XII CONGRESSO NAZIONALE degli ATTUARI

Cyber Risk

XII Congresso Nazionale Attuari

Massimiliano Arizzi

22/11/2018

What is it?

The Institute of Risk Management:

"… any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."

Malicious Insider	▪ Growing incentive for insiders to abuse access to sensitive data for financial gain ▪ Disgruntled current and former employees exploit back-doors ▪ Access controls and behavior monitoring insufficient to detect insider threats
Negligent Insider	▪ Unwary insiders susceptible to attacks that exploit traditional security controls ▪ Users who fail to embrace "culture of security" will find ways to circumvent 'inconvenient' security controls
Criminal Hackers	▪ Tactics have evolved from "hit and run" to "infiltrate and stay." ▪ Industrialization - Black markets exist for all types of personal information ▪ Proliferation of mobile platforms and BYOD policies creates new vectors
Hacktivists	▪ Intent is to disrupt and/or embarrass a target ▪ Motivations are fickle and unpredictable ▪ Massive DDoS attack
Cloud or 3rd party Compromise	▪ Theft of Intellectual Property ▪ Security compromise – loss of sensitive client data ▪ Infrastructure downtime may lead to Dependent Business Interruption claim

Type of Coverage

1st Party

Network Interruption – Costs associated with the loss of profit or increased cost of working from a Cyber Attack (or by extension, any loss of IT function), typically utilises a waiting period or time deductible before cover is given. Calculation basis forms part of the policy wording

Data Restoration – Costs associated with the attempt to restore data

Crisis Management Expenses

i. IT Services – Costs associated with the restoration of the network or IT system to pre-loss conditions
ii. Reputational Protection – Costs associated to hire Lawyers or Public Relations Professionals to mitigate reputational damage
iii. Notification Costs – Costs regarding the notification of data subjects of the release of their personal data
iv. Credit and ID Monitoring – Costs regarding the purchase of protection or identification monitoring for data subjects who's personal data has been lost

Cyber Extortion - Pays credible extortion demands and response costs to demands for money against threats to release or destroy private information, or take down a network.

3rd Party

Network Security Liability - Covers third-party claims arising from an inability to use or access your network, infection of networks of others, information damage to other networks, inability of others to rely upon the accuracy, validity or integrity of their information residing on your network

Data Privacy Liability - Third-Party Claims arising from the unauthorized disclosure, loss, theft, etc. of private information in violation of privacy laws, government privacy regulations or institutional privacy policies.

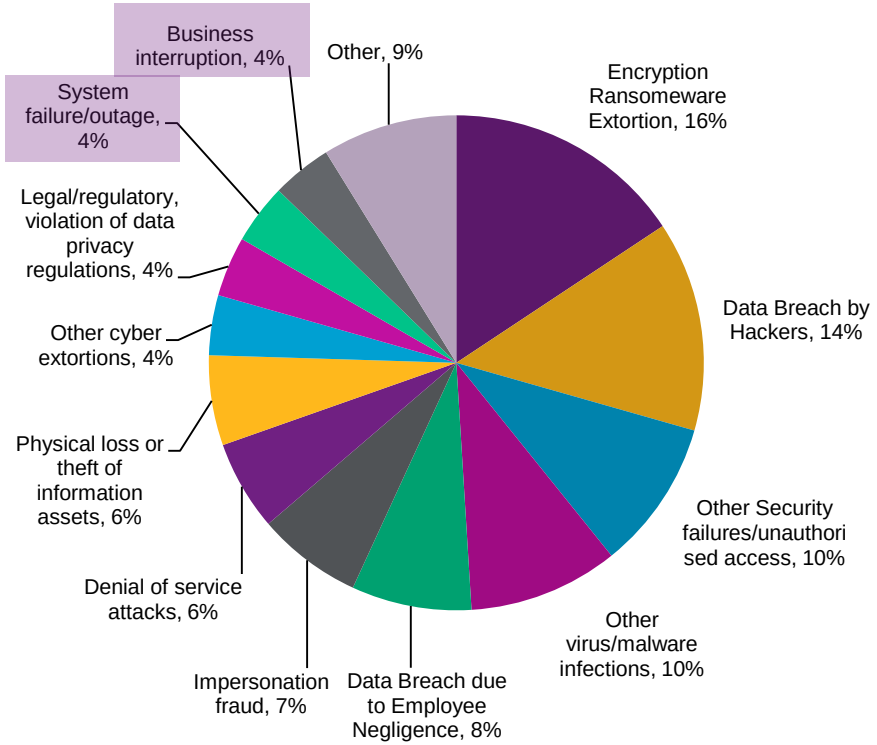
Multimedia Liability - Coverage for indemnity and defences costs for third party claims alleging media wrongful acts in connection with media content in any form

