

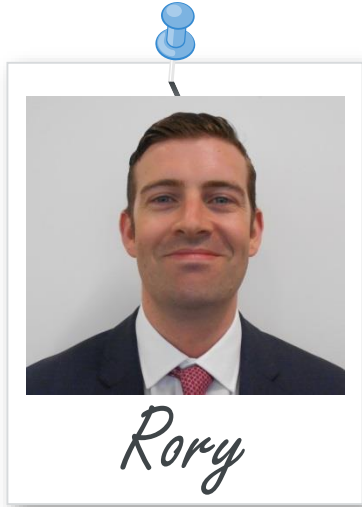


Institute
and Faculty
of Actuaries

Cyber Operational Risk Scenarios for Insurance Companies

Rory Egan, Munich Re
Simon Cartagena, SCOR
Visesh Gosrani, Cyence

Cyber Working Party Representatives



Institute
and Faculty
of Actuaries

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

Cyber operational risk scenarios for insurance companies

Research project

By the Institute and Faculty of Actuaries' Cyber Risk
Investigation Working Party

Presented to the Institute & Faculty of Actuaries



Institute
and Faculty
of Actuaries

Agenda

1) Overview

- Cyber Insurance Losses
- Attacker Motivations
- Threat Vectors
- Operational Risk Landscape

2) Our Journey

- Building Scenarios and Framework
- Main Learning Outcomes

3) Outputs Discussion

- Summary of Results
- Could Cyber sit under a rule of thumb?
- Controls (NIST) Assessment

4) Summary





Institute
and Faculty
of Actuaries

Overview

Rory Egan

17 October 2018

**Massive Equifax data breach
hits 143 million**

**Home Depot to Pay
\$27.25m in Latest Data
Breach Settlement**

**Target to pay
\$18.5M for 2013
data breach that
affected 41
million
consumers**

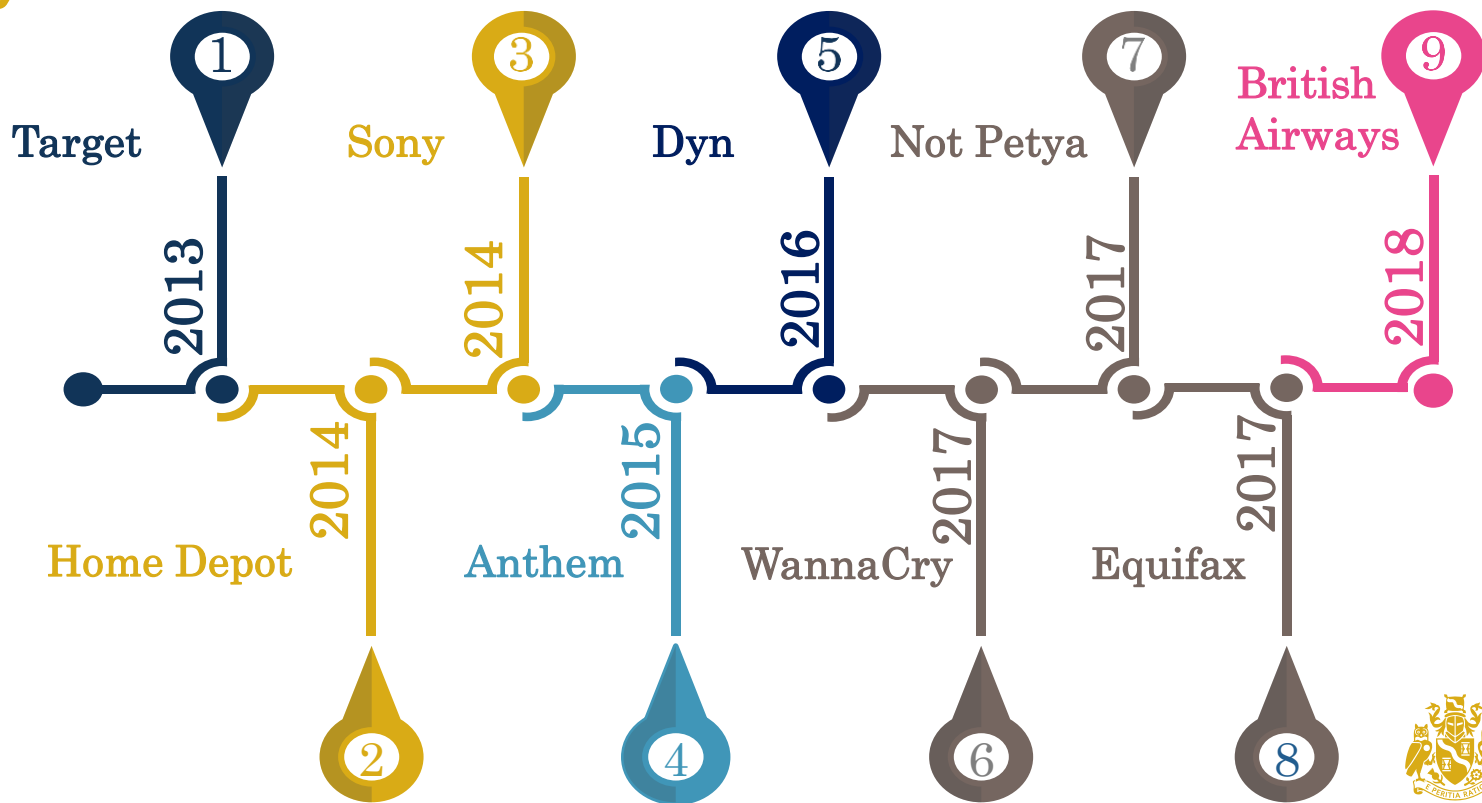
**Uber concealed massive hack that
exposed data of 57m users and drivers**

