Institute and Faculty of Actuaries

Non-Affirmative Cyber Assessment Framework

IFoA Cyber Risk Working Party

Simon Cartagena, SCOR
Visesh Gosrani, Cydelta
Justyna Pikinska, Capsicum Re

September 19

Agenda

- **Overview**
  - Working Party Deliverables
  - PRA Definition & Findings
- **Silent Cyber Framework**
  - Clause Usage & Interpretation
  - Scenario Generation
  - Reporting
- **Summary**

Institute
and Faculty
of Actuaries

Overview

Visesh Gosrani

September 19

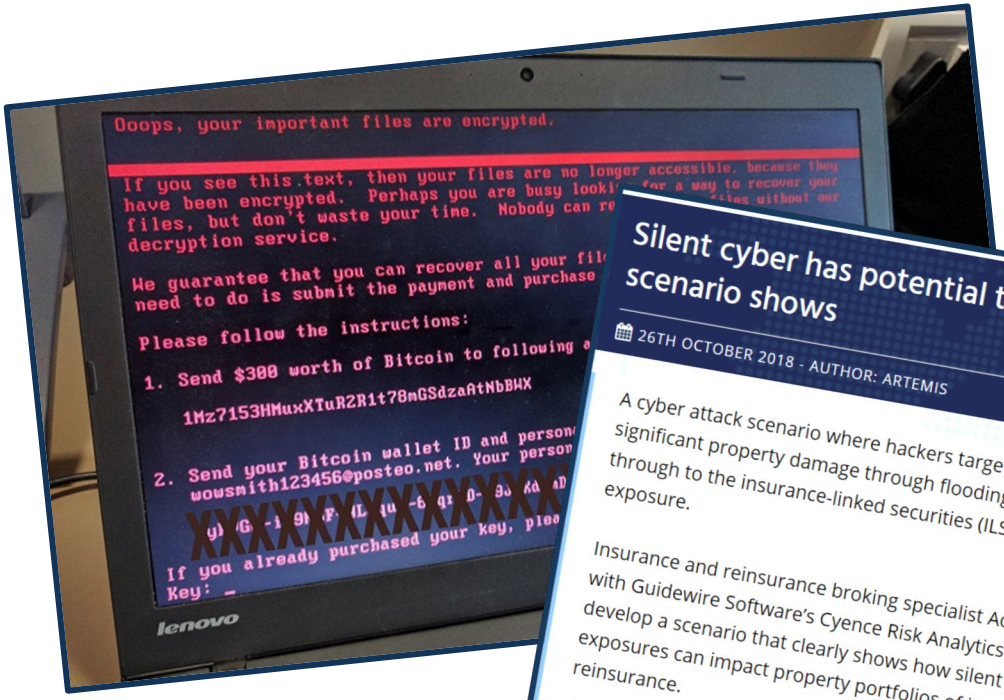
IFoA Cyber Risk Working Party

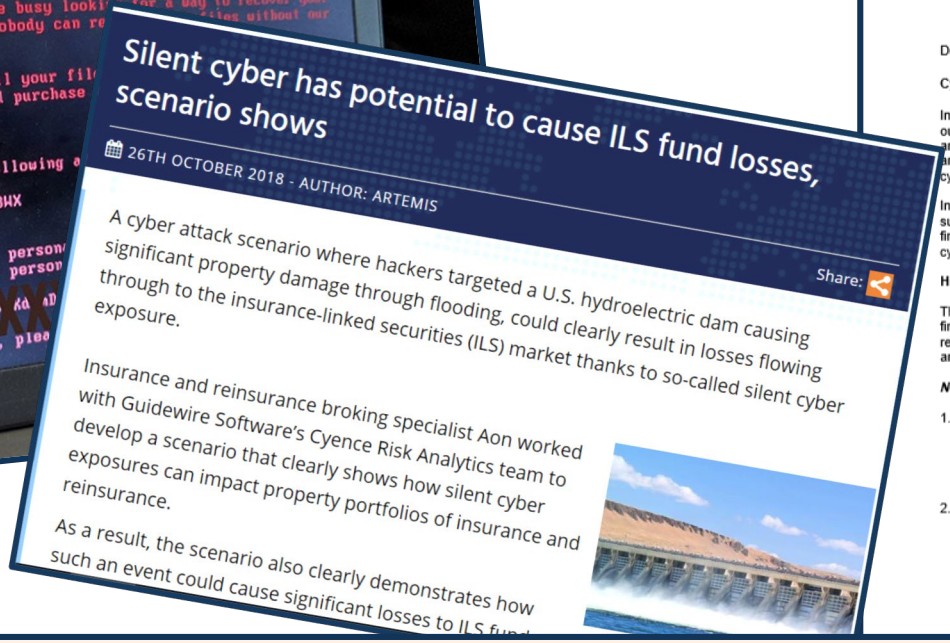
Activity timeline

