Institute and Faculty of Actuaries

Cyber Risk

Ryan Rubin & Dani Katz

27 April 2016

Institute and Faculty of Actuaries

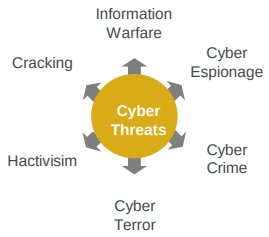
Cyber Risk

What is it? An industry professional's view

27 April 2016

What is Cyber Security?

Data is increasingly getting digitised and internet is being used to save, access and retrieve vital information. Protecting this information is not just a priority, but has become a necessity for most companies and government agencies around the world. Cybersecurity refers to such business function and technology tools used to protect information assets.

Types of Cyber Threats	Methods	Security Measures for Protection
	• Malicious Code such as Viruses, Worms, Trojan Horses • Spyware • Phishing attacks • Spam • Data Theft • Denial-of-Service Attacks • Packet Spoofing	• Access Controls • System Protection • Incident Reporting • Continuity Planning • Physical & Environmental Protection • Communications Protection • Personal Security • Legal Compliance

Institute and Faculty of Actuaries

Sources: Secondary Research

Categories of Cybercrime

Cybercrime describes a variety of attacks and activities, they can be broadly classified into 3 categories -

Business Disruption and Misuse | Online Scams | Theft and Fraud

- Denial-of-Service (DOS) or Distributed Denial-of-Service (DDoS) Attack
- Malware or Malicious Software
- Software and Information Piracy
- Industrial Espionage
- Cyber Extortion / Randsomware

Source: Using Insurance to Mitigate Cybercrime Risk

Institute and Faculty of Actuaries

Categories of Cybercrime

Cybercrime describes a variety of attacks and activities, they can be broadly classified into 3 categories -

Business Disruption and Misuse | **Online Scams** | Theft and Fraud

- Phishing
- Spear Phishing
- Pharming
- Spoofing
- Purchase Fraud

Source: Using Insurance to Mitigate Cybercrime Risk

Institute and Faculty of Actuaries

Categories of Cybercrime

Cybercrime describes a variety of attacks and activities, they can be broadly classified into 3 categories -

Business Disruption and Misuse | Online Scams | **Theft and Fraud**

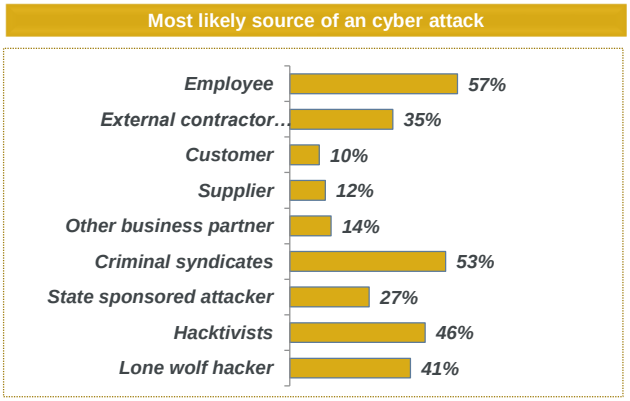
- Identity Theft
- Theft from Business
- Intellectual Property (IP) Theft
- Customer Data Theft
- Fiscal Fraud

Source: Using Insurance to Mitigate Cybercrime Risk

Institute and Faculty of Actuaries

Source of Cyber Attacks

The attacking power of criminals is increasing at an astonishing speed. Attackers have access to significant funding; they are more patient and sophisticated than ever before; and they are looking for vulnerabilities in the whole operating environment — including people and processes.



Source: EY

Breaking news!

