Institute
and Faculty
of Actuaries

IFoA GIRO Conference 2024

18–20 November, ICC, Birmingham

Institute and Faculty of Actuaries

Cyber: evolving threat landscape and the reserving challenges

Chehak Jain | Paul Goodenough

IFoA GIRO Conference 2024

Notable (Re)Insurance milestones

1666 Great Fire of London – Property Fire insurance

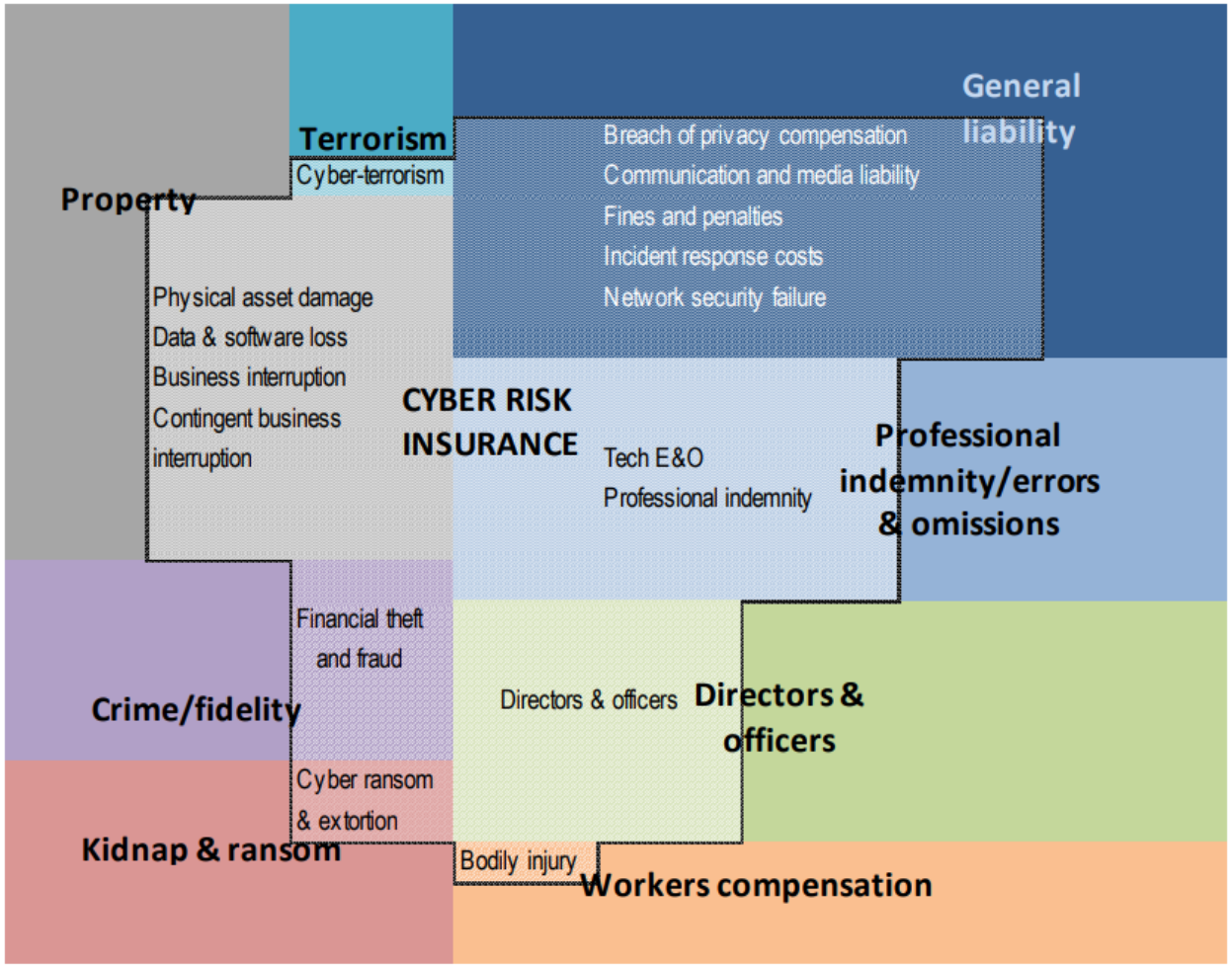
1842 Hamburg Fire & 1861 Glarius Fire – Reinsurance
(Swiss Re & 1st reinsurers)

1886 Motor car invented – Motor Insurance
(Travelers, 1897)

1903 Wright brothers - Aviation insurance
(Lloyd's of London, 1911)

1970s/80s Computer virus - Liability add-ons / Cyber insurance
(Steven Haase, 1997)

Cyber insurance – a messy moveable feast



Source: OECD based on JLT Re (2017).

