a given activity. These can include engaging forensic experts and other consultants, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services.

Indirect costs result from the amount of time, effort and other organisational resources spent, but not as a direct cash outlay. Examples include in house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

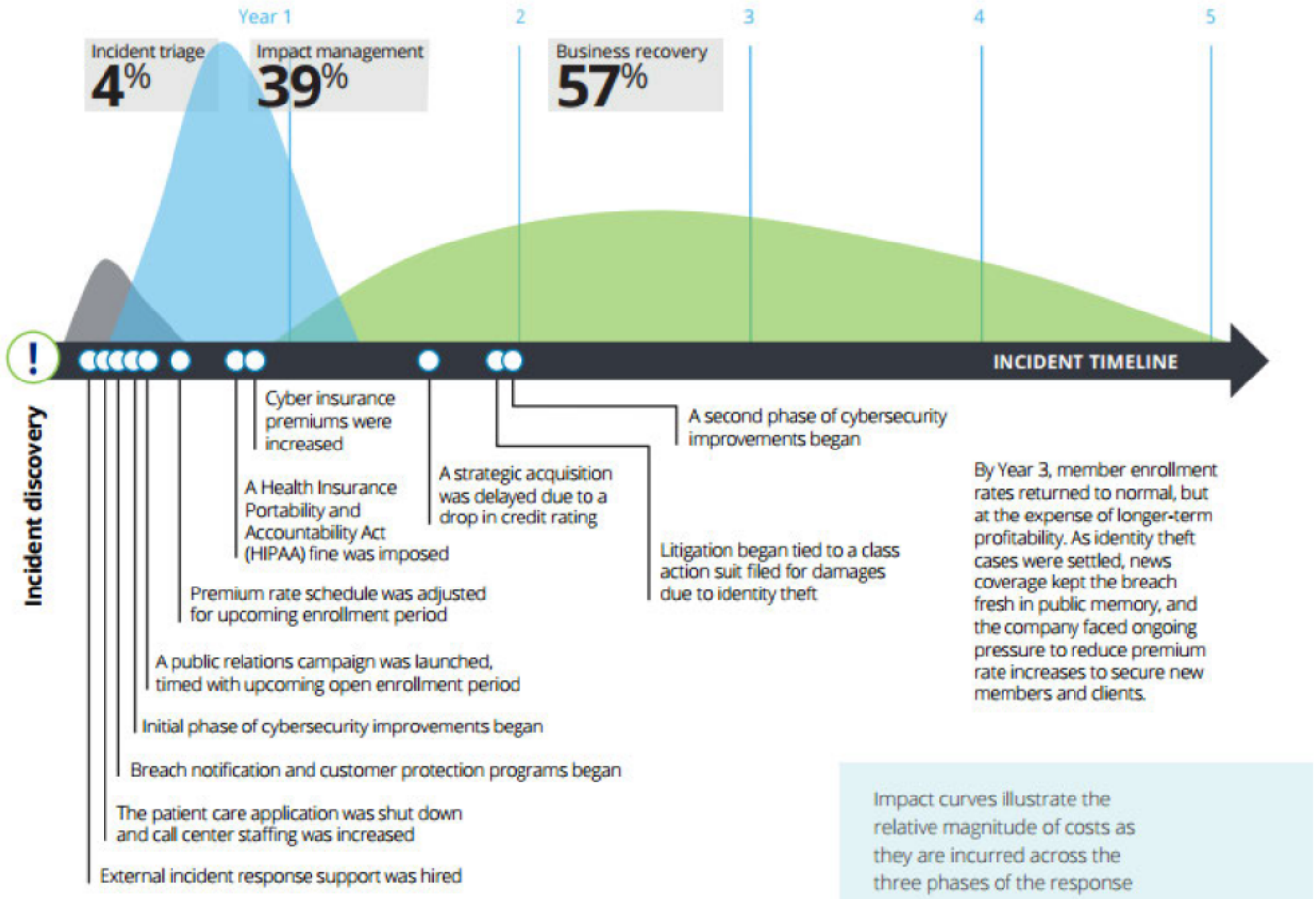
Opportunity costs results in from diminished trust or confidence by present and future customers. Negative publicity associated with cyber incidences can cause reputational damage, that result in lower renewal rates, as well as a diminished rate for new customer acquisitions.