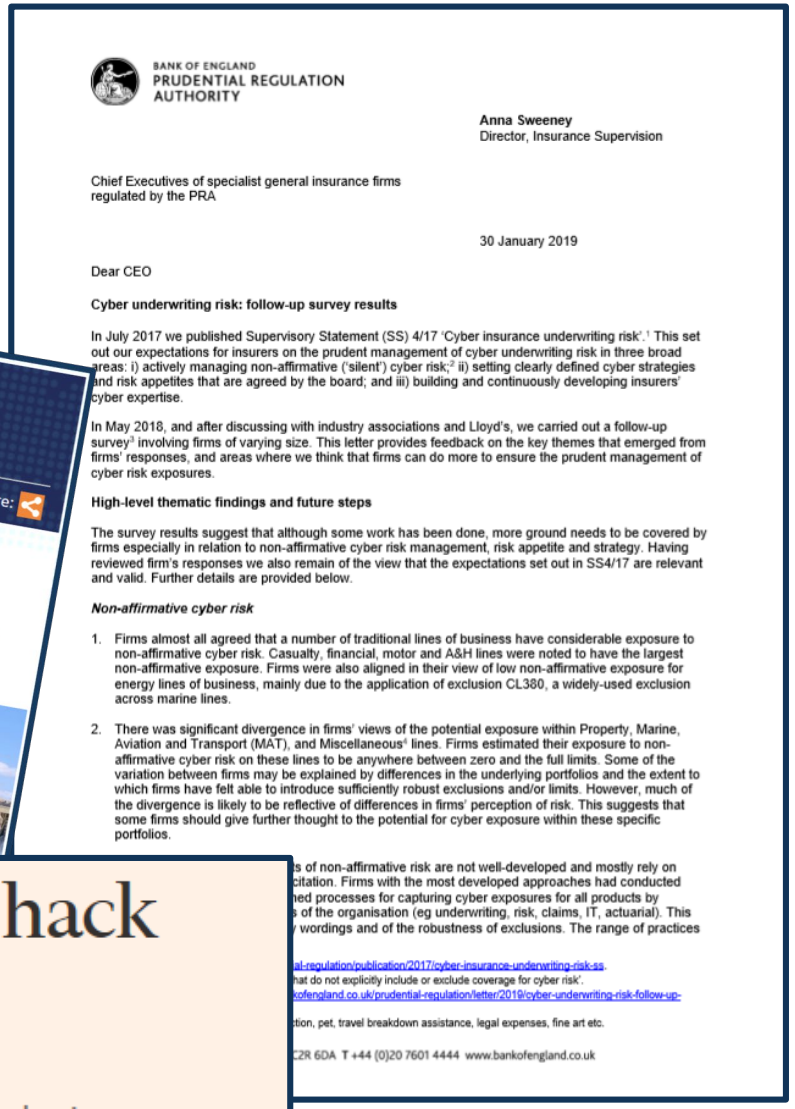
New studies/articles and content under consideration

Please feel free to suggest topics to us that would help you in your roles

Why should we care?







Mondelez sues Zurich in test for cyber hack insurance

Insurance group had refused to pay for NotPetya attack, invoking a war exclusion

PRA Definition & Findings

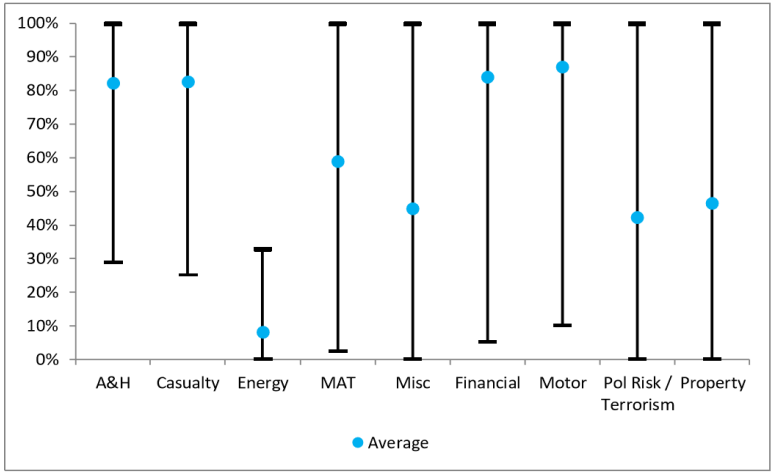
Definition

1.6 The PRA expects firms to be able to identify, quantify and manage cyber insurance underwriting risk. This includes both of the following sources of cyber insurance underwriting risk:

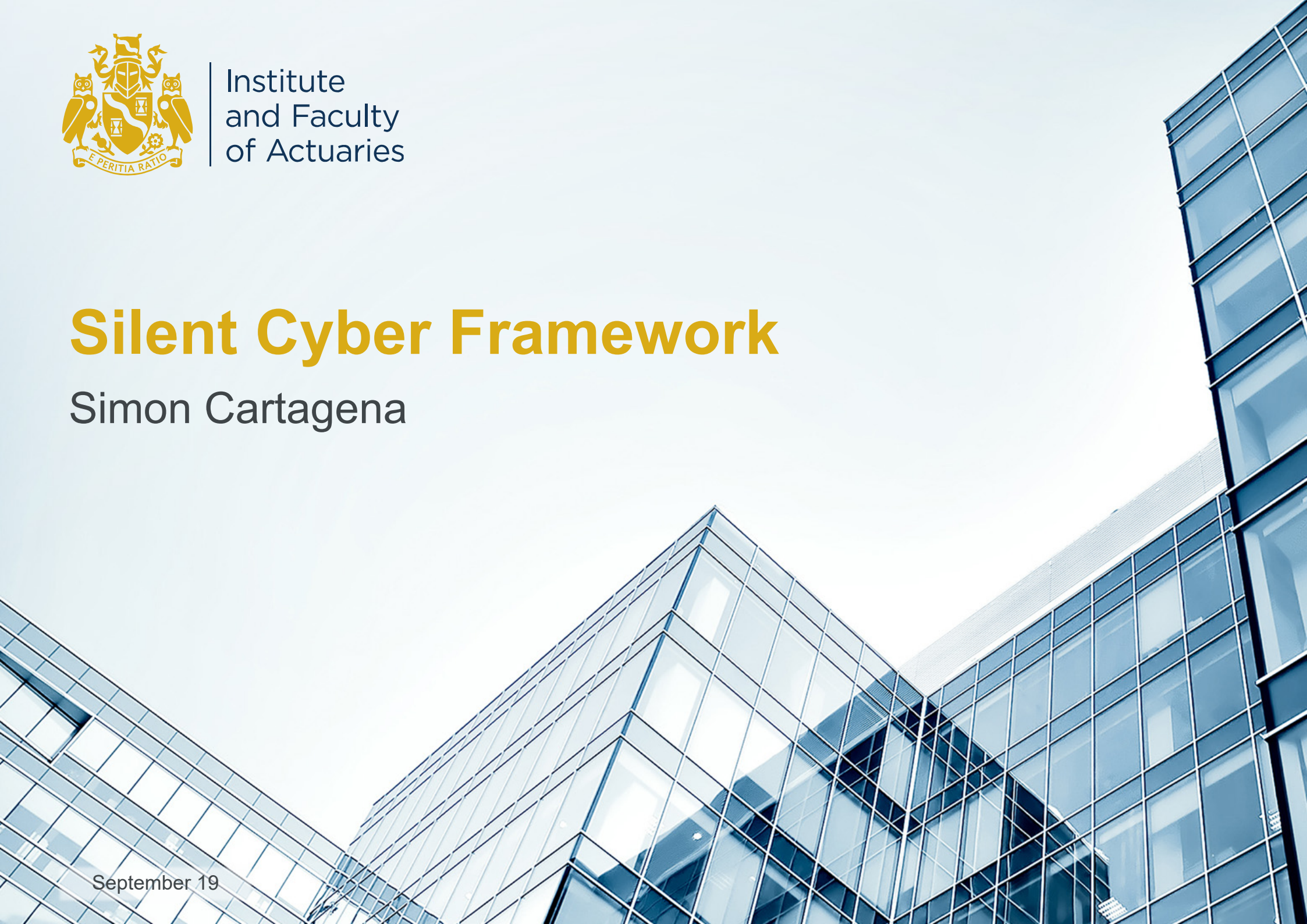
(a) affirmative cyber risk, ie insurance policies that explicitly include coverage for cyber risk; and

(b) non-affirmative cyber risk, ie insurance policies that do not explicitly include or exclude coverage for cyber risk . This latter type of cyber risk is sometimes referred to as 'silent' cyber risk by insurance professionals.