**NHS 'could have
prevented' WannaCry
ransomware attack**

**British Airways Faces
Class-Action Lawsuit
Over Data Breach**

**Government under pressure after NHS
crippled in global cyber attack as chaos looms**

Cyber Events



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

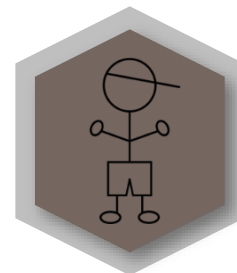


State Sponsored Group

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

Extremist Groups

- Publicity
- Recruitment
- Widespread Disruption
- Espionage
- Sabotage



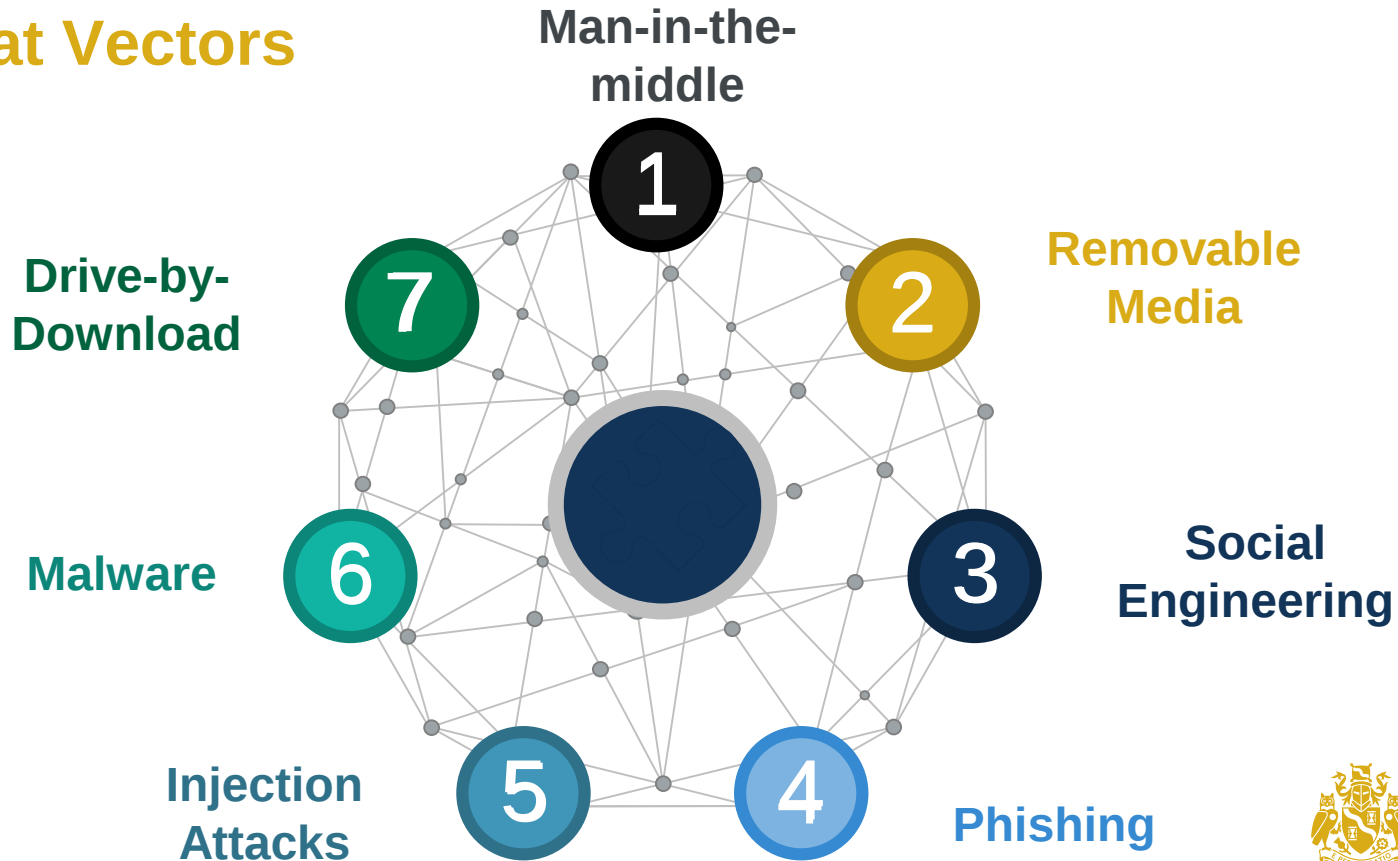
Opportunists / Script Kiddies

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



Institute
and Faculty
of Actuaries

Threat Vectors



Institute
and Faculty
of Actuaries

Operational 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



Institute
and Faculty
of Actuaries

Why Cyber Operational Risk should be assessed



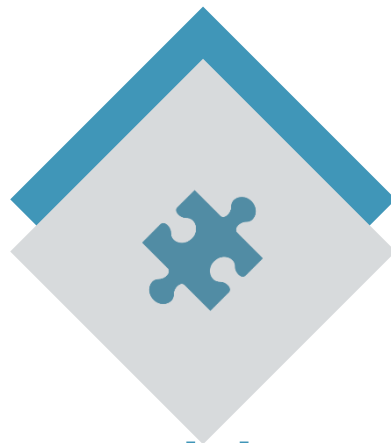
Capital Load

Cyber risk is routinely cited as one of the most important sources of operational risks facing organisations today



Regulation

Regulators and legislators are increasing their focus on this topic (GDPR)



Risk Assessment

Actuaries need to have a robust assessment of the potential losses stemming from cyber risk, as part of an overall risk management framework



