Institute and Faculty of Actuaries

Cyber Risk

Simon Cartagena, SCOR
Justyna Pikinska, Capsicum Re

16 April 2019

Cyber Working Party Representatives

Simon

- SCOR UK Risk Management
- 4 years Cyber modelling
- Current focus on cyber accumulations – affirmative and non-affirmative

Justyna

- Head of Analytics Capsicum Re Brokers
- 2.5 years cyber modelling
- Current Focus – pricing, reserving, accumulations

Institute and Faculty of Actuaries

Agenda

1) Overview

- Cyber Insurance Losses
- Attacker Motivations
- Threat Vectors

2) Pricing & Reserving

- Evolution of Cyber Product Offering
- Data for Pricing Cyber Risks
- Insured Claims and Trends

3) Capital

- Operational Risk
- Cyber Catastrophes
  - Affirmative
  - Non-affirmative
  - Internal vs Vendor solutions

4) Q&A

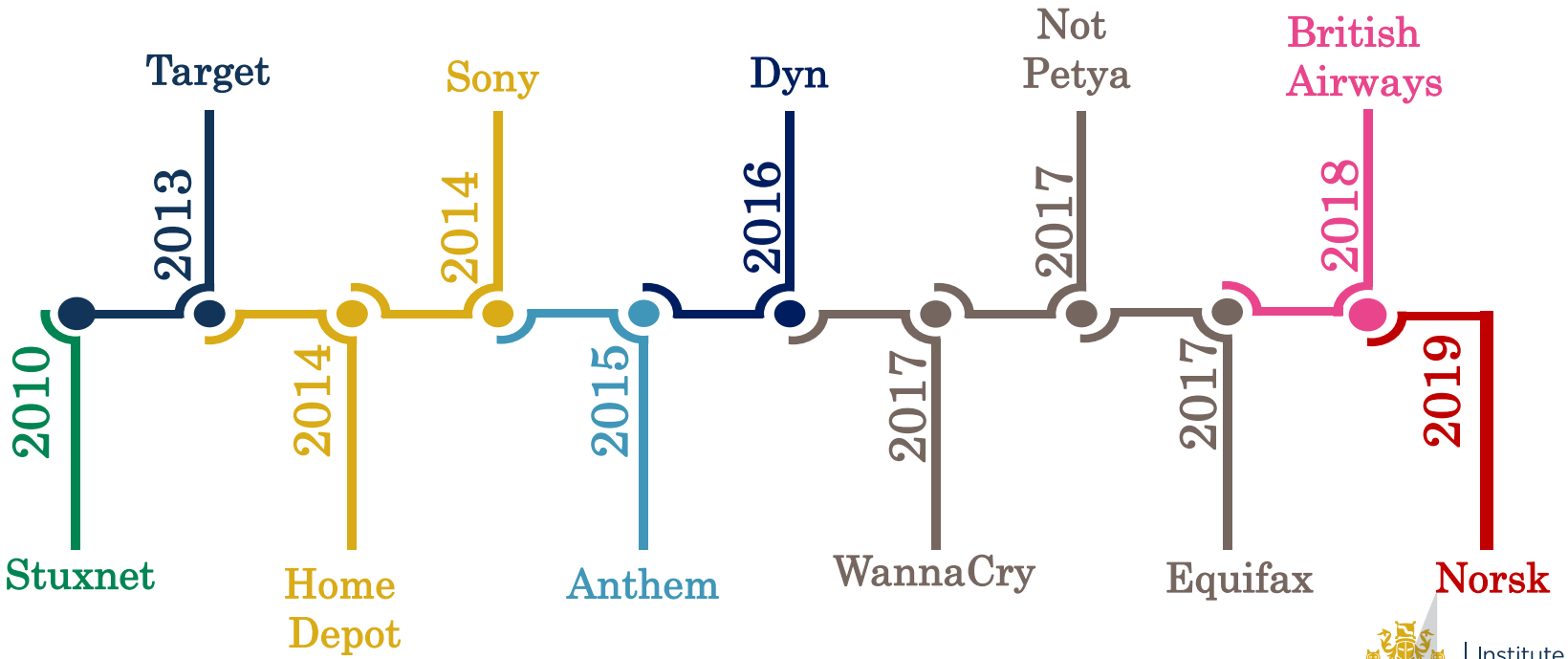
Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Overview