Privacy Regulatory Defence & Penalties - Covers defence of a preliminary regulatory investigation and/or formal proceeding brought by a privacy regulator. Also covers fines and penalties imposed where insurable by law.

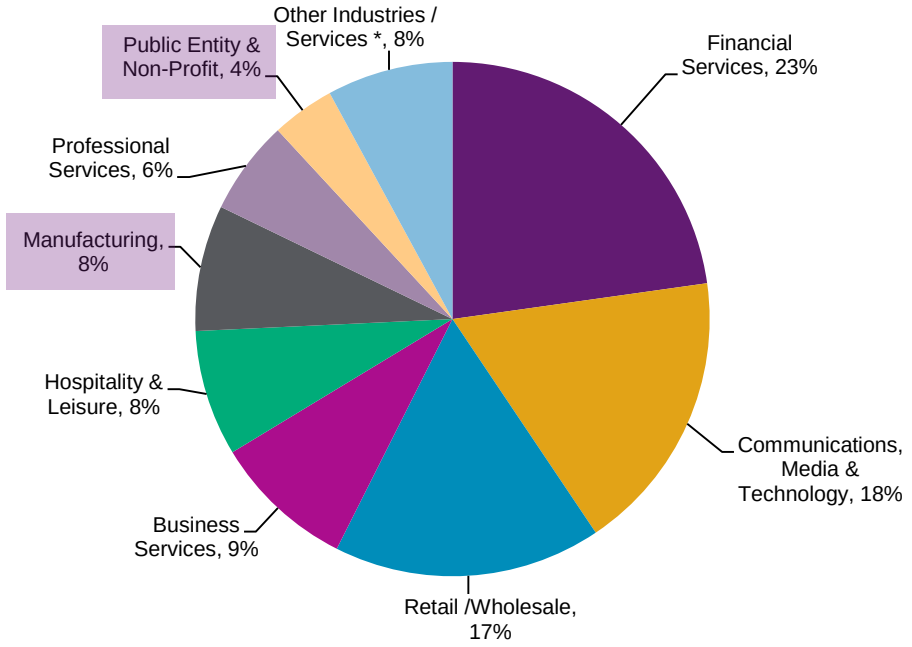
Payment Card Industry Fines & Assessments – Covers defence of a preliminary regulatory investigation and/or formal proceeding brought by under the Payment Card Industry Data Security Standard. Also covers fines and penalties imposed where insurable by law.

Cyber Claims - the norm

Cyber Claims received by AIG EMEA (2013-2016) by Type



Cyber Claims received by AIG EMEA (2013-2016) by Sector



Source: AIG Claims Intelligence: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-intelligence-cyber.pdf

