Institute and Faculty of Actuaries

GIRO Conference 2022

21–23 November, ACC Liverpool

#GiroConf22

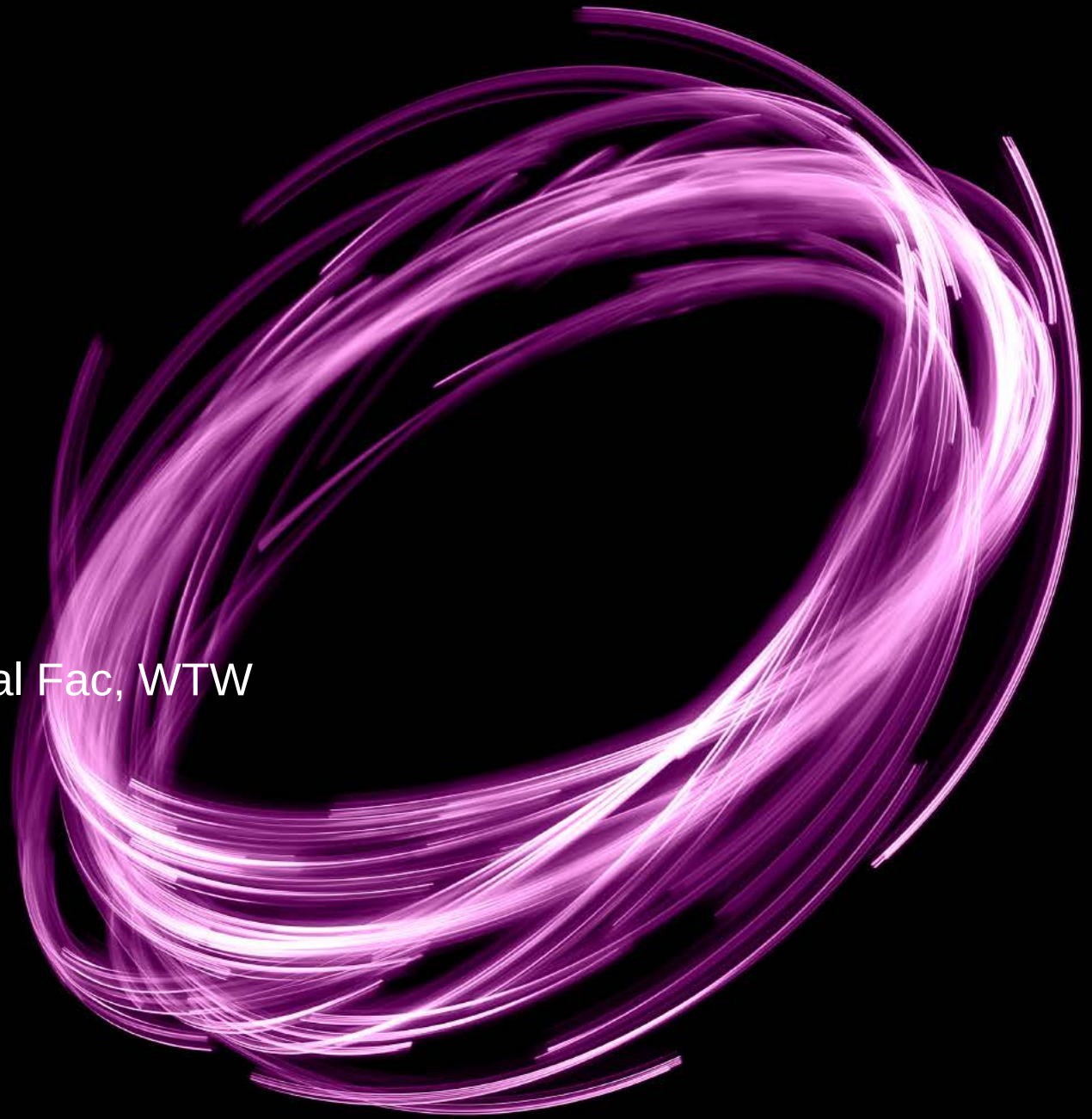
Institute and Faculty of Actuaries

Cyber Risk Capital

Cyber Risk Working Party

Simon Cartagena – Deputy CRO, SCOR UK

Jasvir Grewal - Head of Data & Analytics, Global Fac, WTW



#GiroConf22

Cyber Risk 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.
- The working party has tried to produce frequent and relevant content in order to contribute to the discussion across the industry on cyber risk
- The working party actively and encourages new members with new perspective on the risk. Please get in touch if you'd like to join and actively contribute to the group.