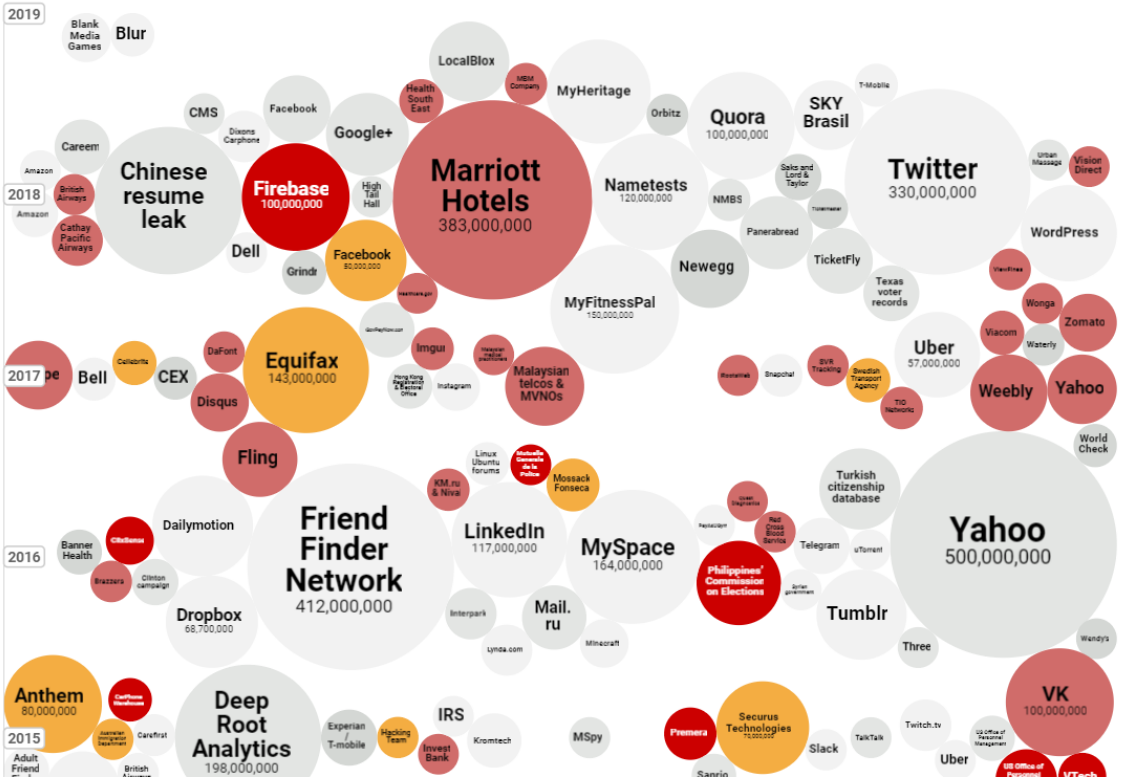
16 April 2019

Cyber Events



Institute and Faculty of Actuaries

Data Breaches



Increasing trend in frequency and severity of data breaches?

If so why?
Easier?
More resources?

How much can this information inform quantification?

Does the past adequately reflect the future?

Institute and Faculty of Actuaries

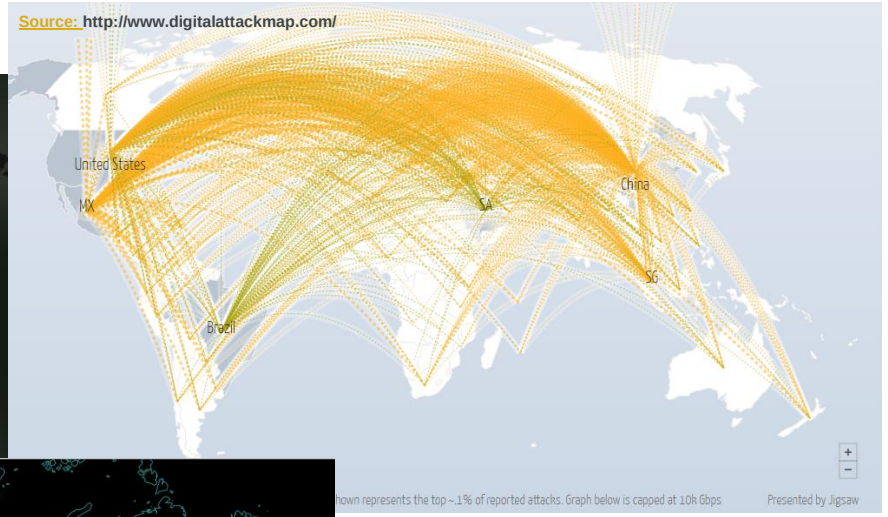
Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cyber Threats Are Global

Kapersky Live Attack Map

Source: https://cybermap.kaspersky.com/

DDOS Live attacks



Institute and Faculty of Actuaries

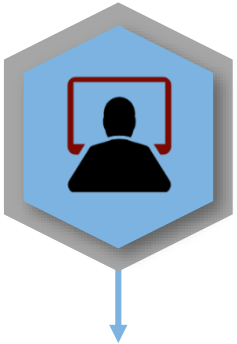
Attacker Motivations

Malicious Insider

- Dispute
- Vengeance
- Data Manipulation

Serious Organized Crime

- Theft of PII
- Credit Card Theft
- Theft of IP
- Ransomware
- DDoS
- Corp. Espionage
- Extortion