Cyber Losses – The largest in history

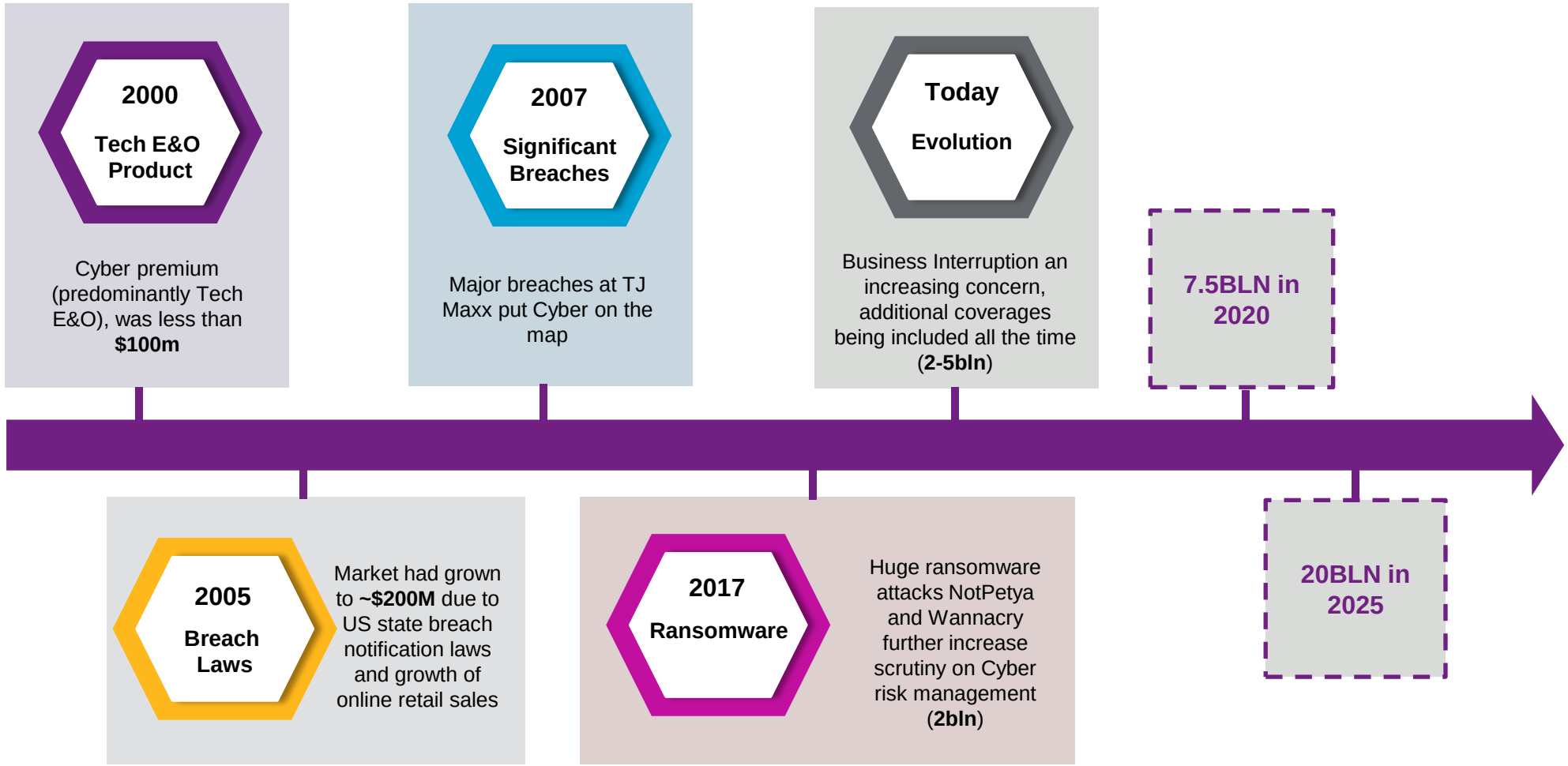
Single Losses

- **Yahoo!** - $350 million drop in acquisition value to Verizon
- **Home Depot** - $298 million reported loss, $100 million cyber insurance recovery expected
- **Target** - $291 million reported loss, $90 million cyber insurance recovery expected
- **TJX** - $170 million reported loss
- **Heartland** – $148 million reported loss, $31 million cyber insurance recovery paid
- **RBS WorldPay** -- $190M costs due to data breach
- **Morgan Stanley** -- $13M in regulatory and Breach Response costs; No litigation
- **Staples** -- $150M Cyber insurance funds paid
- **Anthem** -- $100M Cyber Insurance funds paid