% of Total Policy Limit Exposed to Non-Affirmative Cyber Risk



Source: PRA



Institute
and Faculty
of Actuaries

Silent Cyber Framework

Simon Cartagena

September 19

Silent Cyber Framework

1. Exposure Assessment

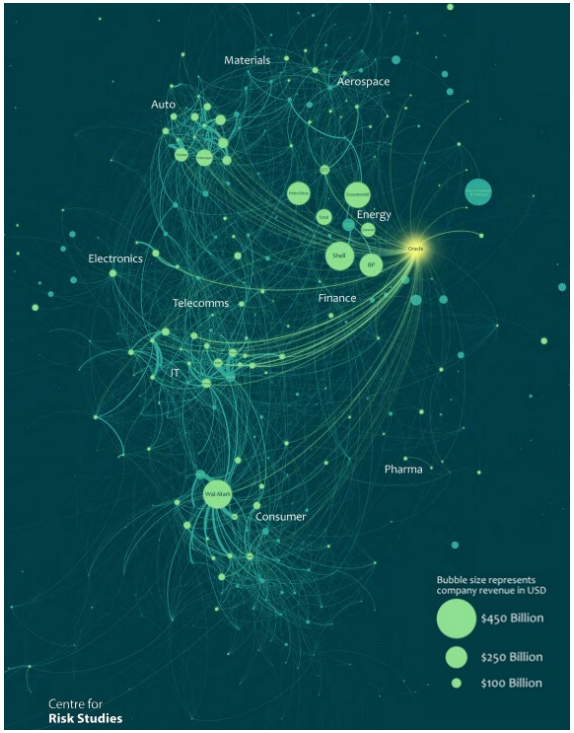
- What is achievable for you?
- Contracts/Clause wordings usage and understanding is crucial!
- Forming your own view of the confidence you as a firm have in those wordings
- Policy level assessment is ideal but difficult to maintain ongoing?
  - Are you confident the data is accurate?
  - Is the company's view on the contract working consistent?

2. Scenario development

- Are you developing/considering scenarios that are relevant to your exposure?

3. Management Reporting

- What do management need to know/understand about the silent cyber problem?
- It's our role to help them understand the complexities by bringing together different disciplines from across the business into a unified view of the potential risk.



Clause Usage & Interpretation

#	LMA Classes	Wordings Intention	Exclusion	Exclusion	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Affirmative	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion
			LMA5272/3/4/5	LMA3150	LMA3141	LMA3127	LMA3092/30	NMA2918	NMA2914/5	NMA2914/5 A	NMA2912/8	CL380	JS2015/8	LSW555	AVN52G	AVN48B	ANV124	LMA5240	LMA5241	LMA5241A	LMA5327	LMA5359
			Cyber Incident Exclusion	Insurance Act 2015 Endorsement - General Liability	Electronic and Computer Crime Policy	HIP 2015 Policy	Terrorism exlcusion (including cyber terrorism)	Terrorism exlcusion (including cyber terrorism)	Electronic Data Endorsement	Electronic Data Endorsement (ammended)	IT Hazard Clarification Clause	The Institute Cyber Attack Exclusion Clause	Cyber Attack Exclusion Clause and Write-Back	Aviation Hull "War and allied perils"	Extended Coverage Endorsement	War/Hijacking and other perils exclusion	Data Event Clause	Cyber Loss Exclusion	Cyber Loss Limited Exclusion	Cyber Loss Limited Exclusion (ammended)	Cyber Loss Limited Exclusion	Cyber Loss Exclusion
1	Aviation Hull		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
2	Aviation Liability		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗
3	Aviation War		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗
4	Casulaty RI		✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
5	Contingency		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
6	D&O		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
7	E&O		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
8	Engineering		✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
9	Financial Institutions		✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
10	General Liability		✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
11	Livestock & Bloodstock		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
12	Marine Cargo		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
13	Marine Hull		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
14	Marine Liability		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
15	Marine War		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
16	Marine XL		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
17	Motor		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
18	Offshore Energy		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
19	Onshore Energy		✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
20	Personal Accident		✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
21	Political Risks		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
22	Power Generation		✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
23	Property D&F		✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
24	Property RI		✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗
25	Property UK Commercial		✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
26	Propery UK Household		✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
27	Specie		✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
28	Terrorism		✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

- **LMA wordings review 2018 was used as basis for a default market view**
- **It's important to evaluate this in context of your own markets and policies**
- **This will need regular review and update over the next 1-2 years as the market addresses contract certainty related to cyber**

Scenario Generation

Non Affirmative Scenarios

Use the output from your analysis of the expoisure and cyber peril coverages to devise relevant and useful scenarios for your business.

Use this to articualte to management why the scenarios chosen are the most appropriate and where potential non-affirmative losses are likely to arise from.

Coverage	Silent	Affirmative	Total	Rank
Business interruption - Interruption of operations	192,633,818	74,489,968	267,123,786	1
Contingent business interruption (CBI) for non-physical damage	192,633,818	74,489,968	267,123,786	1
Data and software loss	39,412,447	6,874,547	46,286,994	21
Financial theft and/or fraud	61,406,627	22,918,841	84,325,468	15
Ransom and extortion	81,281,878	25,603,227	106,885,105	11
Intellectual property theft	61,406,627	22,918,841	84,325,468	15
Incident response costs	161,577,569	35,284,990	196,862,560	6
Breach of Privacy	58,904,617	8,923,118	67,827,736	18
Network Security/Security Failure	67,249,555	8,561,062	75,810,617	17
Reputational Damage (excluding legal protection)	89,243,734	24,605,356	113,849,091	8
Regulatory & Legal Defense costs (excluding fines and penalties)	89,243,734	24,605,356	113,849,091	8
Fine and penalties	89,243,734	24,605,356	113,849,091	8
Communication and media	82,967,254	22,734,582	105,701,836	12
Legal protection – Lawyer fees	81,856,980	23,012,666	104,869,646	13
Assistance coverage – psychological support	122,202,161	11,373,988	133,576,150	7
Products	58,904,617	8,923,118	67,827,736	18
D&O	39,412,447	6,874,547	46,286,994	21
Tech E&O	85,631,450	10,887,719	96,519,168	14
Professional services E&O, Professional indemnity	58,904,617	8,923,118	67,827,736	18
Environmental damage	157,285,036	42,822,386	200,107,422	5
Physical asset damage	152,479,752	56,053,471	208,533,224	4
Bodily injury and death	189,791,158	72,968,483	262,759,641	3