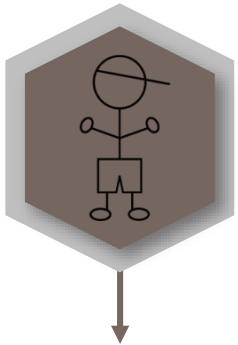


State Sponsored Group

- Theft of PII
- Theft of Secret Intelligence
- Cyber Warfare
- DDoS
- Sabotage

Extremist Groups

- Publicity
- Recruitment
- Widespread Disruption
- Espionage
- Sabotage

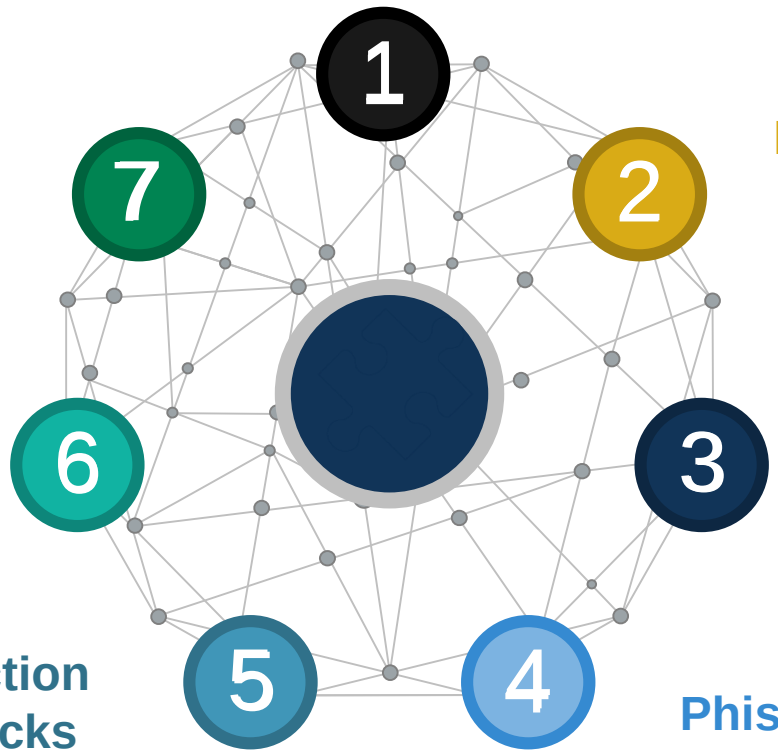


Opportunists / Script Kiddies

- Impress friends
- Gain credit in computer communities
- Unauthorized Entry
- DDoS

Institute and Faculty of Actuaries

Threat Vectors



1. Man-in-the-middle
2. Removable Media
3. Social Engineering
4. Phishing
5. Injection Attacks
6. Malware
7. Drive-by-Download

Institute and Faculty of Actuaries

Risk Landscape

TOP 5 RISKS IN FINANCIAL SERVICES

Source: Allianz Global Corporate & Specialty.
Responses: 515

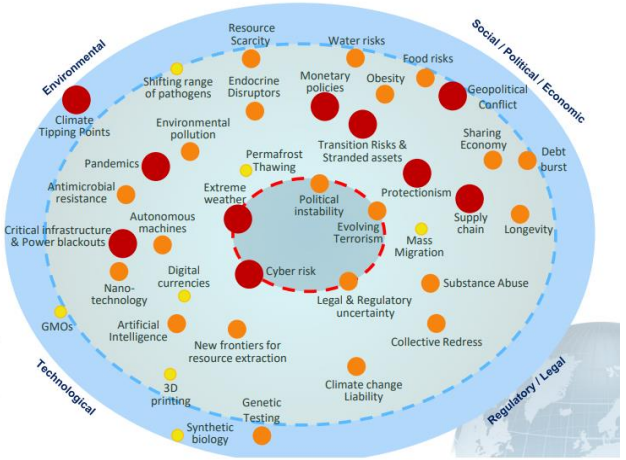
1. **Cyber incidents (e.g. cyber crime, IT failure, data breaches)**
2. Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)
2. Market developments (e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)
4. Business interruption (incl. supply chain disruption) **NEW**
5. New technologies (e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones) **NEW**

TOP RISKS IN THE UK

Source: Allianz Global Corporate & Specialty.
Respondents: 104
Responses: 116

1. **Cyber incidents (e.g. cyber crime, IT failure, data breaches)**
2. Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)
3. Business interruption (incl. supply chain disruption)
4. Loss of reputation or brand value

CRO FORUM



Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Pricing & Reserving

Justyna Pikinska

16 April 2019

Development of Cyber as a Product - Coverage

Historical

- ✓ **Privacy Breach**
- ✓ **Cyber Crime & Fraud**
- ✓ **Data and Software Loss**
- ✓ **Extortion**
- ✓ **Operational Error**

Historical coverages continue to be enhanced with service panels to mitigate losses and improve cyber risk management.

Recent

- ✓ **Business Interruption/CBI**
- ✓ **Network Failure**

In recent years coverage has expanded to focus on **BI/CBI** as demand increases, risk modelling matures and losses materialize in this area.

Current

- ✓ **Cyber Physical Damage**
- ✓ **Physical BI with Cyber Peril trigger**
- ✓ **Reputational Harm**

Coverage continues to expand to other lines of business with a cyber peril trigger. Increasing concern surrounding **Silent Cyber** driving growth in this area as the affirmation process happens. Expansion to cover other intangible assets such as Rep Harm.

Near term

- ✓ **Constantly Broadening Coverage**

Changes in waiting period (12h, 8h, $ deductible, franchise)
Operating error originally to unplanned system outage (manufacturers less concerned with privacy exposure)

Long term

- ✓ **Intangible Assets: Rep Harm**

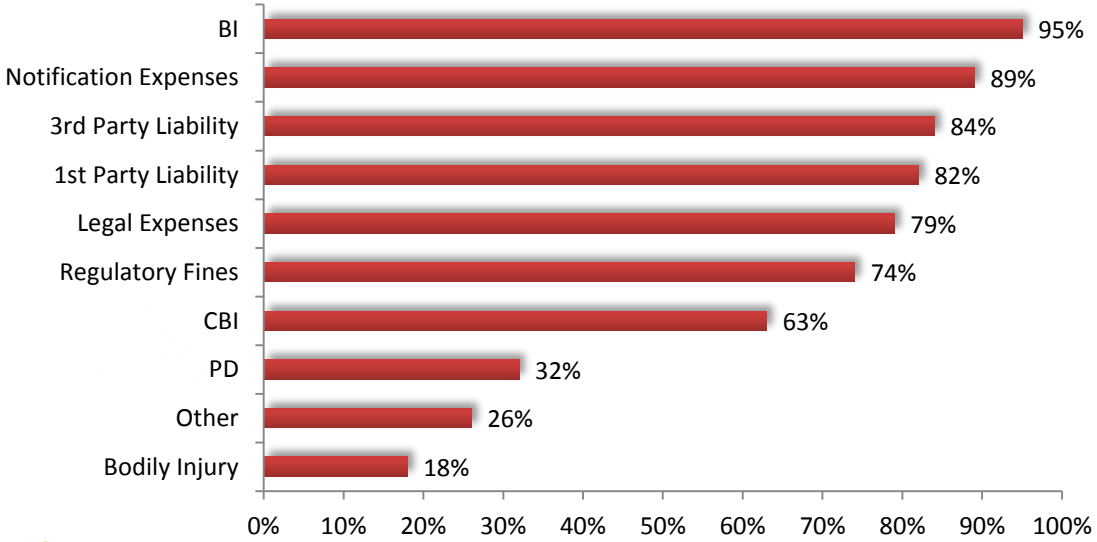
Intangible Assets account for more than 85% of S&P 500 companies. As the importance of Intangible assets continues to grow for companies balance sheets, insurance will need to evolve to protect these assets.