"What makes cyber risk different is that it is not a single type of risk, that it extends to and interconnects nearly every other type of risk....in a way so unpredictible and unprecedented that is hard to imagine these actuarial complexities being captured simply by the collection of more data or the use of more sophisticated modeling tools"

Cyberinsurance Policy, Josephine Wolff

- "Implicit" Silent Cyber
- "Packaged"
- "Standalone"
- Emerging specific considerations
  - Insured/insurer relations; e.g. Cyber audit vs. vendor partnership
  - Wordings, e.g. War/Terrorism
  - 'Fines'

Risk evolution pre-2010

1949 Theory of virus	Early 1970s First virus and antivirus	1976-2006 Insider attack on Boeing	1987 Launch of Commercial Antivirus	1988 Morris Worm	1990s Ascent of Internet	2000s Organized crime
• Concept of computer virus was theorised by John von Neumann	• First virus called Creeper in 1971– purely experimental and no malicious intent • First antivirus called Reaper in 1972 to delete Creeper	• Over 30 years, an employee stole $2bn of aerospace docs and gave them to China • Threat to Boeing and to the entire country	•Andreas Lüning and Kai Figge released their first antivirus product for the Atari ST. •Three Czechoslovakians created the first version of the NOD antivirus •John McAfee founded McAfee and released VirusScan.	• Oldest worm on the internet written by a graduate student at Cornell University • Resulted in first felony conviction in the US under 1986 Computer Fraud and Abuse Act	• Worst virus outbreaks were Melissa and iloveyou and were created by individual entities, usually college students. • Outbreaks had global impacts due to interconnected nature of internet	• Information security grew but so did the viruses, now as a result of more organized crime. • Cyber espionage grew, as evidenced by Flame malware and Stuxnet worm

- First digital computer was built in early 1940s
- Type of cyber attacks have evolved significantly over the years: From ‘bad actors’ trying to make a point to global outbreaks
- Early Ransomware, emergence of espionage, data theft
- Advancements in technology and changes in attacker motivations set the stage for 2010 and beyond

Risk evolution post-2010

Massive data breaches at Yahoo!, Sony, US OPM, Equifax

Leaks of classified documents: NSA, Wikileaks, Snapchat

Big ransomware attacks Wannacry, wiper malware NotPetya

Malware and Ransomware as a service, Log4j, multi-extortion tactics, AI generated threats

Non malicious threats e.g. Crowdstrike

2010 onward: cybercrime escalated and data privacy became a central concern

- First known ransomware attack was in 1989 – called the AIDS trojan, the attack demanded $189; WannaCry demanded much more
- New attack vectors and new defence mechanisms such as usage of machine learning and AI on the rise; What's next – Quantum computing? Biometric data security challenges? 5G and edge computing risks?

GAO-21-477, Accessible Version, CYBER INSURANCE: Insurers and Policyholders Face Challenges in an Evolving Market

Check if your email has been in a data breach

https://haveibeenpwned.com/

Cyber risk categorization

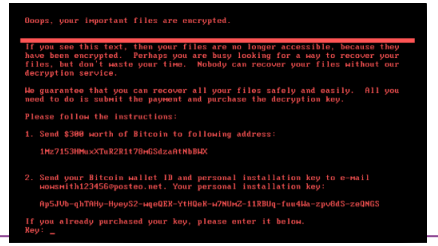
First party risks

- **Directly endangers the organization from accidental or hostile action**, e.g. loss of revenue due to internal systems being impacted by malware.
- Further categorised into business interruption, data breaches, malware attack and cyber extortion, computer and funds transfer fraud, property damage, identity recovery
- Insurance coverage for these risks include paying for remediation, forensic investigations, restoration, mitigation efforts to restore reputational damage. Examples include paying ransom to cyber extortionist, reimbursing company for lost revenue

Third party risks

- Risk of third parties claiming that your **business is liable for damage due to cybersecurity incident for which you are responsible**.
- Further categorised into network security liability, information security and privacy liability, electronic media liability, regulatory defence and penalties / PCI costs
- Insurance coverage for these risks include defence litigation and settlement costs.
- Lines may be blurred between first and third party if both the business and their clients are impacted

When network infrastructure is compromised, there can be different types of impacts.