Source: Ponemon Institute

Institute and Faculty of Actuaries

Cyber Attack Costs - Timeline

Scenario A: Cyber incident response timeline—how the events and impacts unfolded



Source: Deloitte

Institute and Faculty of Actuaries

Data Breach Case Study – Anthem Background

American Health Insurance company with nearly $80bn global turnover, $2.56bn net income as at 2015

- Hackers gained access to over 80m personal data records
- First party costs alone reported to be well in excess of $100m
- Number of class action law suits have been filed
- E&O Tower reported to expect losses (no precedent for such claim yet)
- Government fines are highly likely
- Possible cost data breach? **Could be a significant % of global revenue!**

Source:
Insurance Insider: 11/02/2015
Anthem Key Facts: http://www.antheminc.com/NewsMedia/FrequentlyRequestedMaterials/StatsFacts/index.htm
Anthem Income: https://en.wikipedia.org/wiki/Anthem_Inc.
Target facts: http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx
CSO Online: http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html

Institute and Faculty of Actuaries

Modelling Approach through Operational Risk

- Process Map
  - Benchmark on Industry Loss Data
  - Allow for some key drivers of risk
    - Revenue Size
    - Location
    - Insurance vs Other Financial Institutions
    - General (Commercial & Personal) vs Life
  - Size of tail?

Institute and Faculty of Actuaries

4. What can be done to mitigate the effects of those losses, either through internal prevention measures, exiting sensitive lines of business or purchasing insurance?

Institute and Faculty of Actuaries

Key risks and mitigants

	Risks leading to Cyber security attacks	Mitigants
1	**Lack of accountability and investment in security** results in insecure organisational culture, policies and practices	• **Raise Board/C-suite awareness** – accountability, potential fines, D&O claims, case studies of security threats etc. • Understand top business risks and how cyber risk can impact them – prioritise remediation based on risk appetite and business impact. • Use risk register and capital allocation to track cyber risk via adding cyber explicitly in the internal controls model to shine a light on it.
2	**Lack of perimeter security controls** leads to successful external attacks	Reduce external exposure by **implementing IT controls / processes** such as multi-factor authentication, access rights processes, security monitoring, vulnerability management, firewalls, intrusion detection, email filtering, anti-virus software, segmentation, proxies, mobile device management etc.
3	**Poor employee cyber awareness** leads to security policy breaches	**Training platforms**, sharing lessons learnt, phishing scenario testing, advice around security of physical IT access, straight-forward phishing and error reporting processes
4	**Poor vendor management** / supplier management	Vetting of vendors and regular review/reset of vendor IT access rights is important. **Vendor risk assessment programmes** need active management.
5	**Poor data protection processes** and data governance	• **Categorise internal data by importance/sensitivity and implement standards accordingly**, e.g. protect PCI, PHI, PII, other highly sensitive data e.g. M&A details, K&R clients. • **Define and implement data governance strategy** to establish policies, accountability and suitable data protection measures • **Exit sensitive lines** / vendor relationships e.g. K&R, Healthcare, M&A
6	**Poor response to incidents** and post-incident management	**Incident response procedures** including planning, testing, IT forensics / investigation, client notification, PR/media communications, threat hunting

Cyber insurance as a risk mitigant

- **Risk assessment:** Identify key business processes and information assets that require protection/cover
- **Risk quantification:** Quantify inherent exposure to key risks through scenario analysis
- **Risk appetite:** Establish management's appetite for cyber risk management
- **Risk mitigation**: Weigh up **IT investment vs cyber insurance costs** – determine how to combine risk mgmt. and risk transfer for best outcome
- Which cyber insurance to buy?
  1. Pure financial loss coverage vs broader risk solutions:
     - Consider pro-active solutions beyond pure risk transfer e.g. risk assessment/threat monitoring/incident response/crisis management and other consulting services
  2. Analyse existing (non-cyber specific) property/casualty policies held
     - Is cyber explicitly included/excluded or implicitly included (silent coverage)
     - Consider a cyber specific policy
  3. Look at breadth of coverage closely under the cyber policy (primarily direct costs only)
     - Typical coverage: privacy breach costs, data loss, incident response, extortion
     - Sometimes: Business interruption, regulatory fines, reputational damage
     - Less common: Contingent BI, IP theft, Physical damage, bodily injury

Institute and Faculty of Actuaries

Traditional Insurance Vs Cyber Insurance

Although traditional insurance policies may offer the option to cover some specific areas related to cyber risk, they are not designed to fully cover all potential costs and losses. Cyber insurance policies, on the other hand, provide a variety of coverage options and pre-conditions that need to be considered when purchasing cyber insurance.