Consistent Framework

A logical, consistent and unbiased solution is needed



Institute
and Faculty
of Actuaries



Institute
and Faculty
of Actuaries

Building a Framework for Quantification - Our journey

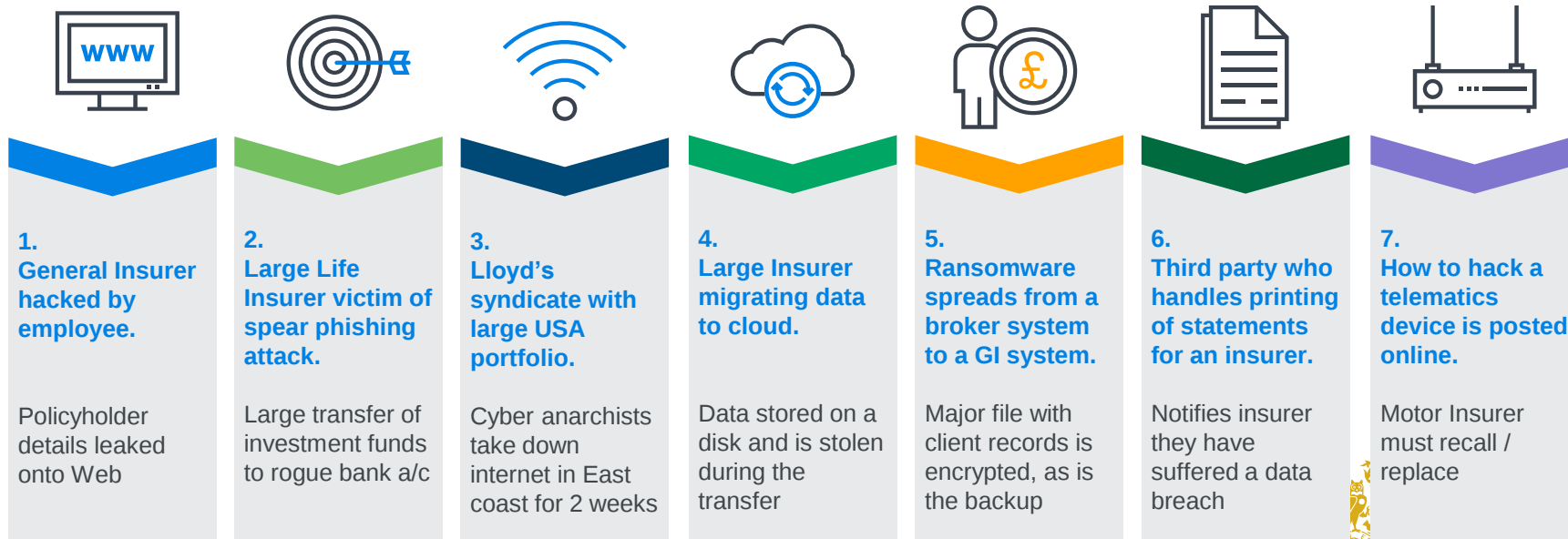
Simon Cartagena

17 October 2018

Building Scenarios and Framework

1. Brainstorming

2. Scenario development



Building Scenarios and Framework

3. Group assessments of selected scenarios

- Results and challenges

4. Framework approach development

- Why do it?
- How do we build scenario that is relevant and consistent?
 - Draw on sources available e.g. CRO Forum/NIST*/Threat reports etc.
- How do we build one that is quantifiable?
 - What are the tangible & intangible costs
- What are the most important aspects of assessments?
 - Consistency/repeatable/updatable
 - Being able to communicate the outputs
- Threat actors/vectors- how much should we care?



