Institute
and Faculty
of Actuaries

Spring Conference 2024

UK Cyber Insurance: Key reserving challenges and considerations

Lynette Calitz
Shamsul Haque

1 May 2024

Agenda

- The Cyber Risk landscape
- Cyber Insurance Cover
- Key Challenges and Considerations
- Cyber Reserving Methods
- Validating Reserve Adequacy
- Risk Mitigation Strategies
- Conclusion
- Q/A

Institute
and Faculty
of Actuaries

The Cyber Risk Landscape

1 May 2024

The Cyber Risk Landscape

Approximately 2.39 million cases of cybercrimes affected UK businesses in 2022 (1)

90% of UK organisations in 2023 have experienced greater exposure to cyber risks due to increased digitisation in the last two years (2)

An annual CEO survey for 2022 revealed that a catastrophic cyber-attack is considered as the number one loss scenario to consider under a resilience plan (2)

WannaCry was a global ransomware attack, which affected 200,000 computers in 150 countries with a $4bn loss globally and cost the NHS £92m (3)

The world economy is potentially exposed to a $3.5 trillion loss - Results from a major cyber-attack risk scenario run by Lloyd's of London (4)

Sources:
(1) Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)
(2) Cyber Security Outlook 2023 - PwC UK
(3) The Latest Cyber Crime Statistics (updated February 2024) | AAG IT Support (aag-it.com)
(4) Lloyd's systemic risk scenario reveals global economy exposed to $3.5trn from major cyber attack (lloyds.com)

Institute
and Faculty
of Actuaries

Cyber Insurance Cover

1 May 2024

Cyber Insurance Cover

First Party Cover

Third Party Cover

Exclusions

Cyber Insurance Cover

First Party Cover

- Covers financial loss from a cyber event to the insured party
- Main exposures are:
  - Damage to data and software
  - Business interruption
  - Extortion
  - Reputational damage
  - Theft of electronic funds.

Third Party Cover

Exclusions

Cyber Insurance Cover

First Party Cover

Third Party Cover

- Covers financial consequence of any liability actions brought against the insured due to a cyber event.
- Main exposures
  - Security and privacy breaches
  - Expenses to notify customers about a breach
  - Investigation
  - Defence costs
  - Damages arising from defamation, breach of privacy and intellectual property infringement
  - Loss of third party data.

Exclusions

Grant Thornton

Institute and Faculty of Actuaries

Cyber Insurance Cover

First Party Cover

Third Party Cover

Exclusions

- Antitrust Violation
- Bodily injury
- Property Damage
- Contractual liability
- War
- Terrorism
- Can vary among insurers.

Institute
and Faculty
of Actuaries

Key Challenges and Considerations

1 May 2024

Challenges and considerations for cyber insurers

Data and Long-tailed nature

Accumulation of risk

Silent Cyber

State-backed exclusions

Post-Covid-19 Working Environment

Geo-Political Risk

Ransomware

- Traditional reserving method assumption - past data a good indicator of the future
- Limited past claims data due to the low frequency and high severity nature of cyber insurance
- Fast-changing cyber risk landscape and technological advances – historical data less reliable for future predictions
- Long tail of the cyber claims due to the uncertainty in the settlement, regulatory fines, and third-party litigation.

Challenges and considerations for cyber insurers

- Data and Long-tailed nature
- **Accumulation of risk**
- Silent Cyber
- State-backed exclusions
- Post-Covid-19 Working Environment
- Geo-Political Risk
- Ransomware

- The biggest challenge
- Systemic nature of cyber attacks
- Interdependency structures between risks
- Interconnected loss scenarios
- Complex dependency structures

Challenges and considerations for cyber insurers

Data and Long-tailed nature

Accumulation of risk

Silent Cyber

- Refers to other classes unintendedly exposed to cyber risk.
- PRA supervisory statement, SS4/17, in 2017
- 2019 ‘Dear CEO Letter’
- Lloyd’s bulletin Y5258
- IFOA Silent Cyber Assessment Framework.