Event Losses

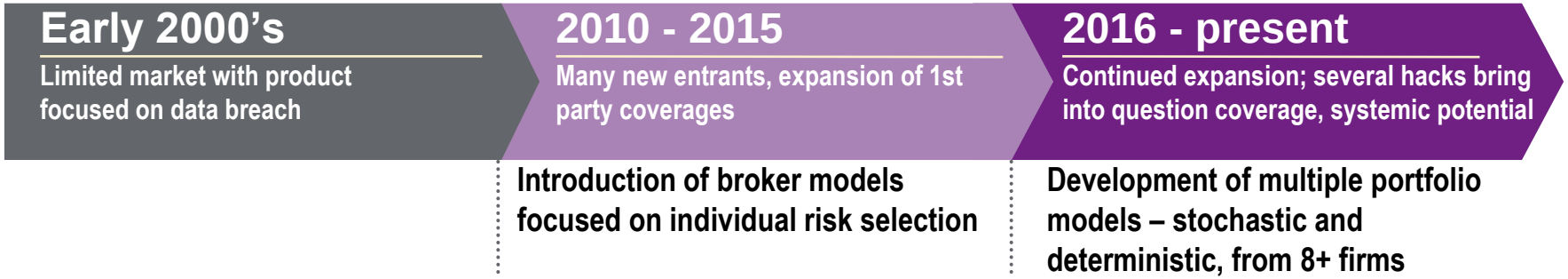
- **NotPetya** – June 27, 2017 Attacks
  - Saint-Gobain – Estimated sales loss of $387 million by year end - $76 million operating income 1H17
  - FedEx/TNT – $300 million loss of revenue
  - Maersk – $200 million to $300 million projected loss 3Q17
  - Mondelez International – Estimated loss of $150 million
  - Reckitt Benckiser - $142 million expected loss in 2Q17
  - Nuance Communication – $90 million to $110 million in estimated losses 3Q and 4Q
  - Beiersdorf - $41 million reported loss
  - Merck – $400 million reported loss

Evolution of the Market - From threat to opportunity



Cyber Modelling

- Early cyber models have been around for several years but the last 12-24 months has seen “analytics arms race” as focus has shifted



- **Stochastic** models
  - Focus is to quantify downside potential for data breach and business interruption
  - There are also scenario based models that focus on the systemic potential
- **Deterministic** models
  - examine the potential severity from specific event characteristics
- It is a vibrant market with many vendor model companies at the stage of developing new propositions

The modelling framework today

General Cat Model Progression

Forward-looking stochastic scenarios inspired by attributes of historical events

Applied to Client's portfolio of exposures

Add uncertainty surrounding events

Output is full set of return period losses

Details on tail losses to identify systemic events, industries, and companies driving extreme losses

Property Cat Model

Hurricane hits Miami with 90 MPH winds

Insured locations construction and occupancy in the storm path

Frame homes have losses equal to 10% of value

Cyber Cat Model

Systemic events such as cloud service provider outages and zero-day vulnerabilities