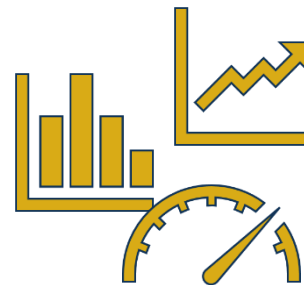
Institute
and Faculty
of Actuaries

*National Institute of Standards and Technology

Building Scenarios and Framework

5. Scenario quantification

- Vulnerable controls & mitigation assessment against the NIST framework
- Ground up costs estimation approach leveraging CRO forum
- Frequency/Severity impacts assessment
- Consistency of estimates
- Transparency/justification of estimates



6. Validation

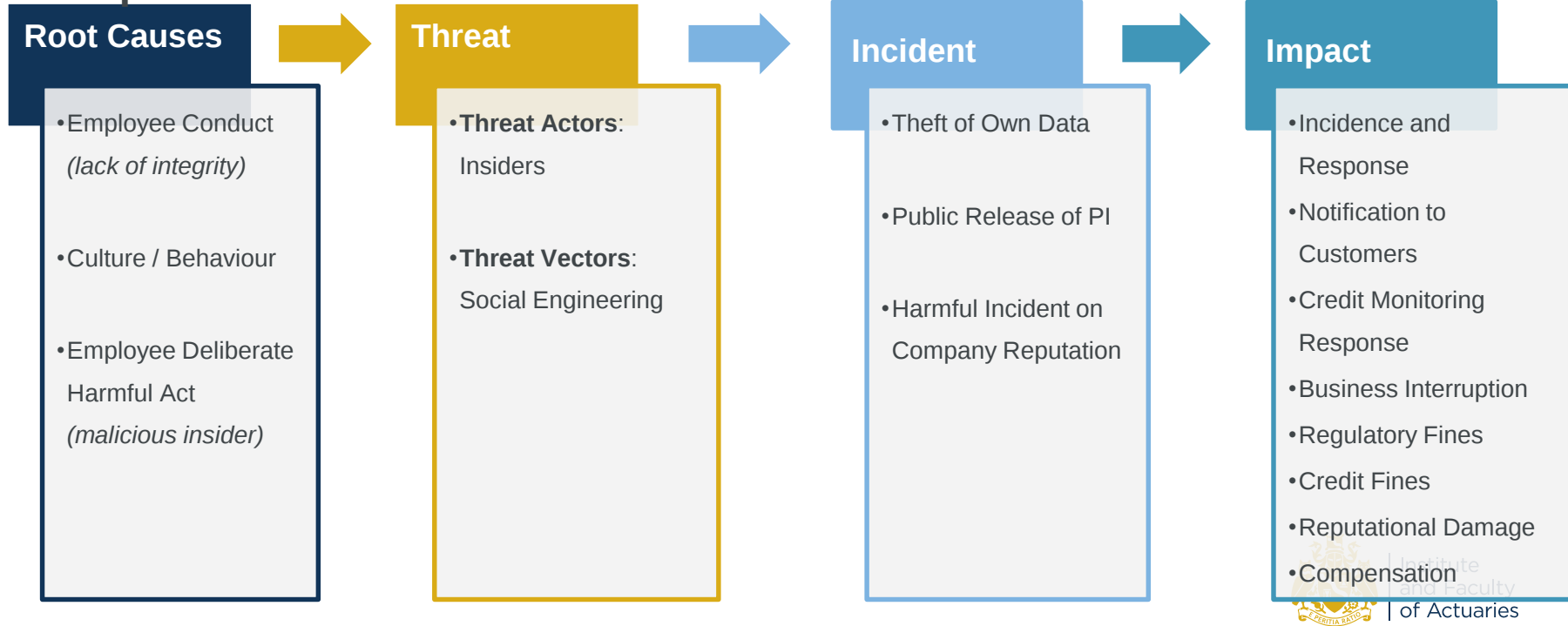
- Do the scenarios make sense to experts? Use experts as often as possible!
- Actuaries cannot solve this on their own
- Breaking down language/jargon/acronym barrier, talking in the same language is difficult
- Uncertainty vs absolutes: combining actuarial and cyber/IT schools of thought to produce a useful basis for quantification.