LMA Classes	Affirmative	Excluded	Silent	Rank
Aviation Hull	2%	90%	8%	19
Aviation Liability	30%	64%	6%	21
Aviation War	33%	63%	4%	25
Casualty RI	5%	53%	42%	6
Contingency	4%	34%	62%	2
D&O	8%	76%	16%	15
E&O	5%	52%	43%	5
Engineering	4%	90%	6%	20
Financial Institutions	22%	53%	25%	9
General Liability	5%	56%	39%	7
Livestock & Bloodstock	7%	90%	3%	27
Marine Cargo	5%	80%	16%	16
Marine Hull	7%	90%	3%	28
Marine Liability	6%	90%	4%	26
Marine War	5%	81%	14%	17
Marine XL	3%	47%	49%	4
Motor	4%	38%	58%	3
Offshore Energy	5%	90%	5%	22
Onshore Energy	5%	74%	21%	12
Personal Accident	2%	21%	77%	1
Political Risks	7%	69%	24%	10
Power Generation	6%	75%	18%	13
Property D&F	5%	90%	5%	23
Property RI	7%	71%	23%	11
Property UK Commercial	6%	77%	17%	14
Propery UK Household	7%	84%	9%	18
Specie	6%	90%	4%	24
Terrorism	5%	59%	36%	8

Example

	2
Scenario Name	Lloyds Business Blackout
Description	An unidentified group motivated to cause significant disruption inside the USA reaches out to the hacking community and purchases the services of a small group of morally dubious programmers who are knowledgeable of reverse engineering in the domestic electricity sector and grid systems. All of the hackers hired have very little idea of what they are working on as a collective.

Coverage	Exposed by Scenario	Comment
Business interruption - Interruption of operations	✓	
Contingent business interruption (CBI) for non-phys	✓	
Data and software loss	✗	
Financial theft and/or fraud	✗	
Ransom and extortion	✗	
Intellectual property theft	✗	
Incident response costs	✓	
Breach of Privacy	✗	
Network Security/Security Failure	✗	
Reputational Damage (excluding legal protection)	✗	
Regulatory & Legal Defense costs (excluding fines a	✓	
Fine and penalties	✓	
Communication and media	✓	
Legal protection – Lawyer fees	✓	
Assistance coverage – psychological support	✓	
Products	✗	
D&O	✓	
Tech E&O	✗	
Professional services E&O, Professional indemnity	✗	
Environmental damage	✓	
Physical asset damage	✓	
Bodily injury and death	✗	

Coverage	Exposed by Scenario	Comment
Aviation Hull	✓	
Aviation Liability	✗	
Aviation War	✗	
Casualty RI	✗	
Contingency	✗	
D&O	✓	
E&O	✗	
Engineering	✗	
Financial Institutions	✗	
General Liability	✓	
Livestock & Bloodstock	✗	
Marine Cargo	✗	
Marine Hull	✗	
Marine Liability	✗	
Marine War	✗	
Marine XL	✗	
Motor	✗	
Offshore Energy	✗	
Onshore Energy	✓	
Personal Accident	✗	
Political Risks	✓	
Power Generation	✓	
Property D&F	✓	
Property RI	✓	
Property UK Commercial	✓	
Propery UK Household	✓	
Specie	✗	
Terrorism	✓	

SIC Name	Exposed by Scenario	Comment
A Agriculture, Forestry and Fishing	✗	
B Mining and Quarrying	✓	
C Manufacturing	✓	
D Electricity, gas, steam and air conditioning supply	✓	
E Water supply; sewerage, waste management and re	✓	
F Construction	✗	
G Wholesale and retail trade; repair of motor vehicle	✓	
H Transportation and storage	✓	
I Accommodation and food service activities	✗	
J Information and communication	✓	
K Financial and insurance activities	✓	
L Real estate activities	✗	
M Professional, scientific and technical activities	✗	
N Administrative and support service activities	✓	
O Public administration and defence; compulsory soc	✓	
P Education	✗	
Q Human health and social work activities	✓	
R Arts, entertainment and recreation	✓	
S Other service activities	✗	
T Activities of households as employers	✗	
U Activities of extraterritorial organisations and bodi	✗	