Institute and Faculty of Actuaries

Constantly Broadening Coverage

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Coverage offered by Cyber Products (based on PRA Survey SS4/17, April 2018)



Comments published by the PRA:

- ✓ We have observed a material widening of coverages. Three particular examples include: 1) BI, 2) CBI, 3) Reputational Damage. Although widening cyber coverage is welcome, it should be accompanied by appropriate risk management and controls
- ✓ Cyber stress test results suggest gross losses can run in the multiples of annual cyber premiums
- ✓ Cyber limits are often significant considering relatively low premium and lack of comprehensive claims experience

Institute and Faculty of Actuaries

Pricing using Limited Data

1) Data Collection

- ✓ Identifying cyber policies and cyber premiums in a consistent and easy to manipulate data format, this includes (but not limited to):
  - ✓ **Primary Policy Information (Underwriters)**: Cyber Risk Codes, Limits, Sublimits, Exposures, Coverage, Waiting Period (hrs / $), Sector, Revenue, Geography, Number of Records (PII, PCI, PHI)
  - ✓ **Supplementary data (Outside In Tools)**: Number of open ports, cloud reliance, service providers (DNS, email, payment), CVE (Vulnerable Technologies with NIST framework score), patching cadence risk, other appropriate rating factors, outside-in tool data or equivalent
  - ✓ Online Breach calculators (At-Bay.com; webscan.upguard.com)
  - ✓ Data collection for Cyber is **limited** but the industry is slowly recognising the benefits of better data. Also driven by regulatory / rating agencies requirements

2) Actuarial Analysis

- ✓ Historical Claims analysis
- ✓ Rate change difficult to track (premium volumes growing and do not reflect the year on year change in risk)
- ✓ Recognise differences between: **SME vs Large Risks**; **PD vs BI**, **Malicious hack vs Accidental**; **Tech E&O vs Standalone Cyber vs Casualty** (**mean, volatility, tail risk, development patterns**)
- ✓ Remember about **Cat Load**
- ✓ Consider R&D in Cyber, White Papers, Market Leaders, Counterfactual Analysis, Changes in Coverage

Industry Groups - *Examples*

- ✓ Each industry has very specific exposures that need to be understood in order to build an underwriting picture
- ✓ **Retailers** also tend to have large amounts of **PII related data**

Industry Class Matters

- ✓ Depending upon whether the focus of the insurance is on 3rd Party Liability or 1st Party Coverage
- ✓ **Manufacturers** have high levels of **BI dependency** but in many cases tend to have less PII related information (unless they have an on-line presence)

Hazard Class Rating will differ

- ✓ **Hotels** tend to have franchise arrangements, external management, various staffing arrangements and carry large amounts of **PII related data**

Vendor Reliance

Institute and Faculty of Actuaries

SME vs Open Market

Small Businesses

Attritional

- ✓ Lower Frequency of Breaches, but when a breach does occur, the losses can exceed company revenue and put the company at risk of failure.

Catastrophe

Less reliance on common service providers (cloud, DNS etc.), so a lower risk of CAT aggregation losses. Even if a provider fails their systems seem to be simpler and more easy to move to a backup. The question is whether they have done the proper preparation for such a scenario.

Large Businesses

Attritional

- ✓ Higher Frequency of breaches but the severity of any given breach tends to be lower. Their overall AAL will be higher than SMEs but a lower percentage of their revenues.

Catastrophe

- ✓ More reliance on common service providers leading to a higher risk of aggregation losses. Additionally they tend to have more complex systems making it more difficult to switch providers.

Industry Loss Ratio Considerations

Security Breach Frequency Industry Relativities, by Company Size

Industry	small business								large business	
Agriculture, Forestry, Fishing and Hunting										
Mining, Quarrying, and Oil and Gas Extraction										
Utilities										
Construction										
Manufacturing										
Wholesale Trade										
Retail Trade										
Transportation and Warehousing										
Information										
Finance and Insurance										
Real Estate and Rental and Leasing										
Professional, Scientific, and Technical Services										
Management of Companies and Enterprises										
Administrative and Support and Waste Management and Remediation Services										
Educational Services										
Health Care and Social Assistance										
Arts, Entertainment, and Recreation										
Accommodation and Food Services										
Other Services (except Public Administration)										
Public Administration										

While company size is not a perfect proxy for line size, an assumption has been made that on the whole; larger businesses will purchase greater limits of insurance. Moving from colour Green to Red implies an increasing frequency of breach