State-backed exclusions

Post-Covid-19 Working Environment

Geo-Political Risk

Ransomware

Challenges and considerations for cyber insurers

- Data and Long-tailed nature
- Accumulation of risk
- Silent Cyber
- **State-backed exclusions**
- Post-Covid-19 Working Environment
- Geo-Political Risk
- Ransomware

- State-backed cyber attacks affecting the major infrastructure of a country, impacting millions.
- NotPetya ransomware attack in 2017, allegedly backed by the Russian government, caused a $10 bn global loss.
- Lloyd's requirement for exclusion from cyber policies and non-cyber policy wording guidelines.
- State-backed attacks difficult to prove

Challenges and considerations for cyber insurers

- Data and Long-tailed nature
- Accumulation of risk
- Silent Cyber
- State-backed exclusions
- **Post-Covid-19 Working Environment**
- Geo-Political Risk
- Ransomware

Working from home due to Covid 19:

- Employees more exposed to cyber-attacks
- Increased usage of cloud computing, broadband connectivity, and increasingly powerful collaboration tools, and employees using their own equipment.
- Not having a proper system of protection at home, such as an anti-virus or VPN.

Challenges and considerations for cyber insurers

- Data and Long-tailed nature
- Accumulation of risk
- Silent Cyber
- State-backed exclusions
- Post-Covid-19 Working Environment
- **Geo-Political Risk**
- Ransomware

Increased Geo-Political risks due to:

- Increased development of sophisticated technology - access to machine learning tools, AI, deep fakes, chatbots and social media.
- Cybercriminals participating in Cyber warfare to spread disinformation and destabilisation efforts.
- Cybercriminal groups targeting critical infrastructure, intellectual property or processes like government elections.

Grant Thornton

Institute and Faculty of Actuaries

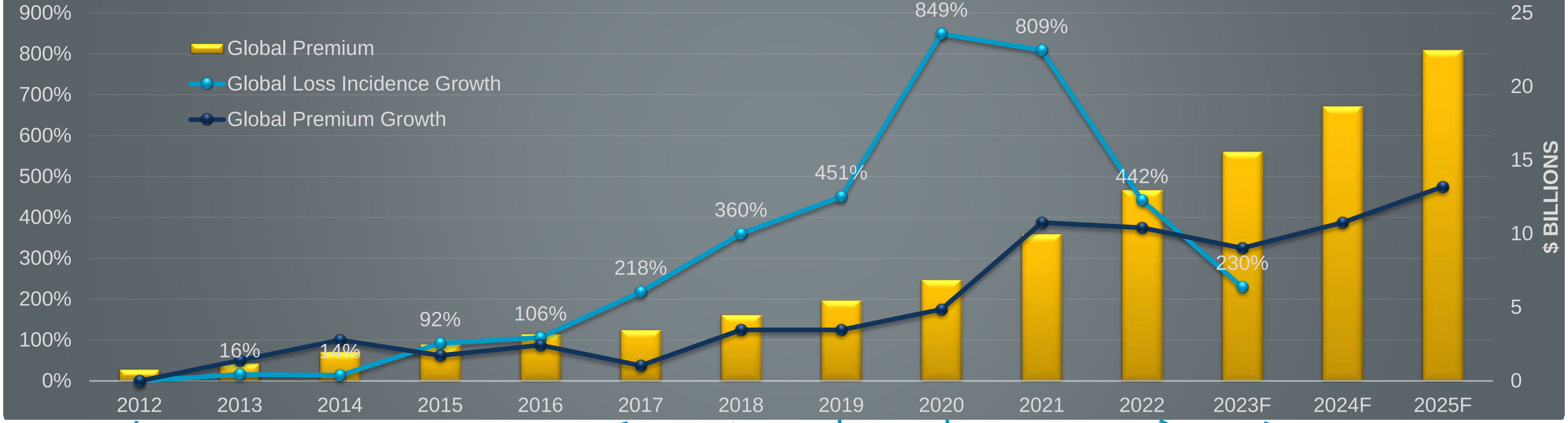
Challenges and considerations for cyber insurers

- Data and Long-tailed nature
- Accumulation of risk
- Silent Cyber
- State-backed exclusions
- Post-Covid-19 Working Environment
- Geo-Political Risk
- **Ransomware**

Ransomware is

- A malware that prevents a user from accessing their computer
- Enabling criminals to lock computers or steal, delete or encrypt the data held
- Spreading to other computers connected to the same network
- An example: in May 2017, the ‘WannaCry’ malware infiltrated the NHS network and affected thousands of computers
- The costliest cyber claims peril.