Institute
and Faculty
of Actuaries

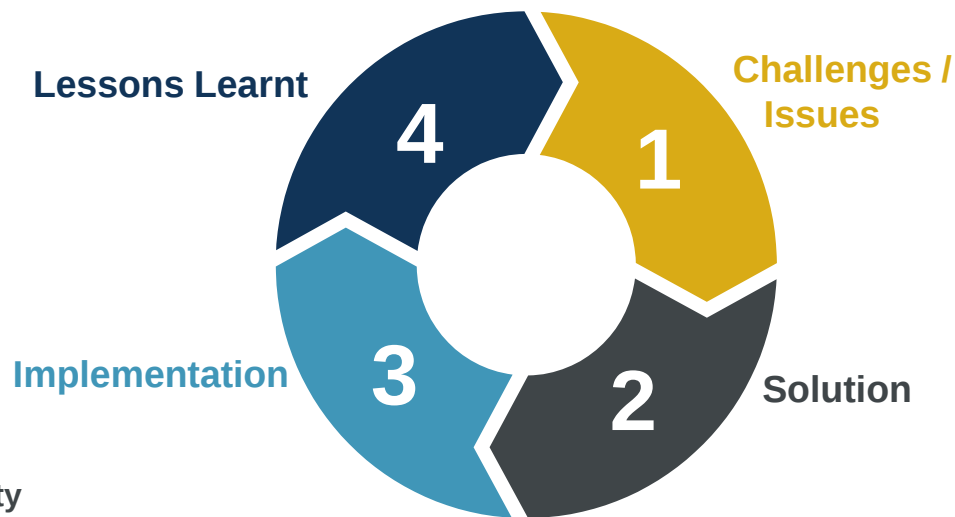
Building Scenarios and Framework

Example



Main Learning Outcomes

1. Build a scenario structure/taxonomy
2. Build a cost structure/taxonomy
3. Think about the threat actors and vectors
 - scenario should be relevant to your entity
4. Consult Cyber/IT experts (as many as possible)
5. The Cyber landscape changes rapidly, be prepared to keep learning and evolving



Institute
and Faculty
of Actuaries



Institute
and Faculty
of Actuaries

Scenarios – Outputs Discussion

Visesh Gosrani

17 October 2018

Summary of Results

	(1)	(2)	(3)
Scenario:	Employee leaks data at a General Insurer	Cyber extortion at a Life Insurer	Motor insurer telematics device hack
Threat Vectors:	Insider attack, social engineering	External attack, social engineering	External attack, software vulnerabilities
Security:	Protect & respond	Detect, respond & recover	Identify, protect & detect
Main Cost Component:	Compensation, regulatory fines	Business interruption, reputational damage	Remediation (device replacement)
1 in 200 Loss (£m): (% of annual revenue)	£211m ~2%	£180m ~6%	£70m ~18%



Could Cyber sit under a rule of thumb?

- Different groups
 - Personnel changes
 - Developing cyber environment
- Varying scenarios
- Types and sizes of insurer
 - Differing motives
 - Differing attack perimeters
 - Take Cyber maturity into account
- Estimating a 1 in 200



Controls (NIST) Assessment

Summary of the key controls for each scenario that impact the severity and/or the frequency of the event. Key Risk Management and Operational assessment for the scenarios would therefore focus on improving or mitigating these key control areas.

	(1)	(2)	(3)
Scenario:	Employee leaks data at a General Insurer	Cyber extortion at a Life Insurer	Motor insurer telematics device hack
	• Protection e.g. Access Controls, Data Security and Information Protection Processes • Respond e.g. Response Planning, Communication and Improvements	• Detect e.g. Security Continuous Monitoring and Detection Processes • Respond e.g. Analysis, Mitigation and Improvements • Recover e.g. Recovery planning, lessons learned	• Identify e.g. Asset Management & Inventory • Protect e.g. Access Controls, Data Security, Remote Management and Information Protection Processes • Detect e.g. Anomalies and Events



This is really important!