Institute and Faculty of Actuaries

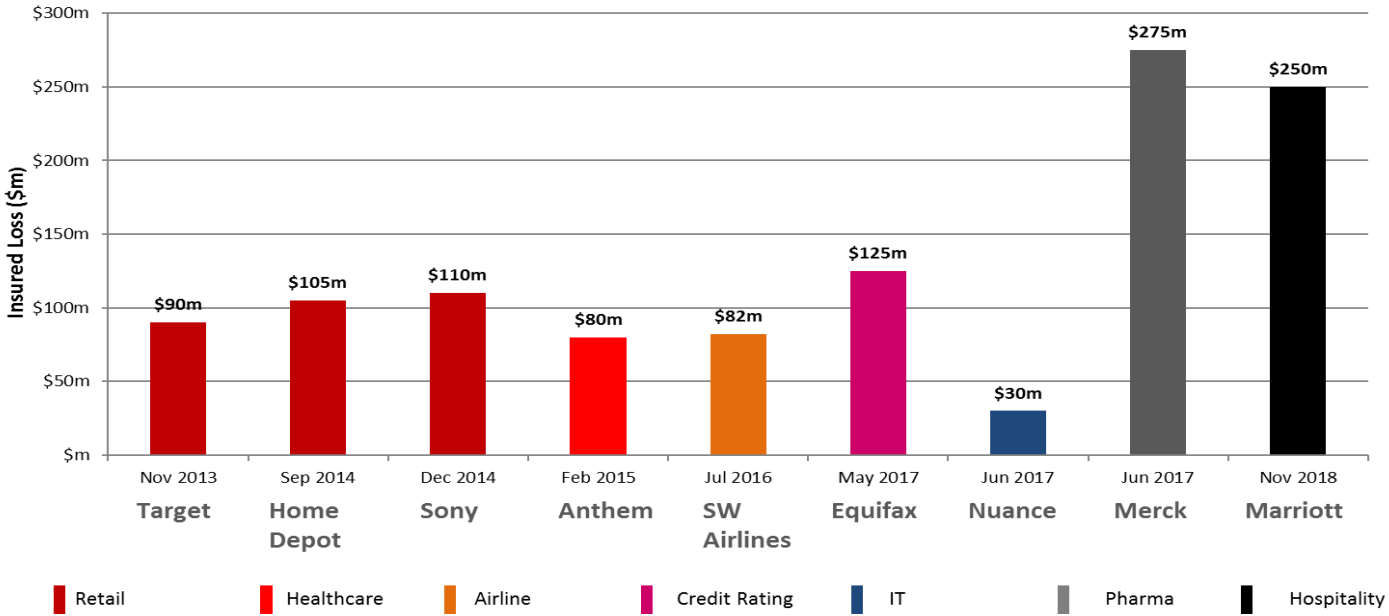
Cyber Claims – Cause of Loss

Source: AIG Cyber Claims Study 2018

AIG

Institute and Faculty of Actuaries

Large Insured Losses since 2013 – Trends



Institute and Faculty of Actuaries

Capital

Simon Cartagena

16 April 2019

From Kill Chain to an Insured Loss

CYBER THREAT

- ✓ **Accidental / Human Error**
  - Security failure (general)
  - System failure
  - Program failure
- ✓ **Malicious Insider / Rouge Employee**
- ✓ **State Sponsored Groups / Government**
- ✓ **Kid in the basement / IT-Geek**
- ✓ **Serious Organised Crime / Terrorist**
- ✓ **Competitor**
  - Hacker attack
  - Malware (Virus, Worm)
  - Social Engineering (Phishing, USB Drop)
  - Cyber Extortion (Ransomware,…)
  - DDoS
  - Disclosure of data

ECONOMIC IMPACT

- ✓ **Consider Industry / Geography / Revenue**
  - Software / Hardware Manipulation
  - Server / Network Outage
  - Loss of control
- ✓ **PD Loss**
  - Loss of machinery
  - Loss of data
- ✓ **BI Loss**
  - Stopped production line
  - Supply chain issues (CBI)
  - Reputational Risk
  - Data restoration
- ✓ **Bodily Injury**

INSURED LOSS

- ✓ **Coverages Triggered**
  - Property Damage (PD)
  - BI / CBI
  - Bodily injury
  - Pure data loss
  - Machinery breakdown
  - Third party PD
  - Third party financial loss
- ✓ **Consider**
  - Underinsurance
  - Exclusions
  - Disputes
  - Regulatory Fines
  - Legal Fees

Institute and Faculty of Actuaries

NotPetya: **Ransomware** **>$10Bn** **$3.3Bn (mostly BI)**

Cyber Catastrophes

Aggregating Scenarios

1. Affirmative Exposure

- Key challenge is how well do we understand the risk? At both insured and aggregate level. To what level do we need to?
- Do we have enough data to estimate losses accurately and any dependencies?
- Does the past give a good indication of the future?
- Common Scenarios
  - Ransomware
  - Data Breach
  - Cloud Outage
  - Physical Damage/ Bashe (new)

2. Non-affirmative/Silent Scenarios

- Very difficult
  - What is the silent exposure within your exposure?
  - Which LoBs are exposed and to what scenarios?
  - Wordings strength? Is CL380 strong enough?
  - Which insurable costs are impacted?
- What are the relevant scenarios?
  - Control systems/SCADA
  - Business Blackout/Critical Infrastructure
  - Product recall
  - Black Swan

"I don't think we or anybody else really knows what they're doing when writing cyber insurance" - Warren Buffet, 2018

Institute and Faculty of Actuaries

Cyber Catastrophes

Modelling Aggregations

I. In-house Modelling

- What is your modelling philosophy toward cyber? Can you gain comfort from deterministic model?
- Can you obtain suitable, reliability and relevant data to even attempt modelling?
- Do we need to understand individual risks to understand the aggregation?
- Can you give management confidence?