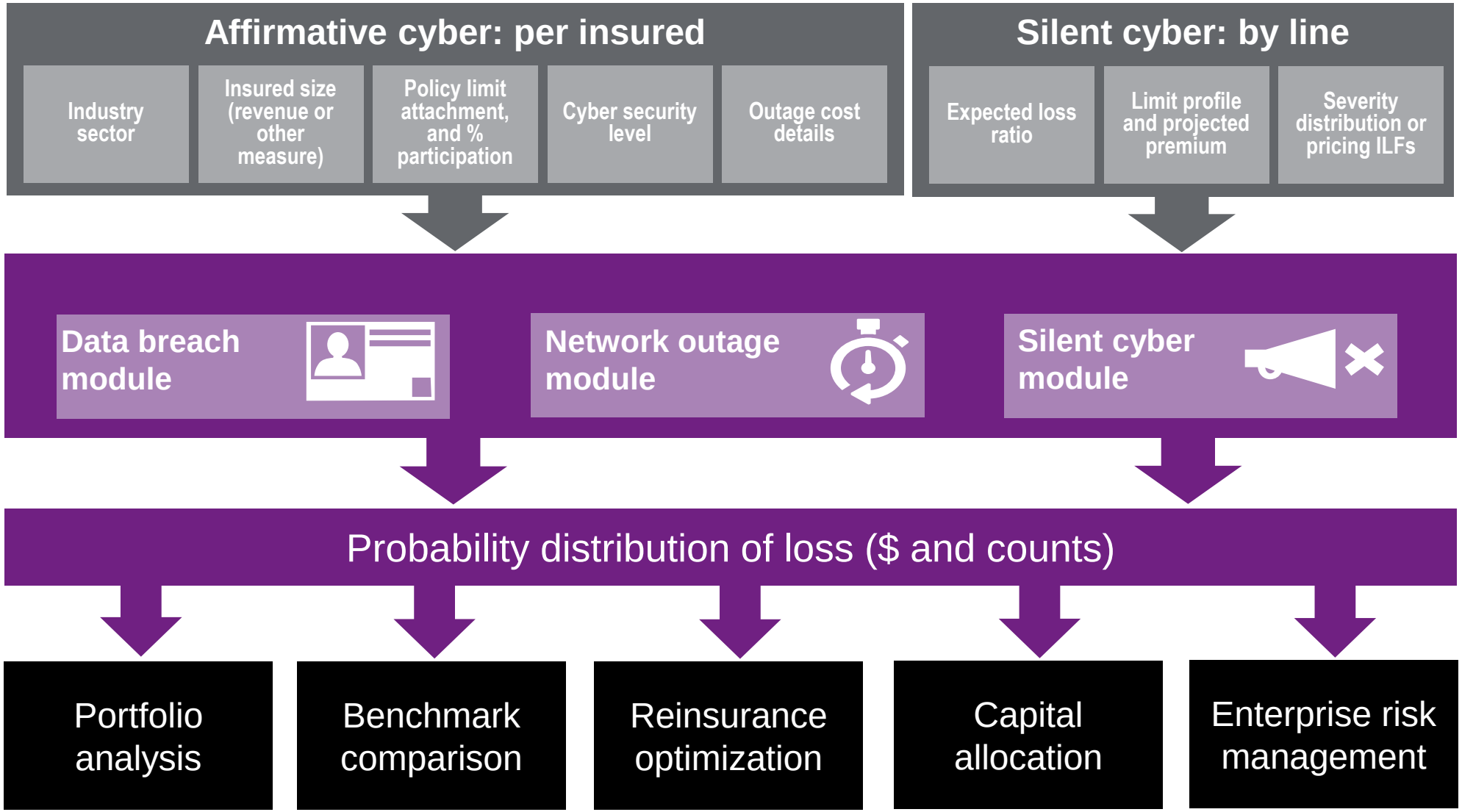
Insured characteristics: industry sector, exposure size, website domain, cyber security level, etc.