Global Cyber Insurance Premium and Loss Incidence and Premium Growth Compared to 2012



Steady Growth

NotPetya and WannaCry ransomware attacks

EU implementation of GDPR

Guidance on Silent Cyber – PRA & Lloyd's

Increased ransomware incidence and COVID-19

Rate increases and re-underwriting

Decrease in ransomware incidence

Stabilisation of rates

Premium Growth and Loss Incidence data indexed against the baseline year of 2012

Sources:
https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html
https://www.chubbcyberindex.com/#/incident-growth

GrantThornton

Institute and Faculty of Actuaries

Institute
and Faculty
of Actuaries

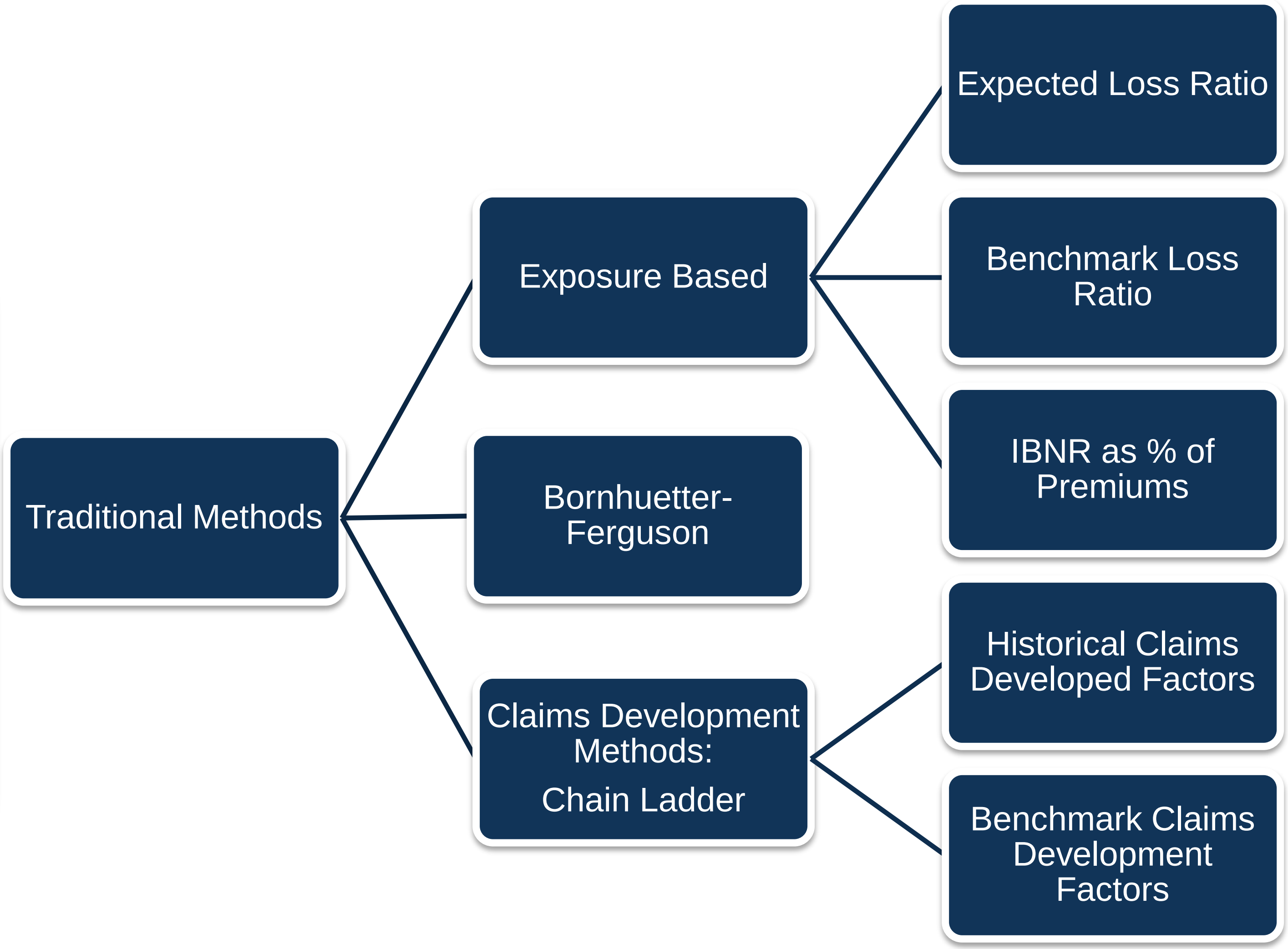
Cyber Reserving Methods

1 May 2024

Traditional Methods

The challenges and considerations for the cyber insurance industry lead - reserving challenges for actuaries.

Traditional reserving methods rely on industry benchmarks and specialist knowledge from underwriters and claim teams.