"Combined external attackers now significantly more likely as a risk source than internal threats"

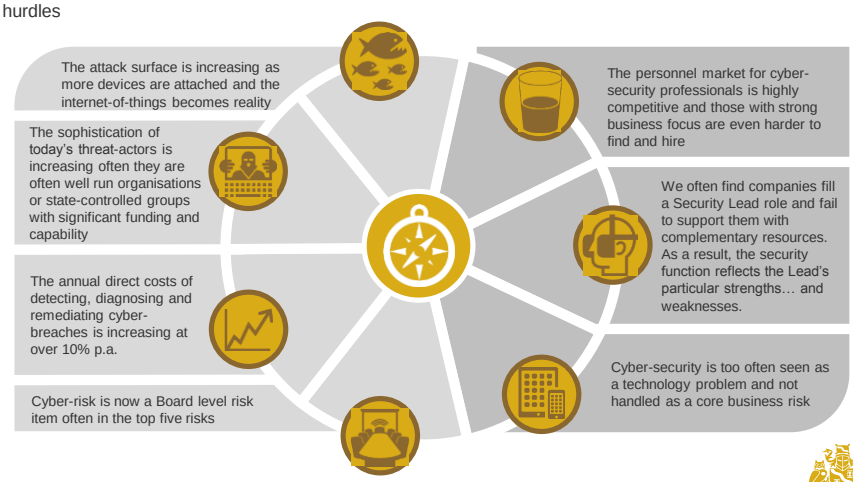
"Its not a matter of if an attack will happen it's a matter of when"

"Internal attacks are most likely but are least thought through from a defense perspective"

Institute and Faculty of Actuaries

The Cyber Security Challenge

Organisations are now faced with a challenging cyber-threat environment exacerbated by operational hurdles



Institute and Faculty of Actuaries

Protiviti View On Cyber Security

Most organisations have to change their approach and management of cyber- security: starting at the very top and shifting it from the technology agenda

Traditional approaches to cyber-security are not working …

- A **risk based approach** needs to be adopted: a one size fits all approach is all too often adopted and is not practical, too costly and will ultimately fail
- **Top down ERM** approach to security risk assessments is essential, identifying sensitive data, assessing threats, capturing risk appetite, and informing risk mitigation strategies
- 'Intelligent' security **monitoring** techniques that highlight abnormal behaviour or potential incidents and enable a real time response are increasingly important
- **People** are often the weakest link: security awareness training that works is essential

… and most organisations struggle to answer five key questions

- Do you know the **value** of your data?
- Do you know **where** your data is?
- Do you know **who** has **access** to this data?
- Do you know **who** is **protecting** the data?
- Do you know **how** to **respond** in case the data is compromised?

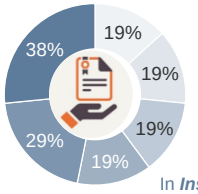
Institute and Faculty of Actuaries

What is Cyber Risk ?

'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

Cyber risk could materialize in the following ways:

- Deliberate and unauthorized breaches of security.
- Unintentional or accidental breaches of security.
- Operational IT risks due to poor systems integrity or other factors.



- Confidential records (trade secrets or IP) compromised or stolen
- Customer records compromised or stolen
- Financial fraud
- Unauthorized access/use of data, systems, networks
- Financial losses
- No incidents

In ***Insurance services***, 29% of the cases reported were due to ***Financial Losses***.

Institute and Faculty of Actuaries

Source: Allianz, PWC

Typical Cyber Risk Scenarios for Insurers

Below are example risk scenarios for Insurers

- Reputational Damage
- Loss of Confidential Data
- Financial Damage
- Fines from Regulators
- Data Privacy breach
- Lack of Availability
- Integrity of Data
- Breach of Contract
- Third Party Impact
- .....

Institute and Faculty of Actuaries

Sources: Secondary Research

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		+	+		✓

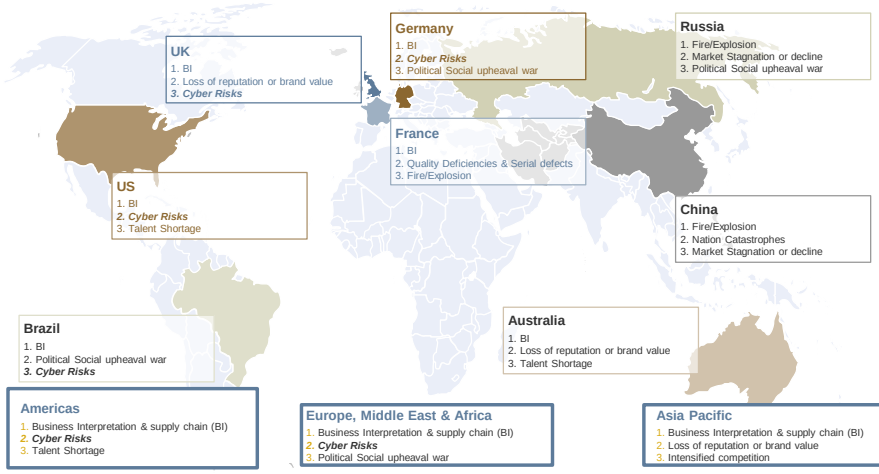
+ Possible ✓ Coverage

Source: Deloitte

Institute and Faculty of Actuaries

Top Business Risks Around The World

This risk map shows the top risk for businesses per geographical region and in selected countries. It also shows the main changes in risk perception across these territories year-on-year.