	Wordings		Writeback/coverage of covered peril		Non-Malicious Exclusion		Malicious Exclusion	
Wordings	Exposed by Scenario	Confidence	Relevant	Confidence	Exposed by Scenario	Confidence	Exposed by Scenario	Confidence
LMA5272/3/4/5	✗							
LMA3150	✓	Medium	✗		✗		✓	Medium
LMA3141	✗							
LMA3127	✓	High	✗		✓	Medium	✗	
LMA3092/30	✓	Medium	✓	Medium	✗		✓	Medium
NMA2918	✓	Low	✗		✓	Medium	✗	
NMA2914/5	✓	High	✓	Medium	✓	Medium	✓	Medium
NMA2914/5 A	✓	Medium	✗		✓	Medium	✓	Medium
NMA2912/8	✓	Low	✗		✓	Medium	✓	Medium
CL380	✓	Low	✓	Medium	✗		✓	Medium
JS2015/8	✗							
LSW555	✗							
AVN52G	✗							
AVN48B	✓	Medium	✗		✗		✓	Medium
ANV124	✓	Low	✓	Medium	✓	Medium	✓	Medium
LMA5240	✓	High	✗		✗		✓	Medium
LMA5241	✓	High	✓	Medium	✗		✓	Medium
LMA5241A	✓	High	✓	Medium	✗		✓	Medium
LMA5327	✓	High	✗		✗		✗	
LMA5359	✗							

Build structure around how you develop your scenario so that it is:

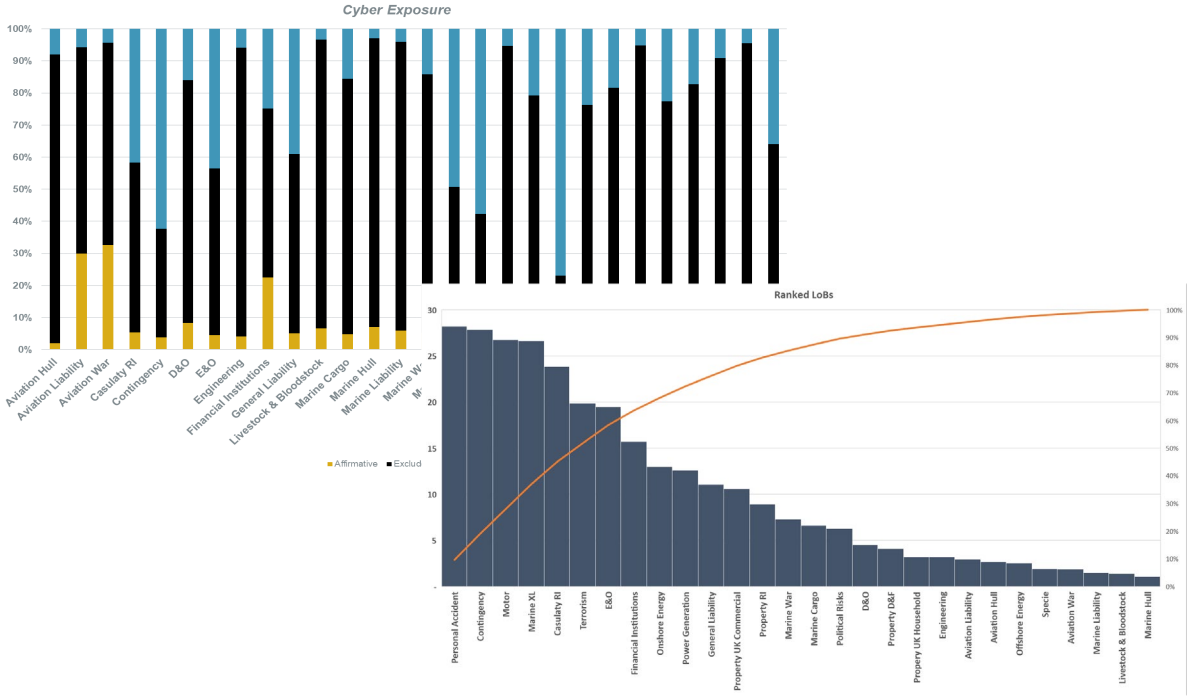
a) **Relevant to your business/exposures/policy wordings**

b) **Can be articulated and rationalise in a transparent way to management**

This is a complex problem so being able to articulate the process that derived the outcomes is key to gaining stakeholder confidence in you and your process