	General Liability	Property	E&O\D&O	Crime	Cyber
Network Security	+	+	+	+	✓
Privacy Breach	+	+	+	+	✓
Media Liability	+		+		✓
Professional Services	+		+	+	✓
Virus Transmission	+	+	+	+	✓
Damage to data	+	+	+	+	✓
Breach Notification	+		+	+	✓
Regulatory Investigation	+		+	+	✓
Extortion	+		+	+	✓
Virus/Hacker attack	+	+	+	+	✓
Denial of service Attack	+	+	+	+	✓
Business Interruption Loss		+	+		✓

+ Possible ✓ Coverage

Source: Deloitte

Institute and Faculty of Actuaries

5. An Industry Perspective

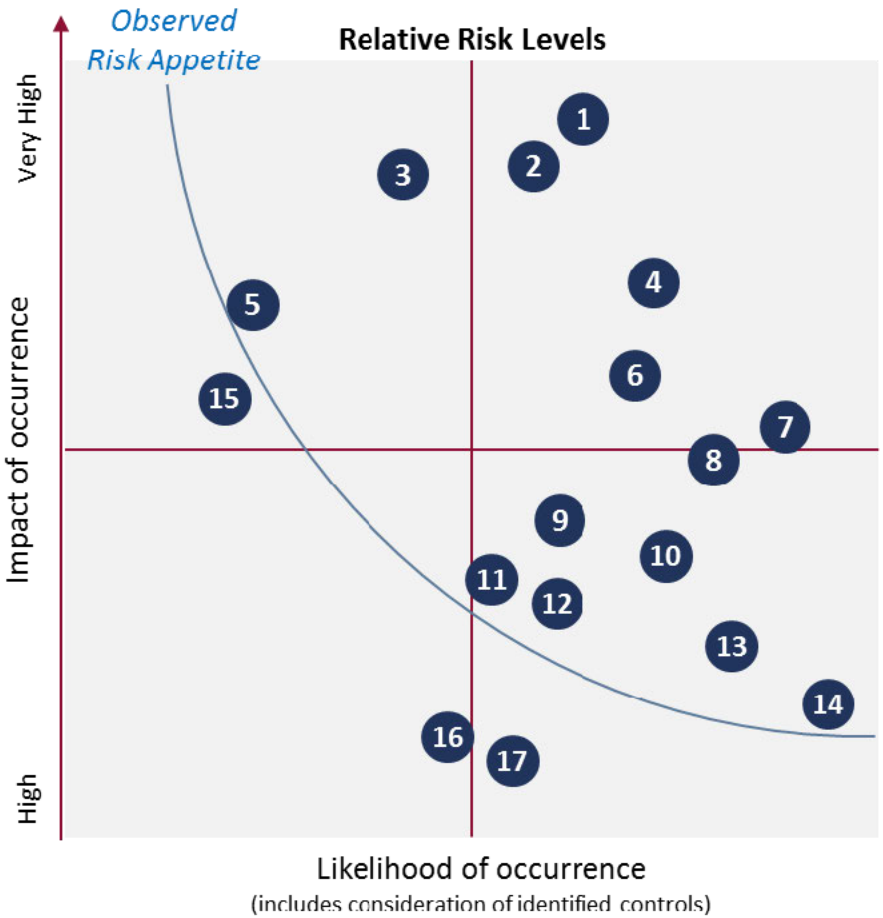
Institute and Faculty of Actuaries

Understanding Risk Appetite

Where on the continuum does your organisation perceive they are and where do they want to be ? The answer to this is critical for either over or underspending on Cyber Security and also remember Cyber Security is a business risk and should be managed as such.