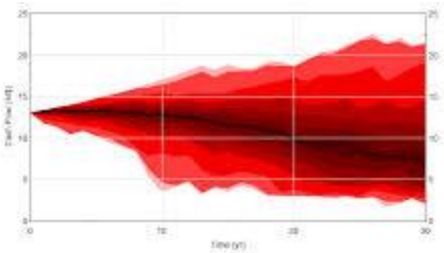
Deterministic/Footprint

$f(x)$

LLOYD'S

VS

Stochastic



II. Vendor Market

- Established vendors vs new entrants, what value are you looking for
- Each have different approaches to the problem and different IP hence estimates can very significantly!
- Very early stages of model development for silent cyber
- Crucially are the models relevant for your exposure
- Does data augmentation matter?
- Top down vs bottom up approaches

CyberCube

KOVRR

CYENCE

AIR

RMS

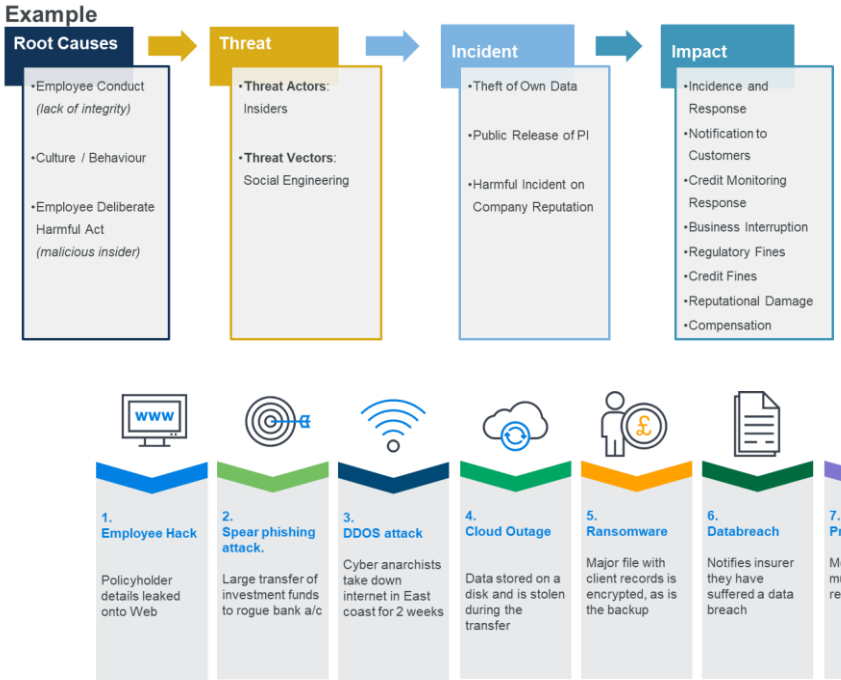
corax

Institute and Faculty of Actuaries

Operational Risk

Quantification Framework

1. **Scenario structure/taxonomy**
   - Narrative important and relevant
   - Leveraging NIST framework or similar
2. **Cost structure/taxonomy**
   - Impacts to business on frequency and/or severity
   - Mitigation of impacts in relation to NIST
3. **Threat actors and vectors**
   - Important to understand the scale and nature of the event
4. **Consult Cyber Security/IT experts**
   - Important to use as much technical knowledge as possible
   - Determine what is realistic and a tail event
5. **Continuous Monitoring**
   - The Cyber landscape changes rapidly, be prepared to keep learning and evolving

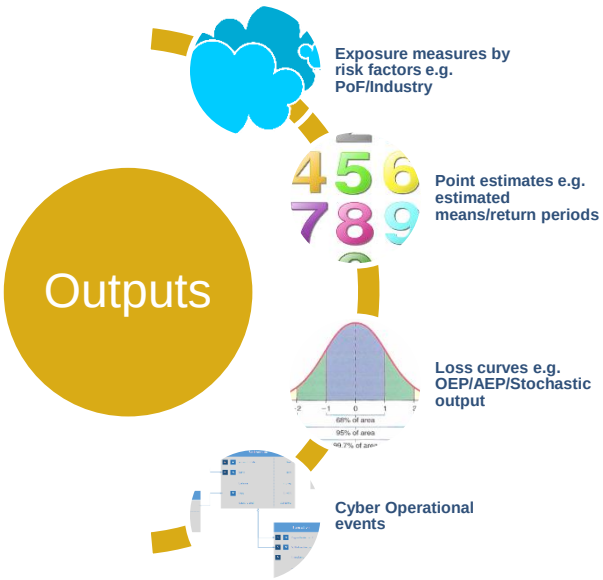


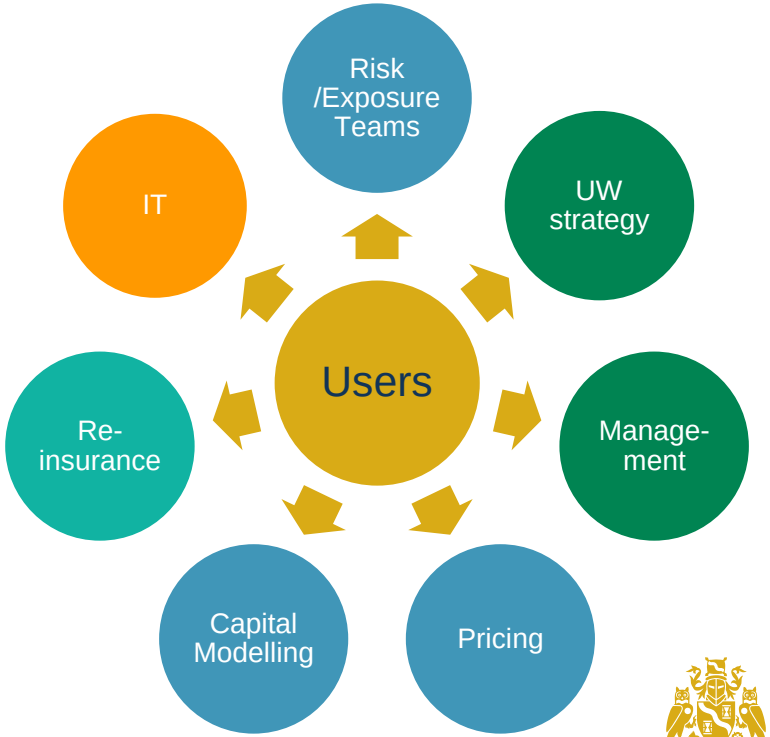
Institute and Faculty of Actuaries

Is Cyber OP Risk standalone or does it increase the frequency and severity of existing OP Risks?