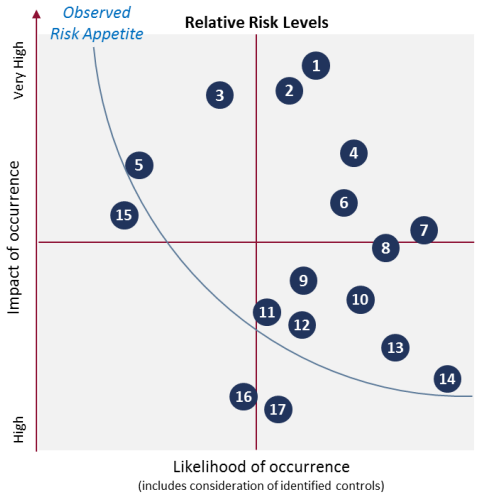


Institute and Faculty of Actuaries

Source: Allianz

Risk Appetite Case Study

IMPACT KEY:
C = Confidentiality
I = Integrity
A = Availability

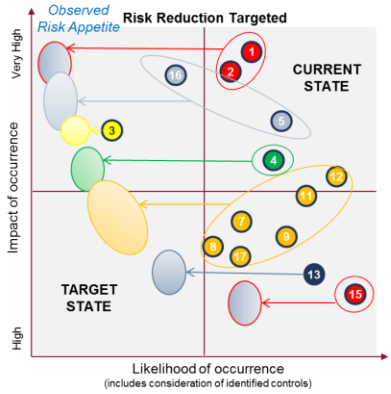


Risk Scenario Descriptions

#	Risk Scenario Description (Primary Threat Actors*)	Impact		
		C	I	A
1	Critical systems are taken offline. (OI, SA, WM)			✓
2	Critical business system A taken offline. (OI, SA, WM)			✓
3	Incorrect or malicious manipulation of data in financial losses. (OI, WM, SA)		✓	
4	Billing system and backups are maliciously deleted. (OI, SA)		✓	✓
5	Unauthorised (or unintended) trades executed. (OI)		✓	
6	Fraudulent payments made by an insider. (OI)		✓	
7	Private internal electronic communications disclosed externally. (WM, OI)	✓		
8	Board papers or committee meeting papers are disclosed externally. (WM, OI)	✓		
9	Personnel remuneration information is disclosed internally or externally. (WM, OI)	✓		
10	Customer contact details, contract terms, pricing and margin information stolen. (OI)	✓		
11	Sensitive contracts disclosed externally. (WM, OI)	✓		
12	Sensitive tax policies, data and related information are disclosed externally. (WM, OI)	✓		
13	Inappropriate or unauthorised journals are posted in Finance System. (OI)		✓	
14	Websites or externally facing applications are compromised. (UA, SA)	✓	✓	✓
15	Fraudulent payments made caused by an external party (e.g. using Phishing). (UA, SA)		✓	
16	Large transactions under negotiation are disclosed externally. (WM, OI)	✓		
17	Counterparty / customer contracts / pricing/terms disclosed externally. (WM, OI)	✓		

Institute and Faculty of Actuaries

Prioritising Remediation



KEY:
= Entity level activities
= Primary risk reduction
= Secondary risk reduction