4 policies are expected to have at least 1 data breach in a given year

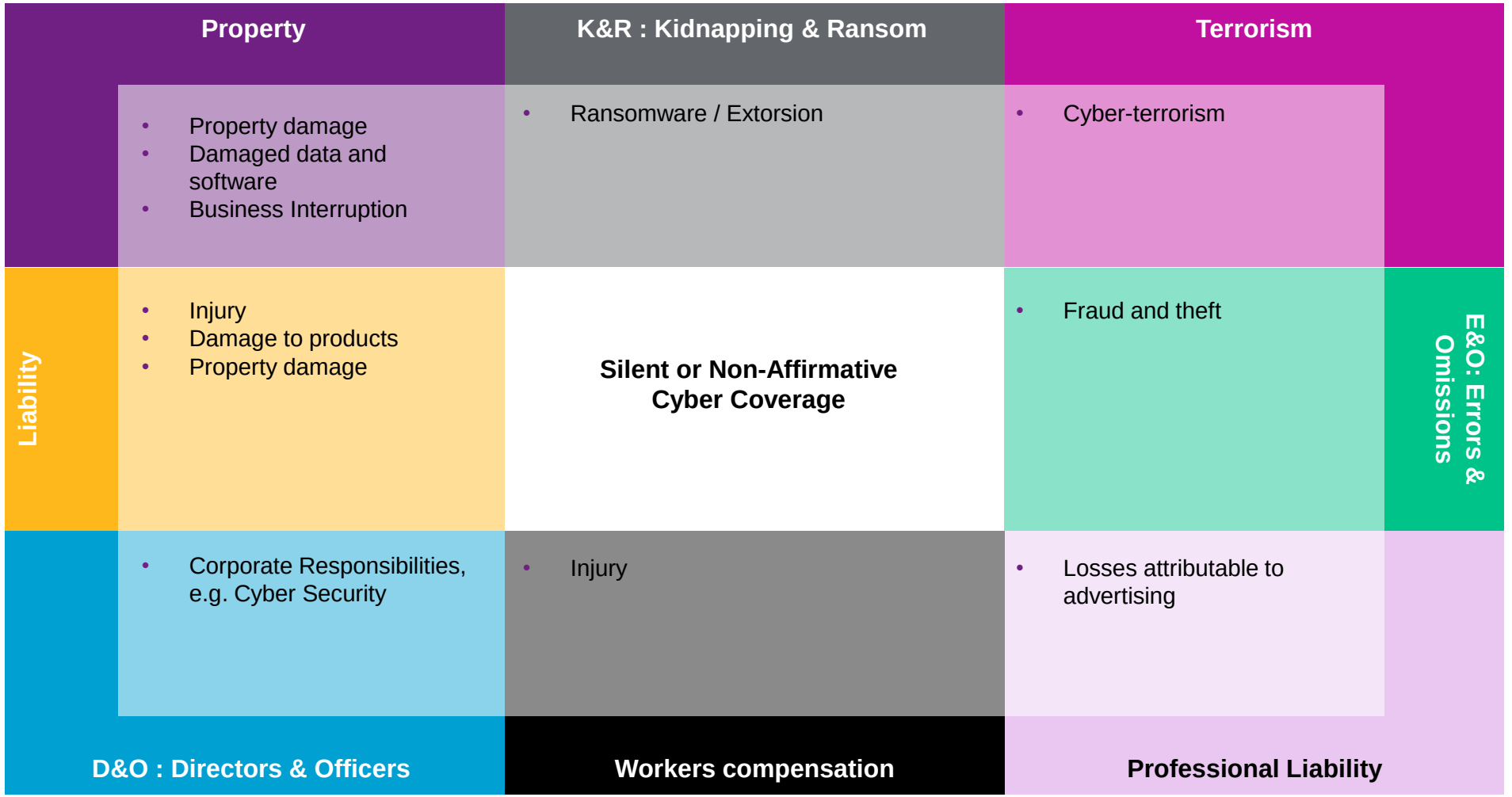
Probability distribution of loss

Details on tail losses to help analyze portfolio, manage downside risk & satisfy rating agency requirements

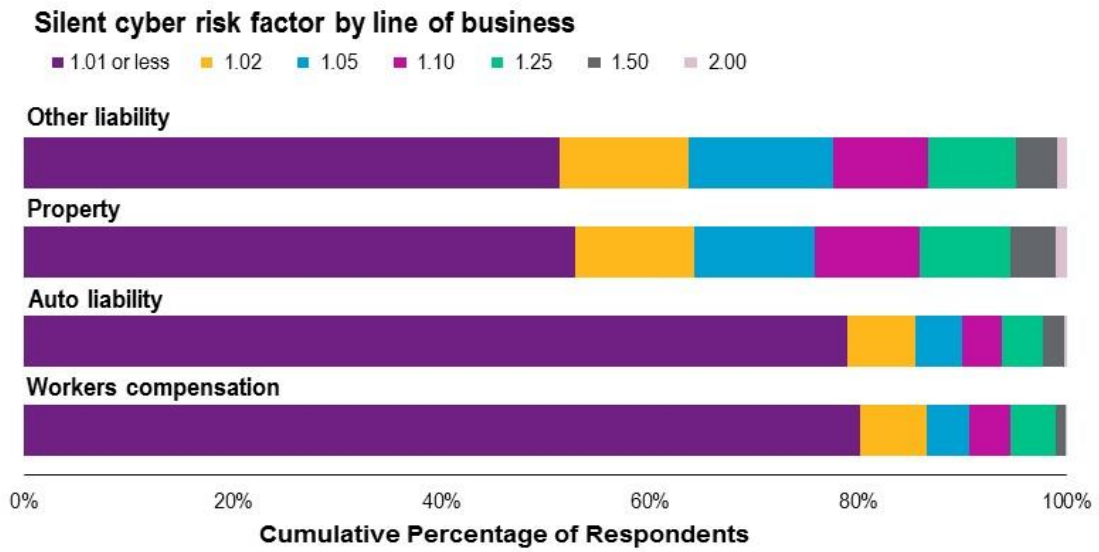
Cyber modelling framework – a case study