Case study: NotPetya and Crowdstrike

NotPetya – Wiper malware as a weapon of war?

The NotPetya attack occurred on June 27, 2017, and was initially believed to be ransomware. However, it was later identified as a wiper malware designed to destroy data rather than encrypt it for ransom. The attack was attributed to the Russian military intelligence agency, the GRU, and targeted Ukraine but quickly spread globally, causing significant damage to many organizations, major ones being Maersk, Merck, Mondelez

Lawsuits and Settlements

Mondelez vs. Insurers: Mondelez filed a lawsuit against their insurer for denying coverage under its property insurance policy, arguing that it covered cyberattacks. The insurer claimed that the NotPetya attack was a “hostile or warlike action”. The case was settled out of court, but the terms were not disclosed.

Merck vs. Insurers: Merck sued its insurers over denied claims, arguing that the NotPetya attack did not fall under the policy's war exclusion. Merck eventually won a $1.4 billion settlement, with the court ruling that the attack was not an act of war.

Cyber Risk Classification

First-Party Cyber Risks: In the case of NotPetya, companies like Merck and Mondelez experienced first-party risks as their own systems and operations were directly impacted.

Multiple blue screens of death caused by a faulty software update on baggage carousels at LaGuardia Airport, New York City

Crowdstrike

On July 19, 2024, a routine software update for CrowdStrike's Falcon sensor program caused a global outage. This faulty update affected over 8.5 million Windows-based systems across various industries, including airlines, banks, hospitals, and emergency services. The outage led to significant operational disruptions and financial losses.

CrowdStrike faced multiple lawsuits as a result. Notable ones include

Delta Air Lines: Threatened to sue CrowdStrike for up to $500 million in damages. Delta experienced significant flight delays and operational disruptions due to the outage.

Shareholders: Filed a class action lawsuit against CrowdStrike, alleging that the company misled them about its software testing procedures. The lawsuit claims that CrowdStrike's share price fell by 25%, wiping out $22 billion in market value.

Microsoft: Although not a direct lawsuit, Microsoft was drawn into the situation as the faulty update affected Windows machines.

Cyber risk classification

First-Party Cyber Risks: The downtime and operational disruptions experienced by CrowdStrike and its customers due to the faulty update are considered first-party risks

Third-Party Cyber Risks: These risks involve claims from third parties who suffered damages which they were potentially not responsible for. In this case, Delta Air Lines and other affected companies filing lawsuits against CrowdStrike are examples of third-party risks.

What characteristics of a cyber event would make it a cyber catastrophe?

Join at

slido.com

#CyberTalkGIRO

What characteristics of a cyber event would make it a cyber catastrophe?

For Wordcloud output <TBD with on-site technicians>

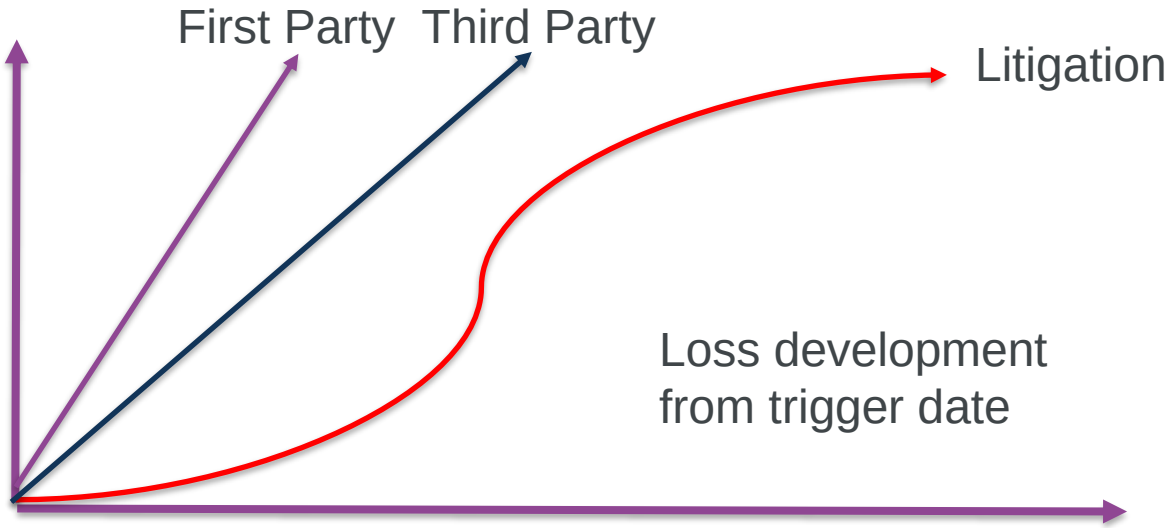
Cyber CAT & Claims: Data Collating and Categorisation