Remediation Projects	A Critical Systems are compromised or taken offline	B Critical data is incorrectly deleted or manipulated	C Fraudulent payments transactions	D Inappropriate or unauthorised journals posted	E Disclosure of sensitive information	F Unauthorised trading
	Risk Scenario Categories					
Enhanced policy framework	●	●	●	●	●	●
Organisational enhancements	●	●	●	●	●	●
Education & Awareness	●	●	●	●	●	●
Privileged Access Management	✓	✓	✓	✓	✓	-
Identity and Access Management	✓	✓	✓	✓	✓	✓
SAP Sensitive Access and SoD	-	-	✓	✓	-	-
Trader SoD	-	-	-	-	-	✓
Security Risk Management	+	+	+	+	+	-
Data Loss Prevention	-	-	-	-	✓	-
Logging & Monitoring	✓	✓	+	+	✓	-
Network Security Enhancements	✓	+	-	-	+	-
Vulnerability Management & Malware	✓	✓	-	-	✓	-
Incident Management Enhancements	+	+	+	+	+	-

Institute and Faculty of Actuaries

5

Key Messages

- Traditional approaches to Cyber Security are not working
- Many tools available for assessing your Current state and remediating gaps
- All organisations will be subject to attacks and/or security incidents and the frequency and sophistication of these events is increasing
- Insurers need to assess and report on whether the organisation is focused on the right risks and solving the real problems
- Boards and Senior Management need to be supported, educated and more honest about risk appetite
- Cyber Security should be factored into everything we do
- The organisation must implement a risk based strategy that reflects true risk appetite and has a chance of success
- Insurers should ensure they are really prepared to respond and deal with an attack

Institute and Faculty of Actuaries

16

Institute and Faculty of Actuaries

Cyber Risk Working Party

Introduction

Cyber Risk Working Party – What is it all about?

- The Cyber Risk Working Party emerged from the Institute of Actuaries Risk Management Research Sub Committee in response to requests for more information.
- The aim of the working party is to **provide insight** to actuaries working on capital requirements for insurers.
- We will be researching cyber risks for insurers, working alongside industry experts to get a better understanding of the **nature of the risk** faced by insurers, the **size of the potential loss** and the **risk mitigating options** available to insurers.

Institute and Faculty of Actuaries

Topics to be covered

- The working party will address the following topics:
  1. What makes insurers unique from a cyber risk perspective?
  2. Description of potential cyber risk scenarios for insurers
  3. Thoughts on operational risk capital requirements
- The starting point is to clarify what cyber risk is.
  - Given the breadth and variety of cyber risks faced, it was important to create a taxonomy of risk outcomes.
  - It is also important to draw a boundary between other operational risks and cyber risk.

Institute and Faculty of Actuaries

19

Understanding why insurers are unique

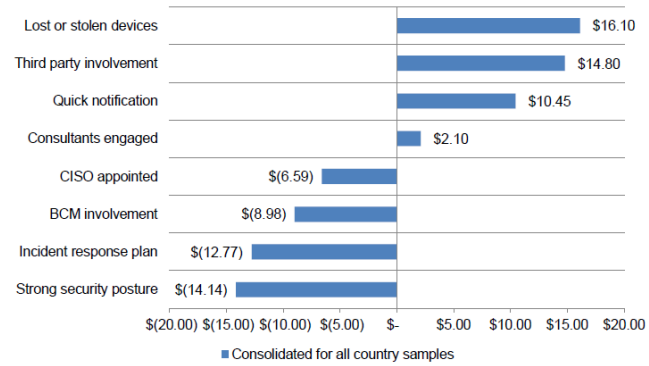
- Insurers have a number of features that are attractive to cyber criminals, and create exposure to cyber risks:
  - They tend to hold large customer databases with very detailed and often sensitive information about their customers.
  - They manage a large percentage of UK assets (insurers in the UK control £1.9trn of assets).
  - They have large volumes of annual transactions that are exposed to cyber attack.
  - They have legacy systems which can date back many years due to the term of many of their policies.

Institute and Faculty of Actuaries

20

Risk mitigating actions are available

Figure 9. Impact of eight factors on the per capita cost of data breach



Source: Ponemon institute report, 2014

Institute and Faculty of Actuaries

Next steps

- The Cyber Risk Working Party has been set up recently, and will be meeting monthly.
- We will produce regular updates on our research at upcoming events, and welcome any inputs and recommendations.
- We plan to publish reading lists for actuaries wanting to learn more.

Institute and Faculty of Actuaries

Questions

Comments

Expressions of individual views by members of the Institute and Faculty of Actuaries and its staff are encouraged.

The views expressed in this presentation are those of the presenters.

Institute and Faculty of Actuaries