Risk Reporting MI

#	LMA Classes	Cyber Exposure		
		Affirmative	Excluded	Silent
1	Aviation Hull	2%	90%	8%
2	Aviation Liability	30%	64%	6%
3	Aviation War	33%	63%	4%
4	Casulaty RI	5%	53%	42%
5	Contingency	4%	34%	62%
6	D&O	8%	76%	16%
7	E&O	5%	52%	43%
8	Engineering	4%	90%	6%
9	Financial Institutions	22%	53%	25%
10	General Liability	5%	56%	39%
11	Livestock & Bloodstock	7%	90%	3%
12	Marine Cargo	5%	80%	16%
13	Marine Hull	7%	90%	3%
14	Marine Liability	6%	90%	4%
15	Marine War	5%	81%	14%
16	Marine XL	3%	47%	49%
17	Motor	4%	38%	58%
18	Offshore Energy	5%	90%	5%
19	Onshore Energy	5%	74%	21%
20	Personal Accident	2%	21%	77%
21	Political Risks	7%	69%	24%
22	Power Generation	6%	75%	18%
23	Property D&F	5%	90%	5%
24	Property RI	7%	71%	23%
25	Property UK Commercial	6%	77%	17%
26	Propery UK Household	7%	84%	9%
27	Specie	6%	90%	4%
28	Terrorism	5%	59%	36%



- What do management need to know/understand about the silent cyber problem?
  - Peak exposures
  - Wordings usage
  - Potential vulnerabilities/single point of failures/industries at risk
- If a LoB is perceived as being excluded be clear with management on the confidence of that exclusion.
- There is a difference between single loss and systemic scenarios e.g. clauses may be more susceptible stand-alone vs an accumulation event and visa versa. Make sure management are aware of the potential of both
- Is there a scenario your business should be concerned about?

Silent Cyber Scenarios

Justyna Pikinska

September 19

Counterfactual Analysis:
Cyber Scenarios and Real Life Examples

1. Energy Grid Blackout

Overview:

- Limited **power distribution** leads to regional blackouts
- **Large loss and accumulation**: insurers face claims in many lines of business, including large commercial accounts, energy, homeowners, and specialty lines
- **Big BI loss potential** via many triggered policies due to interruption of incoming electricity service (and CBI)

Coverages: **PD, BI, CBI**

Impact: **$20Bn - $70Bn Insured Loss**

Real Life Examples:

- Ukraine blackout (2015)
- *University of Cambridge & Lloyd's: US Blackout Scenario*

2. Industrial Plant (ICS)

Overview:

- **Fire / explosion** loss as a result of a targeted hacking incident
- Threat of specifically targeted attacks on industrial control systems (ICS)
- **High aggregation potential**: Risk of attacks on multiple plants by targeting same ICS
- Insurers face potential sizeable claims for fire and explosions at several major industrial facilities

Coverages: **PD, BI,** Third Party, Envirom

Impact: **$500m - $1Bn**

Real Life Examples:

- German Steel Mill (2014)
- UAE solar power plant (2011)
- Stuxnet/Iranian nuclear power plant (2010)
- *University of Cambridge: Cyber-Induced Explosion in a Chemical Facility Scenario*

3. Machinery Breakdown

Overview:

- New automated technology may lead to increased **machinery breakdown** risks, resulting in large business interruption and delayed / stopped production lines or construction projects and wiped out data
- This may have a significant knock-on effect on the **Supply Chain** structure and cause CBI losses