Simon Cartagena
Deputy CRO – SCOR Specialty

Jasvir Grewal
Head of Data & Analytics – Global Fac, WTW

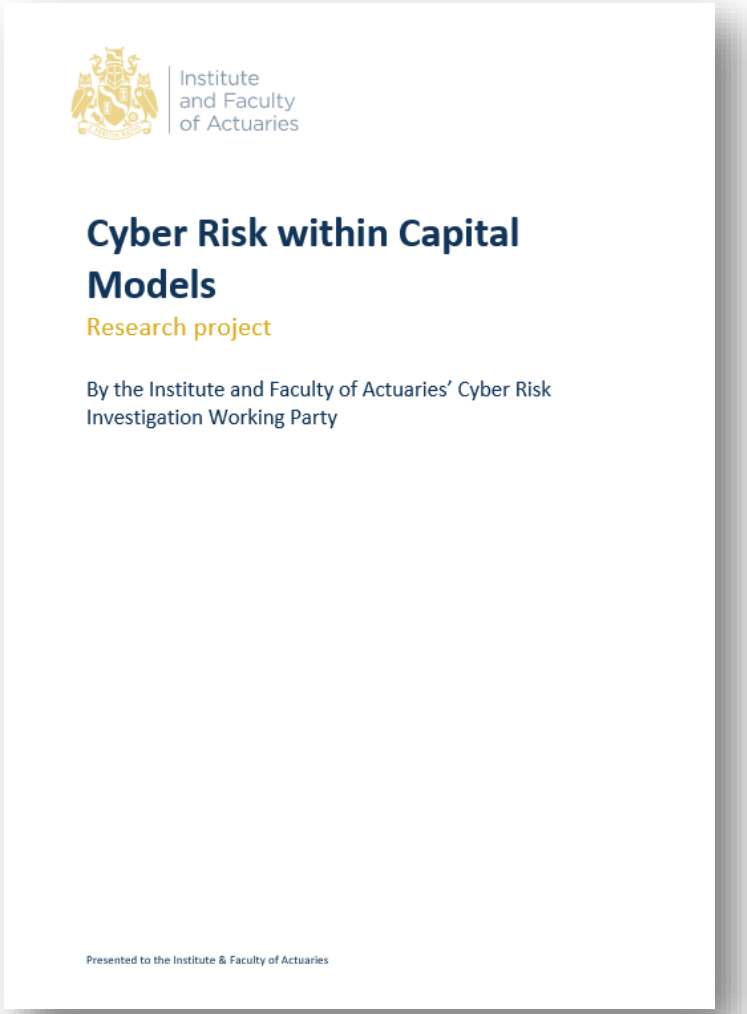
Volunteer vacancies

https://www.actuaries.org.uk/practice-areas/risk-management/risk-management-research-working-parties/cyber-risk-investigation

Institute and Faculty of Actuaries

Sessional Paper

- The (re)insurance industry is maturing in its ability to measure and quantity cyber risk. The risk and threat landscapes around cyber continue to evolve and in some cases rapidly. Both the threat actor environment can change as well as the exposure base depending on a variety of external factors such as political, economic and technological factors.
- The rapidly changing environment poses interesting challenges for the Risk & Capital actuaries across the market. The ability to accurately reflect all sources of material losses from cyber events is challenging for capital models and the validation exercise. Furthermore, having a robust ERM framework supporting the business to evaluate cyber risk is an important consideration to give the board comfort that cyber risk is being effectively understood and managed by the business.
- This paper discusses cyber risk in relation to important risk and capital model topics that actuaries should be considering. The capital models are faced with a challenge to model this rapidly changing risk in a proportionate way that can be communicated to stakeholders. As model vendors continue to mature and update models the validation of these models and the ultimate cyber capital allocation is even more complex as one's view of risk could change rapidly from year to year depending on the threat or exposure landscape as demonstrated by the ransomware trends in recent years).
- This paper has been prepared primarily with General Insurers in mind however the broader aspects of capital modelling, dependencies and ERM framework are relevant to all disciplines of the profession.



Institute and Faculty of Actuaries

Scope

- Cyber Risk definition - the scope includes all three of the main categories of cyber risk that an insurance company is exposed to:
  - **affirmative** (underwriting) cyber risk,
  - **non-affirmative** (underwriting) cyber risk, and
  - **operational** cyber risk.

- Capital definition: we do not consider the differences between different solvency capital setting regulations.
  - Considerations discussed are as those that would be used within a **Solvency II "internal capital model"** (as opposed to standard formula or any other regulatory guidance).
  - However, many considerations can generally be applied more broadly to situations where cyber risk needs to be modelled.