- Firms need to take Cybersecurity seriously
 - We currently estimate each of these scenarios would be a significant cost to a business (largely driven by required speed of response, fines & regulatory response)
- The NIST framework is a useful place to start when assessing your key Cyber Operational risks
- Figures produced are highly subjective
 - Key uncertainties exists on the likelihood of each scenario and is bespoke depending on each firm.
 - Knowledge/experiences varies so widely from person to person
- Communication rationale for scenario selection and cost calculation is important for transparency and development, given speed of development of subject matter



Questions

Comments

The views expressed in this presentation are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this [publication/presentation] and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this presentation.

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this presentation be reproduced without the written permission of the IFoA.



Institute
and Faculty
of Actuaries



Institute
and Faculty
of Actuaries

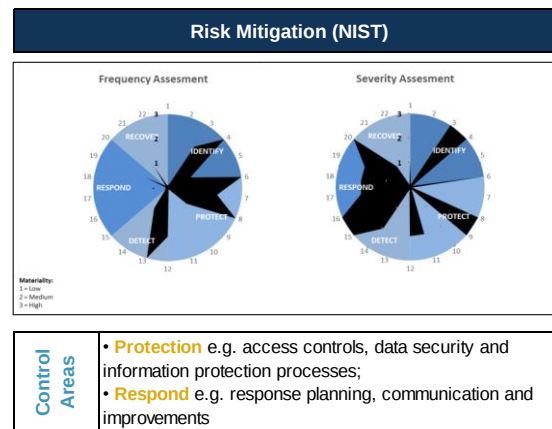
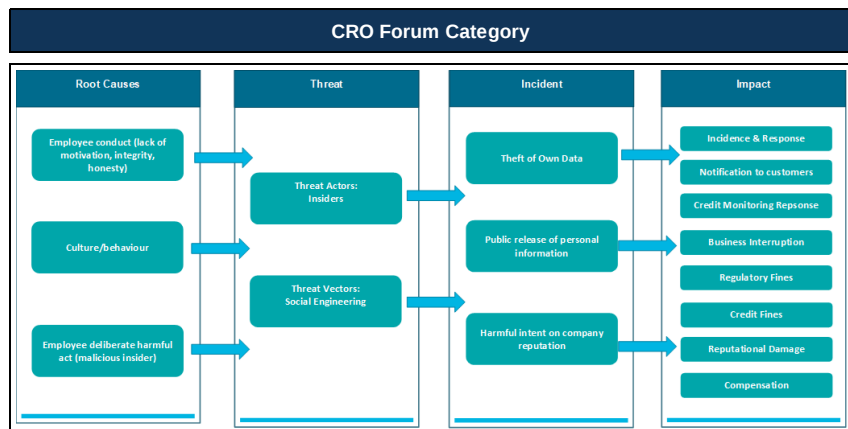
Appendix

17 October 2018

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.

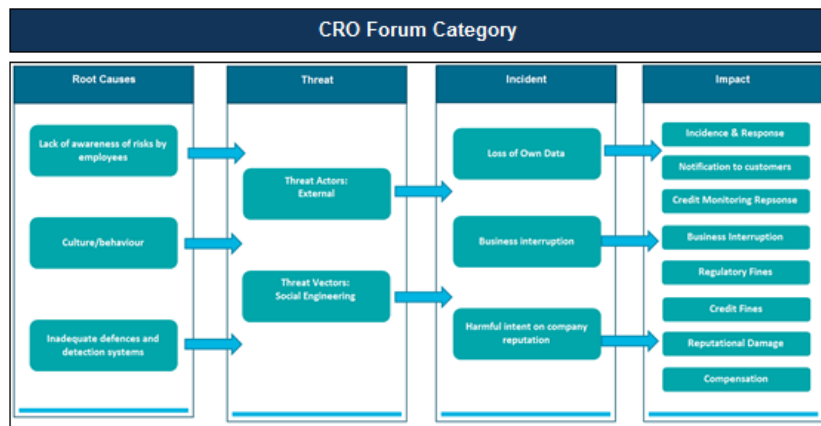
Cost Impacts		
Total Cost	£210.5m * ~2% of Revenue	
Top 3 Cost Drivers	1)	Compensation £130m
	2)	Regulatory Fines £40m
	3)	Financial Ombudsman fine £25m