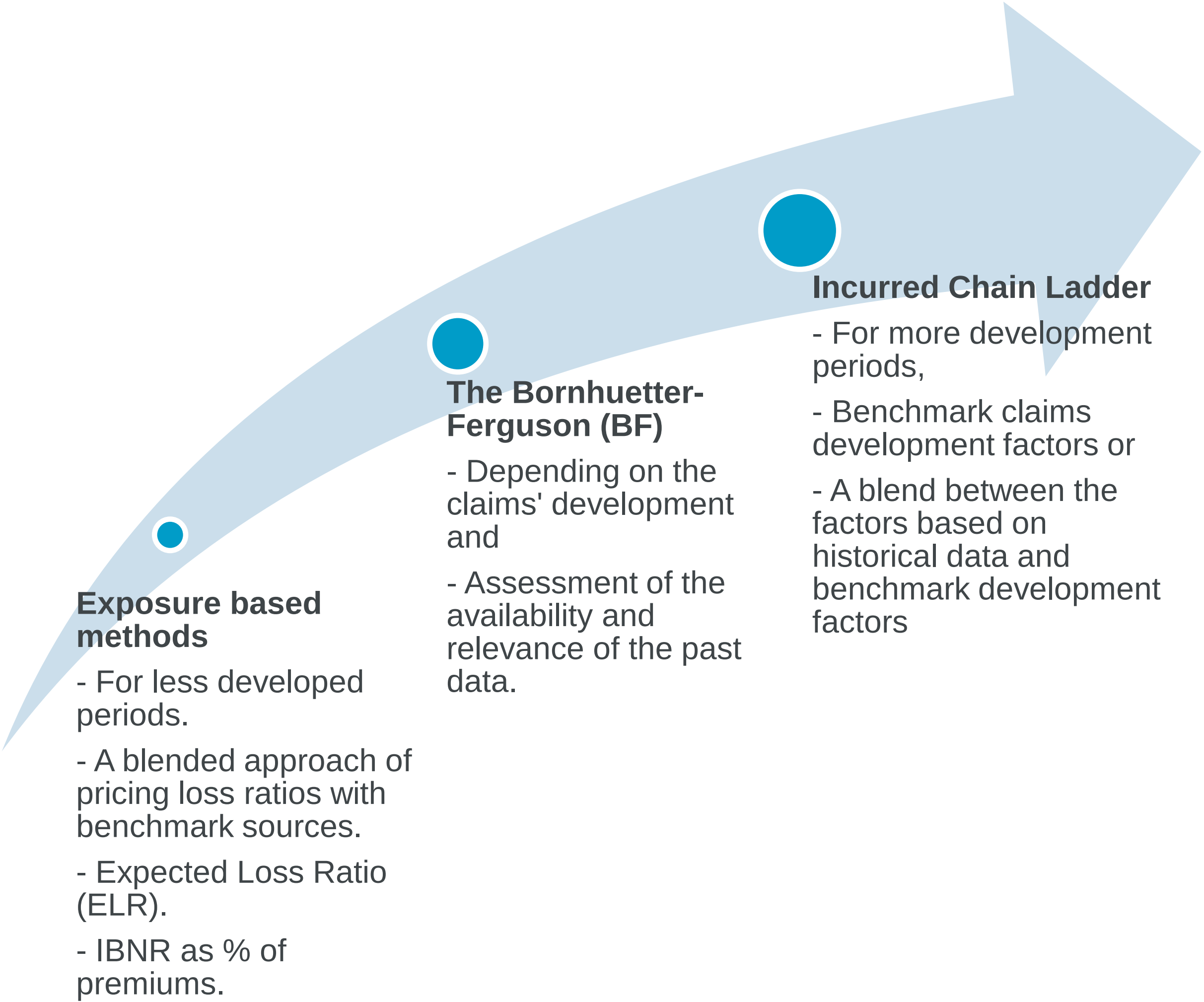
Traditional Methods

Selection of the method depends on:

- The development of the origin period.
- The discussion with the claims department on the assumptions.
- The availability and relevance of past data at different development periods.

In practice:

- Different estimates of reserves are calculated based on different assumptions and methods.



Exposure based methods

- For less developed periods.

- A blended approach of pricing loss ratios with benchmark sources.

- Expected Loss Ratio (ELR).

- IBNR as % of premiums.

The Bornhuetter-Ferguson (BF)

- Depending on the claims' development and

- Assessment of the availability and relevance of the past data.

Incurred Chain Ladder

- For more development periods,

- Benchmark claims development factors or

- A blend between the factors based on historical data and benchmark development factors

Traditional Methods: Allowance for ENID

The best estimate calculated from the traditional reserving methods:

- ✓ Expected mean of future claim liabilities.
- ✓ May not consider tail risk
- ✓ Need further allowance for Solvency II and UK GAAP requirements

- Loadings to allow for losses from Events Not In the Data (ENID), also known as binary events, such as large and catastrophe cyber events.
- Compare the best estimate with the “true” mean of claims from all possible events, including events up to the 1:200 year level.