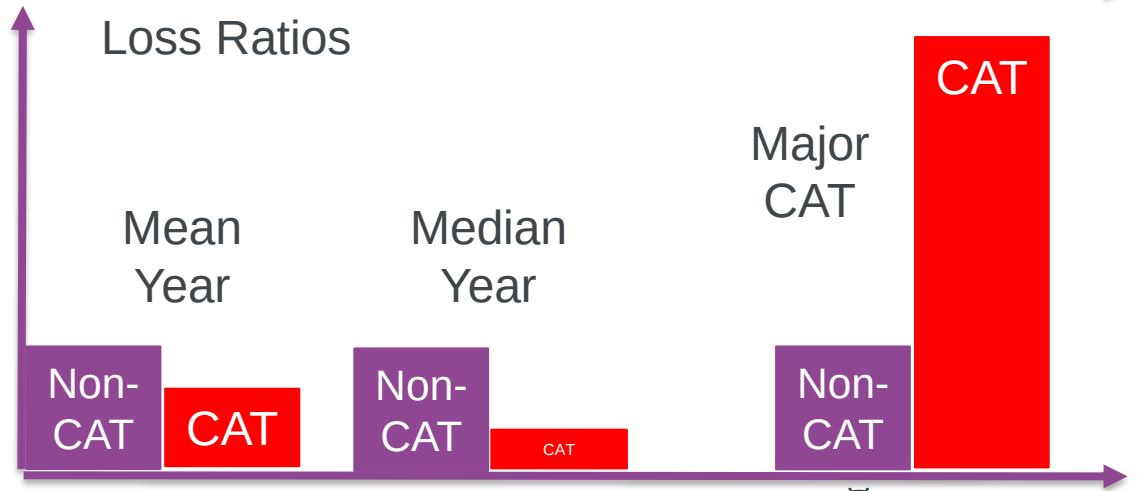
Claims Data collection

- First vs. Third Party
- Non-CAT vs. CAT
- Malicious vs. Non-malicious
- Modelled/non-modelled
- Litigation

Loss Ratios – CAT / Non-CAT

- Frequency / Severity
- Loss Trends, Rates, T&Cs
- Mix of business
- Primary vs. Excess
- Thresholds
- Modelled / Non-modelled





From a reserving perspective, do you think cyber is different to the other lines and why?

Join at

slido.com

#CyberTalkGIRO

From a reserving perspective, do you think cyber is different to the other lines and why?

For Wordcloud output <TBD with on-site technicians>

Cyber reserving challenges: Is Cyber really different to other insurance classes?

DATA

What data should be collected?

Unstandardized data across the market (e.g. rate change, ransomware frequency)

Changing nature of losses

Changing nature of coverage (affirmative, silent cyber, state backed cyber attack exclusion)

Accumulation of risk due to systemic nature of cyber attacks

Modelling Frequency and severity is essential but quite volatile

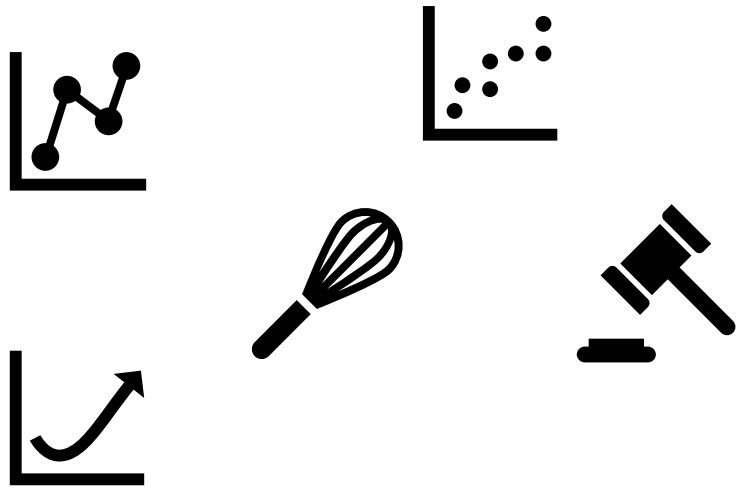
Will traditional triangulation reserving techniques work?