Institute and Faculty of Actuaries

Risk Appetite Case Study



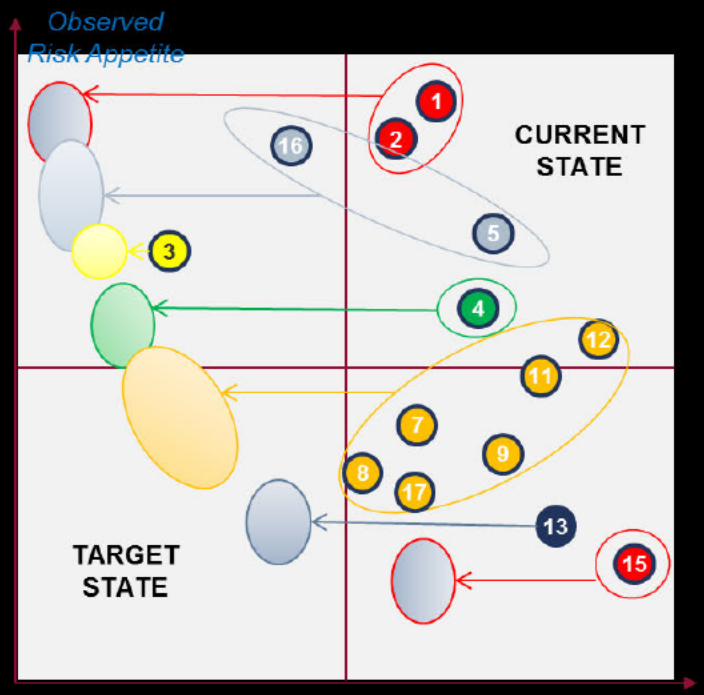
Legend: Cyber Risk Impact

C – Confidentiality
I - Integrity
A – Availability
R - Regulatory

#	Business Outcome – (source of risk)
1	Loss of Client Data (Internal, External)
2	Inability to Calculate Pricing (Internal)
3	Unable to Transact Online (External)
4	Unauthorised payments to Suppliers (Internal)
5	Stolen credit card data (Internal, External)
6	Fraud in Electronic claims process (Internal)
7	Errors in Capital Adequacy Model (Internal)
8	Stolen Healthcare Records (Internal, External)
9	Business process failure due to IT (Internal, External)

Institute and Faculty of Actuaries

Prioritising Remediation



Remediation	A Critical Systems taken offline	B Critical Data Deleted / Manipulated	C Fraudulent Payments	D Inappropriate / unauthorised transactions	E Sensitive Information Disclosure
Enhance Policy Framework	X	X	X	X	X
Change Organisation	X	X	X	X	X
Education and Training	X	X	X	X	X
Privileged Access	X	X	X	X	
Identity & Access Management	X	X	X	X	X
Access Management			X	X	X
Sensitive Data Access		X	X	X	X
Segregation of Duties			X	X	X
Logging & Monitoring	X	X			X
Data Loss Prevention					X
Vulnerability Management	X	X			X
Malware Management	X	X			X

Next Steps

- Running 6 months -> still more to do
- Continued research for each of the 4 questions
- Obtaining further data and analysis
- Sharing results with the Community

- PLEASE PROVIDE FEEDBACK AND CONTRIBUTE

Institute and Faculty of Actuaries

Questions / Feedback

Working Party Members	
Dani Katz	Ramiz Mohammed
Keat Ang	Rory Egan
Paul Klumpes	Ryan Rubin
Yves Colomb	Rishav Bajaj
Madhu Acharyya	Christopher Rhodes
Patrick Meghen	Jasvir Grewal

Institute and Faculty of Actuaries

Reference Material

Title	Author
Potential Ratings Indicators for Cyberinsurance: An exploratory Qualitative Study (2009)	Innerhofer-Oberperfler, F., R. Breu
Cyber Catastrophe Scenario October 2014	Centre for risk studies
Cyber exposure data schema jan2016	Centre for risk studies
Ponemon Institute - 2015 report	Ponemon Institute
Insurability of Cyber Risk: An Empirical Analysis (2015)	Biener, C., M. Eling and J. Drkd Wirfs
Data in the age of cyber-risk: Cyber-risk insurance – challenges in modelling the risks	Widermann, P
Insuring against cyber risks: A changing landscape (2015)	Andrew Maher and Stuart Packham
Heavy-tailed distribution of cyber-risks (2010)	Maillart and Sornette
Cyber risk and privacy liability: A click in the right direction? (2007)	William J. McDonough
Cyber security: a critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack (2014)	Jason Mallinder and Peter Drabwell
Learn from insurance: cyber bore (2014)	Mainelli, Michael
Cyber Liability: It's Just a Click Away (2014)	Anthony R Zelle; Suzanne M Whitehead
Data in the age of cyber-risk: Cyber-risk insurance – challenges in modelling the risks,	Widermann, P.
Managing Cyber Insurance Accumulation Risk v2	Centre for risk studies
Cyber Governance Health Check report 2015	UK Government

Reference Material – Anthem case

Insurance Insider: 11/02/2015

Anthem Key Facts:
http://www.antheminc.com/NewsMedia/FrequentlyRequestedMaterials/StatsFacts/index.htm

Anthem Income: https://en.wikipedia.org/wiki/Anthem_Inc.

Target facts: http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx

CSO Online: http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html

Institute and Faculty of Actuaries