Cyber Catastrophes

Cyber Outputs





Institute and Faculty of Actuaries

Questions

Comments

Institute and Faculty of Actuaries

Appendix

16 April 2019

Cyber Risk Investigation Working Party

*The purpose of the working party's research is to provide insight for actuaries working on **capital requirements** for insurers setting out the **potential impact of cyber risk events** and the **measures available to mitigate this risk**.*

The aim is to create a greater awareness of the risks for insurers, and highlight emerging issues in an area that is changing rapidly as the dependency on computer systems to support insurer's business increases.

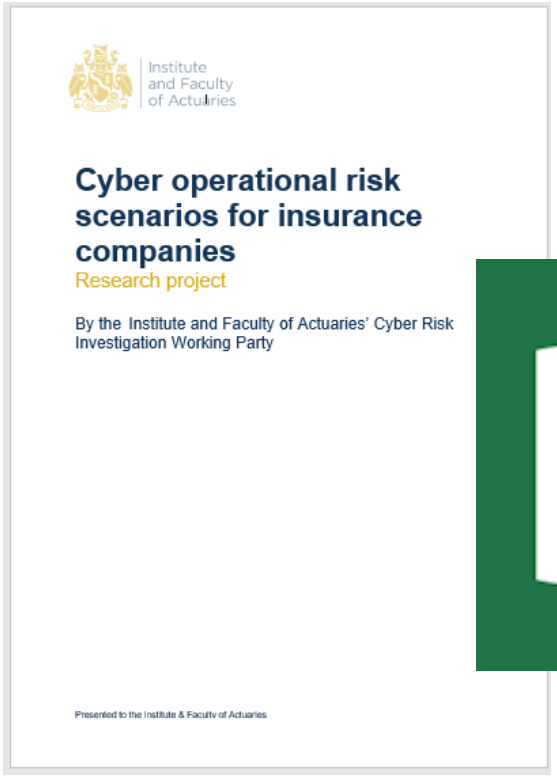
1) Actuaries

2) Cyber experts

3) Academics

Institute and Faculty of Actuaries

Sessional Paper



Institute and Faculty of Actuaries

Scenario 1: Employee leaks data at General Insurer

Overview

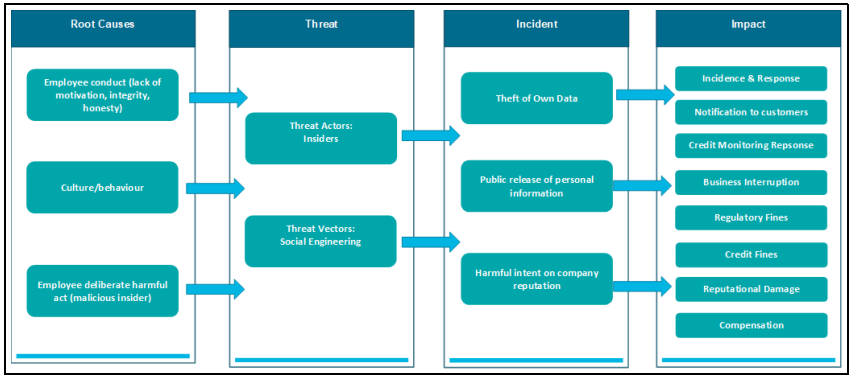
Company Info

The insurer has a global presence, with over **£10bn in revenue**. The UK motor insurance book is a major unit of the insurer, with **£1bn annual premium**. The UK motor insurance portfolio contains **4m data records**, with 3m policyholders on risk and 1m legacy records.

Event Narrative

All motor insurance data was published online. The data leak was noticed by a policyholder who called the emergency claims team. This did not get escalated appropriately and it took another day before key staff members were aware of the data breach. **Slow response** and **poor communication** with the public led to a backlash from policyholders who took to social media to vent their anger.

CRO Forum Category



Cost Impacts

Total Cost

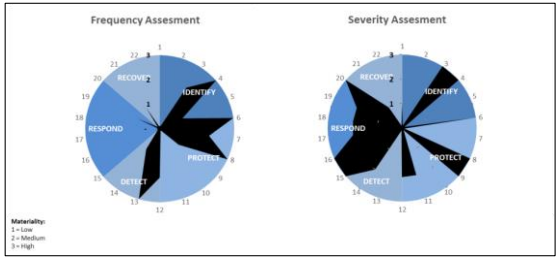
£210.5m

*** ~2% of Revenue**

Top 3 Cost Drivers

1)	Compensation	**£130m**
2)	Regulatory Fines	**£40m**
3)	Financial Ombudsman fine	**£25m**

Risk Mitigation (NIST)



Control Areas

- **Protection** e.g. access controls, data security and information protection processes;
- **Respond** e.g. response planning, communication and improvements