- The difference can be applied to the best estimate as a binary event load or as an uplift factor.
- Also viewed as a contingency reserve, reducing pressure on free reserve requirements

Frequency- Severity Modelling

This modelling method:

- ✓ Models the loss frequency and severity separately.
- ✓ Determines likelihood of frequency and severity of loss events occurring in the next 12 months.
- ✓ Combines parameters to simulate total expected claims at different probability levels to produce an Exceedance Probability (EP) Curve, covered in the next section.

Modelling steps (1):

- 12-month rolling data to increase the observations.
- Maximum likelihood estimation (MLE) to estimate parameters
- Kolmogorov-Smirnov and the Cramér-von Mises statistical to validate the data sample.
- One study (1) selected:
  - ➢ Poisson Log-Normal for frequency
  - ➢ Log-Normal for severity

	Frequency parameters: Poisson log-normal (1)	
Type	Upper Bound	Lower Bound
Mean (μ)	-2.284585	-6.394251
Standard deviation (σ)	0.8690759	1.7831914

	Loss severity parameters: Log-normal (1)
Mean (μ)	12.55949
Standard deviation (σ)	3.068723

[1] https://www.cyentia.com/wp-content/uploads/IRIS-2022_Cyentia.pdf

Institute
and Faculty
of Actuaries

Validating Reserve Adequacy

1 May 2024

Validation Methods

Reserving actuaries should be aware of the company's full exposure to cyber risk, especially the tail risk, as well as the risk mitigating strategies in place. This will enable them to more accurately estimate the reserves.