Organizational, cross – functional and communication hurdles

Lack of expertise

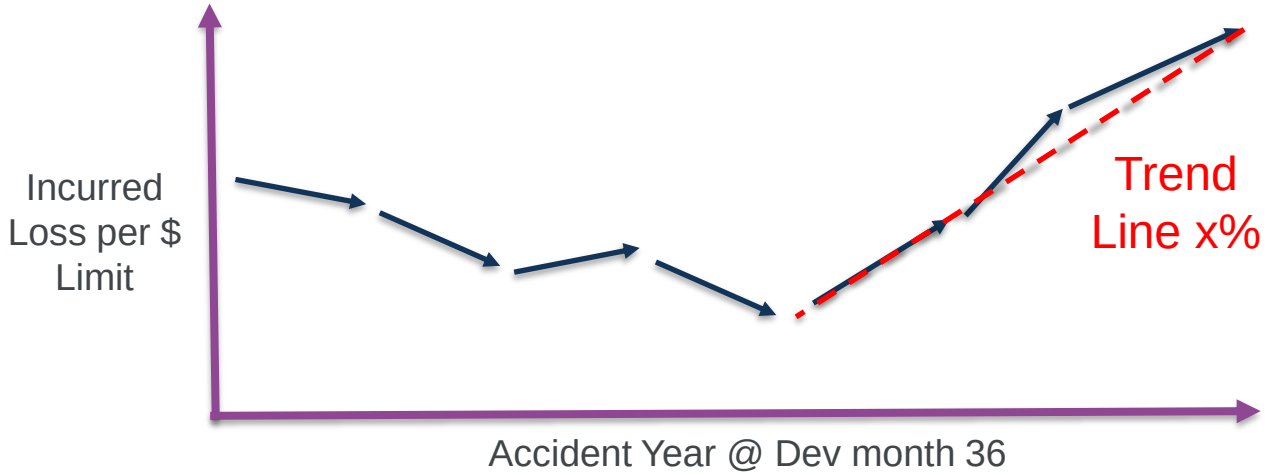
Reserving practical approach

- There is NO fundamental difference in the actuarial techniques and judgments used for Cyber reserving and non-Cyber reserving
- The balance: pessimism; strangling a new product by conservative assumptions vs. Optimism; not allowing for as yet unrealised downside risks or changes to risk
- Homogeneous Groupings; Year-on-year stability in Cyber is volatile
  - Loss trends and rates; rapid softening/hardening
  - Mix of 1st party and 3rd party changing
  - Correlation of 1st and 3rd party increasing
  - Litigation / Systemic development / ENIDs
  - Changing propensity for insureds to notify insurers
  - Correlation to other lines of business may exist
- *Unearned & CAT reserving risk are the big ones*