Silent Exposure within traditional policies



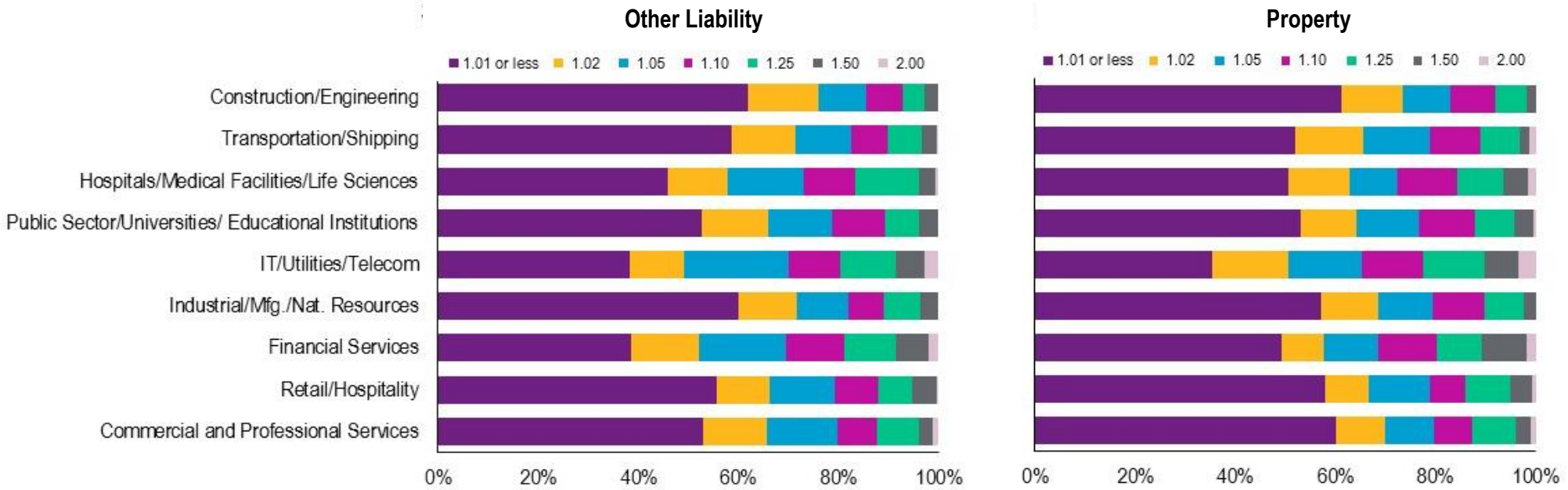
Silent Cyber modelling framework



- Silent cyber risk factor:
  - 1.01 = one cyber-related loss for every 100 non-cyber related losses
  - 1.50 = 50% more covered losses due to cyber

- Significant uncertainty over silent cyber exposure potential:
  - >50% respondents estimated silent cyber risk factor to property as 1.01 or less
  - >1% respondents estimated additional property loss due to silent cyber to be 100%
- Material variation in degree of anticipated silent cyber risk between lines:
  - AL, WC: more than 75% respondents estimated the risk factor as 1.01 or less
  - Property, Liability: around 50% respondents estimated the risk factor to be 1.02 or more

Silent Cyber modelling framework



- **Construction/Engineering** and **Industrial/Manufacturing/Natural Resources** were seen as relatively low silent cyber risk due to smaller perceived data breach threat
- **Hospitals/Medical Facilities/Life Sciences**, **IT/Utilities/Telecom** and **Financial Services** were seen as higher risk as these industries consistently handle consumer information and with larger perceived threats to utilities infrastructure