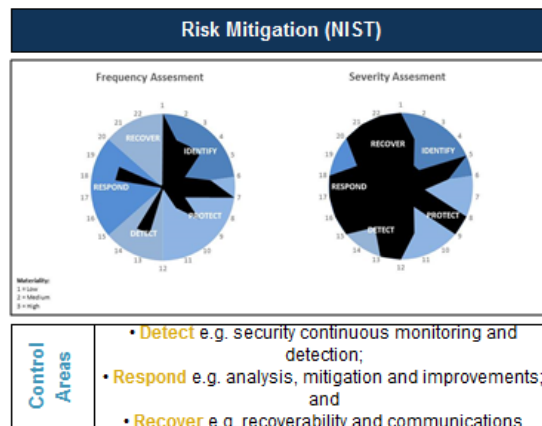
Institute
and Faculty
of Actuaries

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.



Cost Impacts							
Total Cost	£179.5m * ~6% of Revenue						
Top 3 Cost Drivers	<table> <tr> <td>1) Lapses)</td><td>£120m</td></tr> <tr> <td>2) (Productivity)</td><td>£33m</td></tr> <tr> <td>3) Data Restoration</td><td>£10m</td></tr> </table>	1) Lapses)	£120m	2) (Productivity)	£33m	3) Data Restoration	£10m
1) Lapses)	£120m						
2) (Productivity)	£33m						
3) Data Restoration	£10m						



Scenario 3: Motor insurer telematics device hack

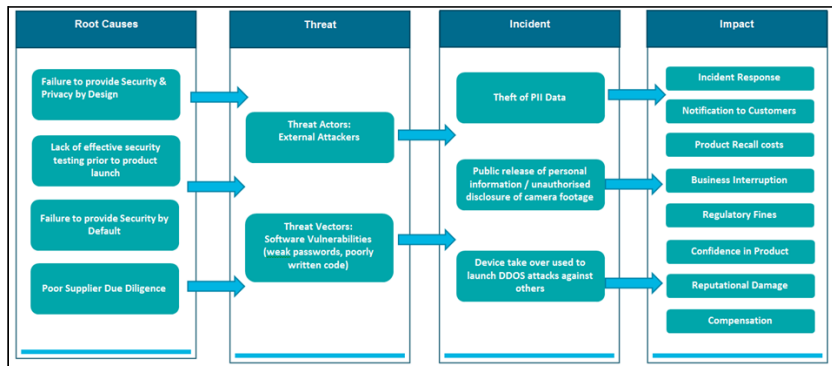
Overview

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.

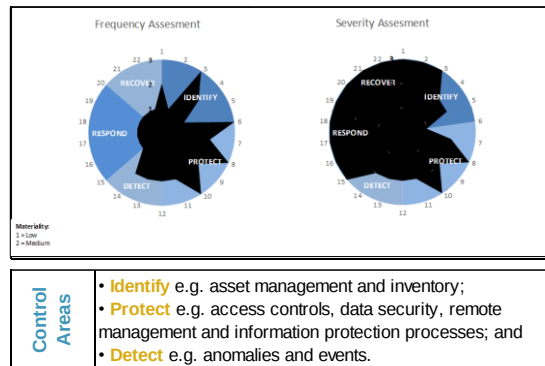
Cost Impacts

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

CRO Forum Category



Risk Mitigation (NIST)



Institute
and Faculty
of Actuaries