- Simulation Techniques
- Exceedance Probability Curve
- Tail Risk
- Scenario Analysis

Validation Methods

Simulation Techniques

- Monte Carlo techniques can construct aggregate loss distributions by simulating possible combinations of loss frequencies and magnitudes.
- Useful for sparse data.
- If underlying distribution can be assumed, then any range of loss events can be simulated.

Exceedance Probability Curve

Tail Risk

Scenario Analysis

Validation Methods

Simulation Techniques

Exceedance Probability Curve

- Also known as the Loss Exceedance Curve (LEC) constructed from simulations.
- Quantifies the probability of experiencing a minimum loss (total expected loss) in a given period.
- Evaluate the risk exposure of a portfolio from a given scenario against the risk appetite of the firm and be used to set mitigating actions.
- Quantifies the Accumulation of risk in tail.

Tail Risk

Scenario Analysis

Validation Methods

Simulation Techniques

Exceedance Probability Curve

Tail Risk

- Tail Value-at-Risk (TVaR) or Conditional Tail Expectation (CTE) captures the risk of long-tail events.
- Focusing on the top percentiles of loss distribution and estimating the average loss value at certain percentile.
- Capturing extreme events or risks, such as the accumulation of risks.
- Compared to the ultimate.

Scenario Analysis

Validation Methods

Simulation Techniques

Exceedance Probability Curve

Tail Risk

Scenario Analysis

- Estimating the likelihood of an extreme scenario occurring in a year.
- Compared with the risk mitigating strategies to evaluate the reserve adequacy.
- The maximum and average loss for cyber claims from historical events, industry trends, and discussions with experts.
- Business interruption (caused by ransomware attacks), service provider outages, and data breaches – are examples of modelled scenarios.
- Interconnected scenarios necessitating a correlation matrix and capturing the accumulation of risks.

Institute
and Faculty
of Actuaries

Risk Mitigation Strategies

1 May 2024

Risk Mitigation Strategies

With correctly applied risk mitigating strategies, reserve risk can be reduced, shared or transferred to lower the uncertainty. The most common strategies are as follows:

- Controls
- Reinsurance
- Cyber Insurance-Linked Securities

Risk Mitigation Strategies

With correctly applied risk mitigation strategies, reserve risk can be reduced, shared or transferred to lower the uncertainty. The most common strategies are as follows:

Controls

- Multifactor Authentication
- Email and website filtering
- Secured, encrypted and tested backups
- Incident Response Plans
- Cyber security awareness training
- Replace or protect end-of-life systems.

Risk Mitigation Strategies

With correctly applied, risk mitigation strategies, reserve risk can be reduced, shared or transferred to reduce the uncertainty. The most common strategies are as follows:

Reinsurance

- Cyber insurers can cede larger or cat claims to reinsurers
- Limits the exposure to large and accumulation losses
- The reinsurance market could be increased by:
  - Offering more excess-of-loss reinsurance over proportional reinsurance
  - Creating or extending formal private sector re/insurance pools to share certain types of risk.

Risk Mitigation Strategies

With correctly applied, risk mitigation strategies, reserve risk can be reduced, shared or transferred to reduce the uncertainty. The most common strategies are as follows:

Cyber Insurance-linked Securities

- Only an option for larger insurers
- Two recent developments in 2023 have been [2]:
  - Beazley issuing Cairney cyber catastrophe bond series raising $81.5m of capital
  - Hannover RE established a collateralised reinsurance with Stone Ridge.

[2]: https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf

Institute
and Faculty
of Actuaries

Conclusion

1 May 2024

Conclusion

The global cyber insurance market

- Soft premium market between 2012 and 2020
- Moved to a hard premium market after 2020.

Reserving methods

- Cyber insurance market challenges and considerations make reserving challenging
- More reliance on exposure-based methods, benchmarks, and specialist knowledge
- ENID Loadings are important
- Frequency/severity modelling used to capture the extreme risk
- Validating reserve adequacy by comparing the reserve against the full cyber exposure
- Consider risk mitigation strategies.

Questions

Comments

Institute
and Faculty
of Actuaries

Thank You

1 May 2024