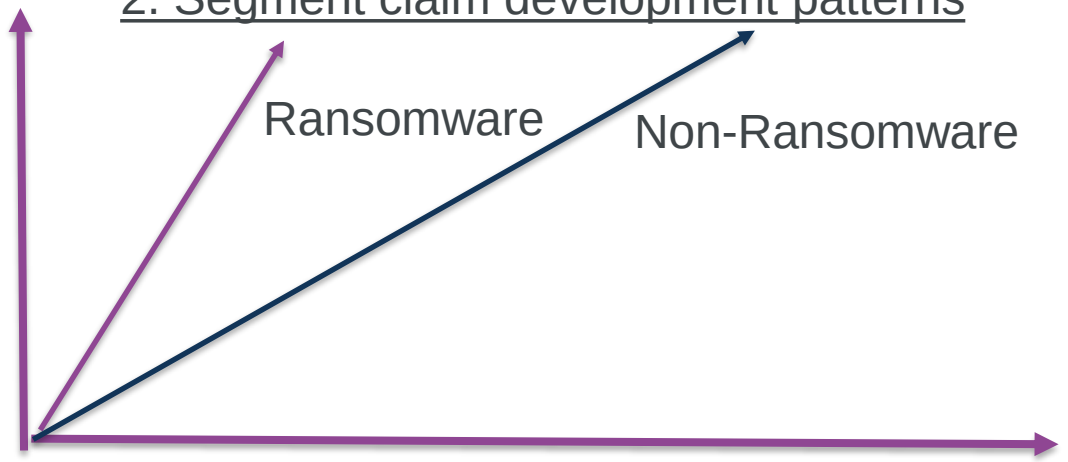


Reserving metric examples

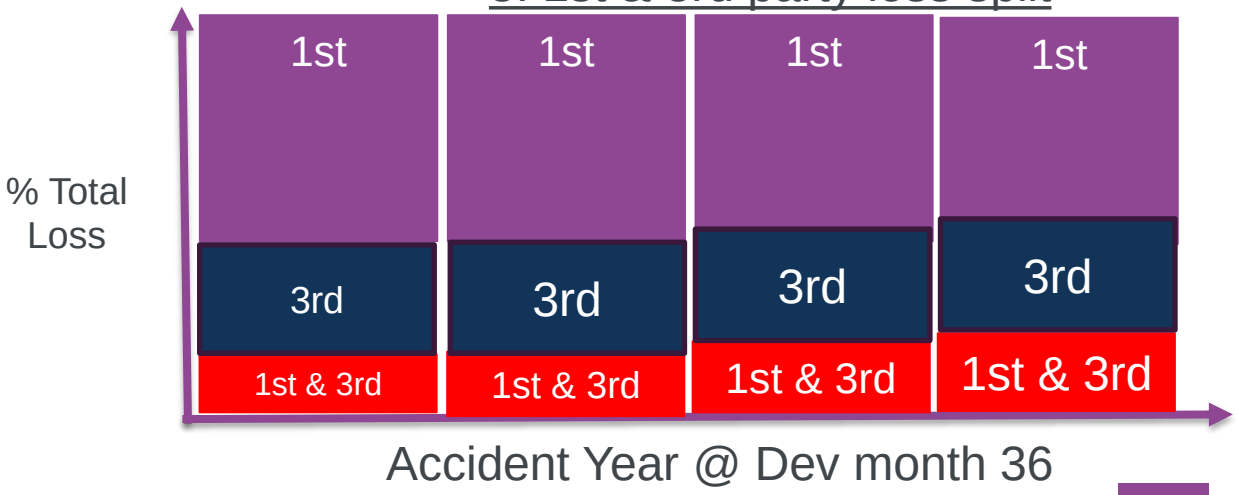
1. Incurred loss trends



2. Segment claim development patterns



3. 1st & 3rd party loss split



4. Reserve Risk CVs

Line of Business	Non-CAT CV (Highest 1st)	Line of Business	CAT CV (Highest 1st)
LOB A	%	LOB A	%
LOB B	%	Cyber	%
Cyber	%	LOB B	%
LOB C	%	LOB C	%

Cyber Reserving metrics

• There is NO fundamental difference in the metrics used for Cyber reserving and non-Cyber reserving	→ More focus should be used where risks are changing rapidly and actuarial data less mature
• To start keep data collection & metrics simple...accuracy, completeness and timeliness...consistency, transparency and liquidity	→ Don't put barriers up to making the 1st step. Be consistent with models as helps monitor assumptions after modelled loss/Cyber CAT
• Ensure categorisation & governance agreed or discussed with other stakeholders	→ Claims, underwriting and risk. Joined up but challenge.
• Know the reliances, limitations and expert judgments underlying your reserving model	→ Monitoring and adding alternative granularity is a strong validation
• Regularly communicate, and don’t forget benchmarks and the bigger picture	→ Communicate on findings in this context to Reserve Committees/Boards; encourages challenge and discussion

Risk mitigation strategies for Insurers

- Policy characteristics / coverage terms
  - Self insured retentions, sub-limits, aggregate limits
  - Waiting period for business interruption coverage
  - Exclusionary language to limit insurer's liability; examples include war and hostile act, nuclear, errors or omissions in programming etc.
- Changing UW guidelines (e.g. MFA, secured offline backups, privileged access management, EDR solutions)
- Longer cyber risk assessments to determine insurance eligibility
- Continuous threat exposure management (CTEM) essential
- Management of cyber risk via cyber CAT bonds, Reinsurance, ILS, parametric covers

Regulatory considerations

- 2003 California Law on data breach reporting
- 2011 SEC issue guidance on cyber risk disclosure
- 2018 GDPR
- 2021 UK GDPR
- 2023 SEC reporting in material cyber incident within 4 business days of the incident

- Regulation, government policy and laws take decades to develop & mature
- Cyber risks continue to grow, e.g. automanous cars, generative AI, 'smart' tech
- The speed at which these risks emerge globally is unprecedented

Dear CEO Letter from PRA; "...work in 2024 will focus on ensuring that firms' capital and exposure management capabilities are commensurate to the growth in exposure, as well as the inherent volatility of this risk"

Today's capital and exposure management matters are tomorrow's reserving hot topics!

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 presenter.