Coverages: PD, **BI, CBI**

Impact: **Industry Driven (NotPetya $3.3Bn)**

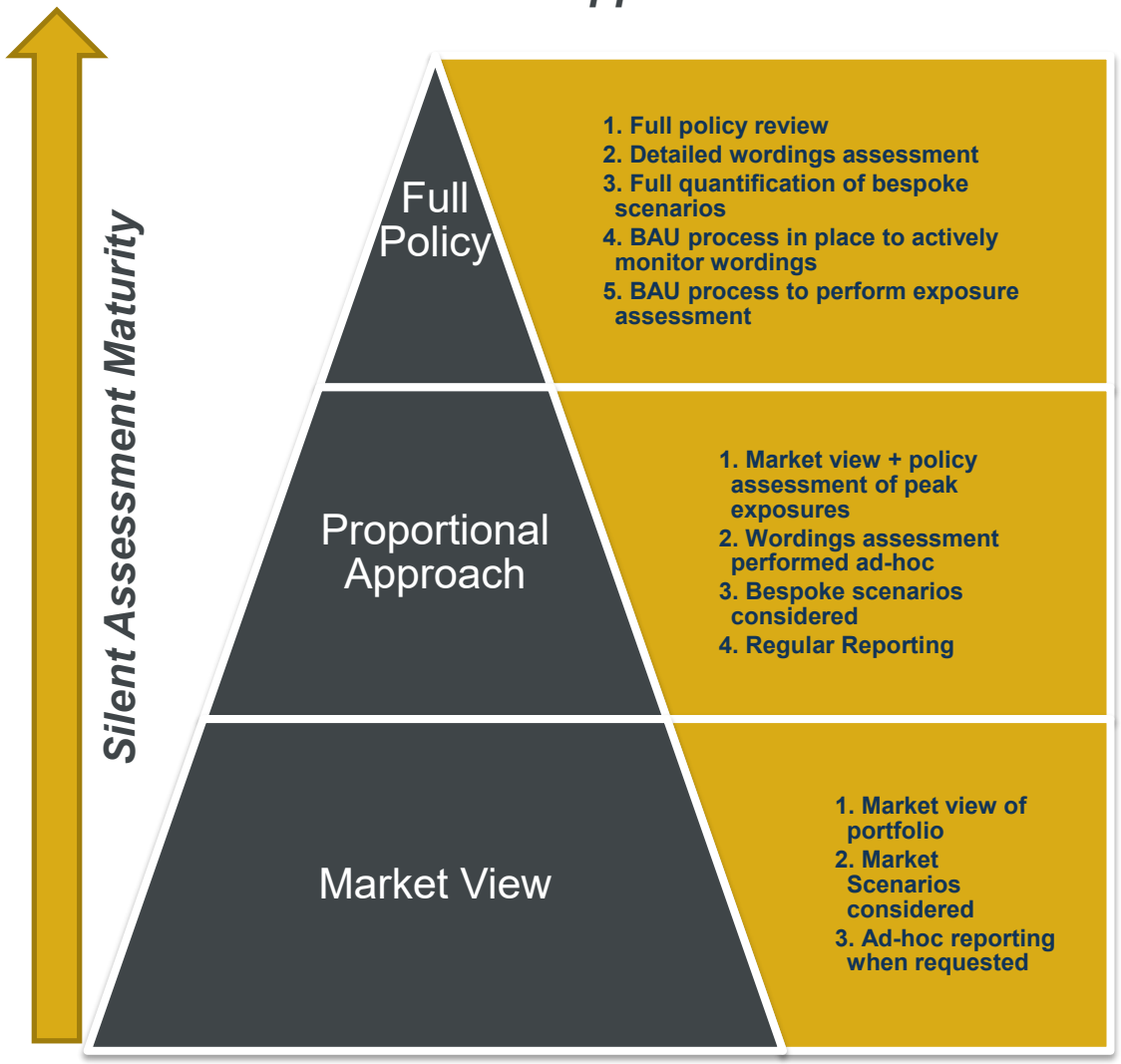
Real Life Examples:

- NotPetya / Merck (2017)
- WannaCry (2017)
- Delta airlines outage (2016)
- Cookie factory Canada (2015)
- *Semiconductor Production Outage Scenario*

Summary

1. **PRA survey's key findings**
   - Considerable exposure to silent cyber across traditional lines of business
   - Quantitative assessments of non-affirmative risk not well developed.
2. **Framework**
   - Proposed to help actuaries assess non-affirmative exposure cover
   - Help focus a structured process for silent scenario generation.
3. **Based on market views**
   - Framework users must review from own company perspective
   - Be aware of upcoming changes to cyber wordings (e.g. Lloyds/LMA initiatives)
4. **Application of framework**
   - Level of use will depend on your own journey to date
   - Some firms will be advanced whilst others starting the journey
   - May want to use to benchmark your own thinking

Framework Application



Questions

Comments

Institute and Faculty of Actuaries

Appendix

09 September 2019

Not Petya:
Significantly Impacted Companies

Loss: $790m - $1bn

- ✓ Malware led to a global disruption, including manufacturing, research and sales operations
- ✓ Permanent damage to 55,000 computers, emails disabled and 70,000 employees forbidden from using PCs
- ✓ **$460m** impact on sales, **$330m** impact on marketing and admin expenses
- ✓ Most operations restored within **6 months**

Cyber Policy: $275m **total loss**
Property Policy: Claiming excess of $275m

- ✓ Reports that Merck are attempting to recover under the PD/BI provision of their Property Policy to cover costs in excess of their affirmative policy.

Loss: $180m

- ✓ Malware infected significant portion of **global sales**, **distribution** and **financial** networks
- ✓ Permanent damage to **24,000 laptops** and **1,700 servers**
- ✓ Negative impact of 0.4% on net revenue **($104m)**
- ✓ Unfulfilled orders and disruption to shipping of snacks
- ✓ Majority of systems restored in **36 days**

Cyber Policy: None
Property Policy: Claiming $100m

- ✓ Mondelez are claiming under the following provision:

"physical loss or damage to electronic data, programs or software" caused by "malicious introduction of a machine code or instruction"

War Exclusion - Zurich

Loss: Unknown (Millions $)

- ✓ **No access to emails for 4 days**, court hearings postponed
- ✓ Every data centre and Windows server impacted globally
- ✓ Paid 15,000 hours of OT to IT workers to recover from incident
- ✓ Had to **recreate their entire Windows environment** after attempting to salvage old systems for two weeks

Cyber Policy: Unknown
Property Policy: N/A
K&R Policy: Speculated

- ✓ News articles citing some insurers are denying the NotPetya claim with DLA Piper on a War Exclusion