Institute and Faculty of Actuaries

Scenario 2: Cyber extortion at a Life Insurer

Overview

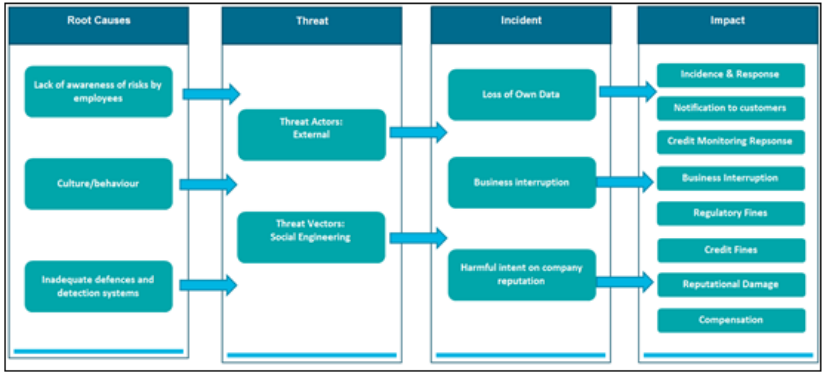
Company Info

The insurer is a subsidiary of a **FTSE100** listed financial services group. **GWP = £3bn, and profit = £300m.** They recently begun an IT transformation programme. It has an **outsourcing arrangement** with a data services company to develop, test, maintain and support new technology applications, both during and after the transformation phase.

Event Narrative

A group of **hackers** carry out series of attacks. Ransomware worm infects almost all of the systems. Request for a ransom payment of £15m is received. Revised ransom figure of **£7.5m is paid** to the hackers, this does **NOT** result in the decryption of data. Malware decontamination is needed. The incident has a **huge impact** on the firm's business. Media focuses on the **poor internal controls**. **Reputational** fallout is **catastrophic** as many customers are not able to check their balances and the firm suffers a **significant drop in sales** as well as **regulator scrutiny**.

CRO Forum Category



Cost Impacts

Total Cost

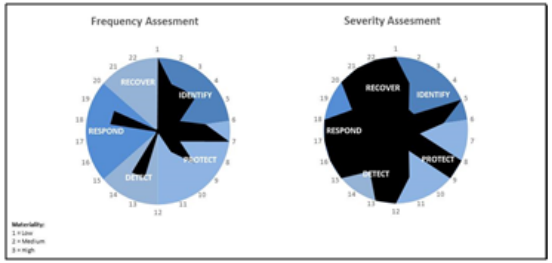
£179.5m

* ~6% of Revenue

Top 3 Cost Drivers

1)	Lapses)	£120m
2)	(Productivity)	£33m
3)	Data Restoration	£10m

Risk Mitigation (NIST)



Control Areas

- Detect e.g. security continuous monitoring and detection;
- Respond e.g. analysis, mitigation and improvements; and
- Recover e.g. recoverability and communications

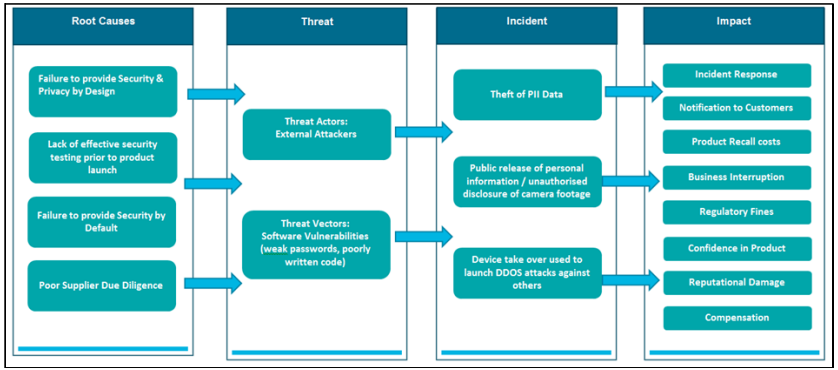
Institute and Faculty of Actuaries

Scenario 3: Motor insurer telematics device hack

Overview

Company Info	**Medium** sized UK only **motor** insurer using telematics devices. GWP **£400 million**, fleet of **500,000 cars** using its telematics device. Average premium of £500 per annum per client for the telematics product, resulting in c£250m premium p.a. for the telematics product.
Event Narrative	All telematics devices get hacked, rendering the devices (costing c£50 each) unusable. Every device needs to be recalled and replaced. Sensitive data from the devices is compromised and published online. Compromised devices are used as part of a Botnet to launch a distributed DDoS. **Week 10 - 20:** Devices replaced**. End of year 1:** The Information Commissioner's Office applies a fine due to loss of customer data resulting from device security weaknesses. **Years 3 – 5:** Damages incurred from complaints cases, reputational damage remains and sales are reduced. **Year 5:** Incident now in past and reputation restored.

CRO Forum Category

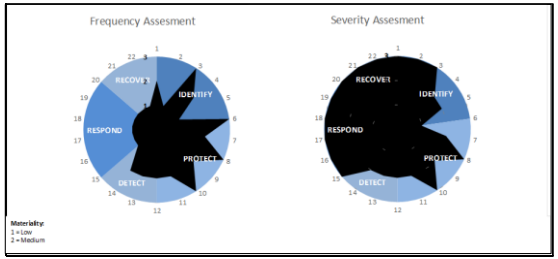


Cost Impacts

Total Cost	**£70.0m** * ~18% of annual premium

Top 3 Cost Drivers			
	1)	Physical Damage	**£42.5m**
	2)	Business Interruption	**£14.0m**
	3)	Compensation	**£10.0m**

Risk Mitigation (NIST)



Control Areas	• **Identify** e.g. asset management and inventory; • **Protect** e.g. access controls, data security, remote management and information protection processes; and • **Detect** e.g. anomalies and events.

Institute and Faculty of Actuaries