Institute and Faculty of Actuaries

Agenda

1. Cyber Risk Landscape
2. Capital Modelling
3. Validation
4. ERM

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Cyber Risk Landscape

Simon Cartagena

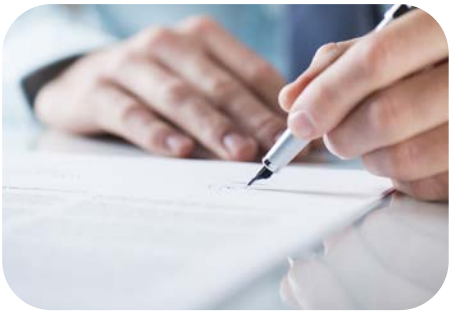
#GiroConf22

Why is Cyber Capital Uncertain?

Threat Actors

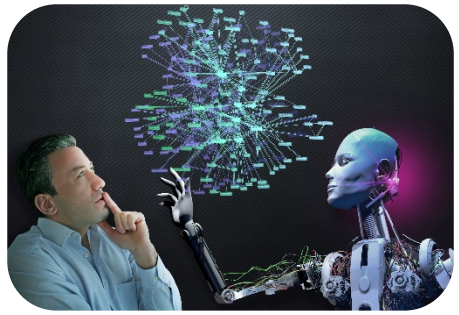
Treat Vectors

War



Wordings

Terrorism

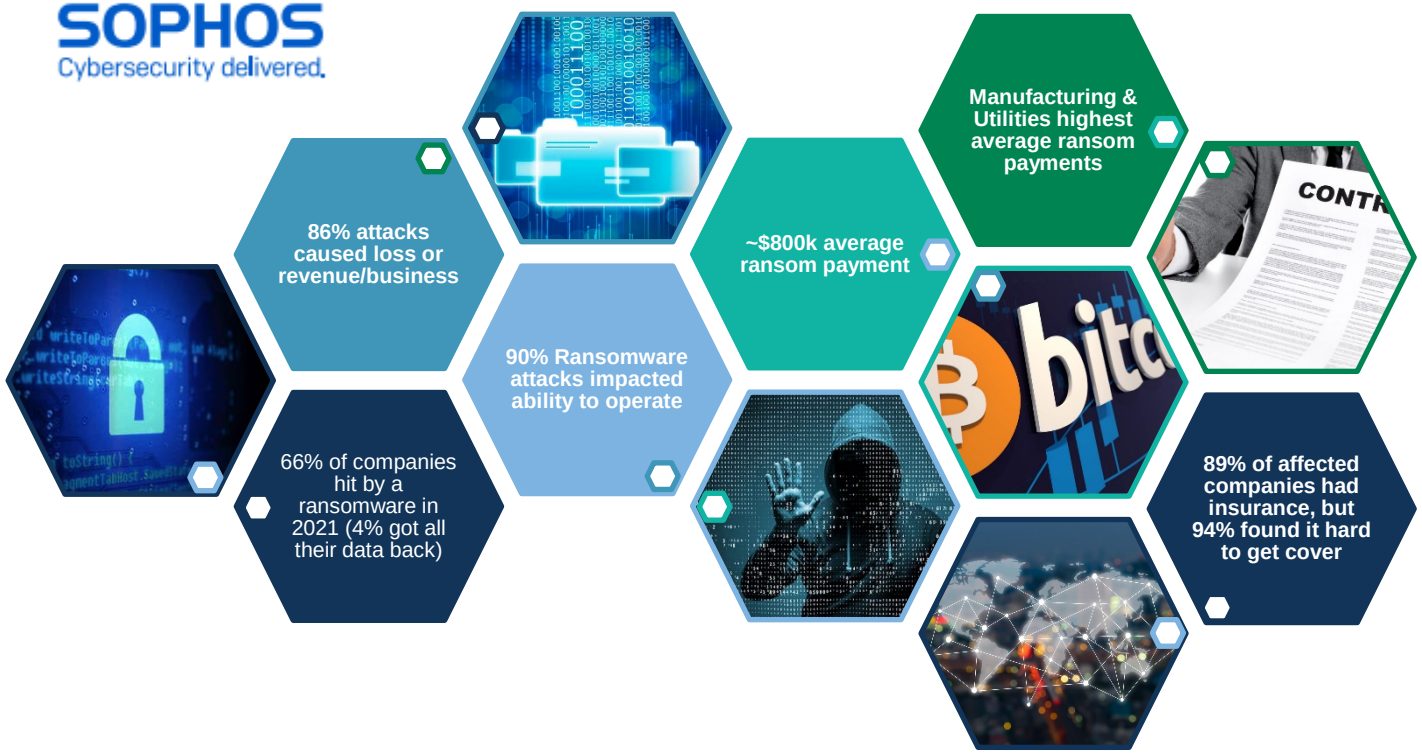


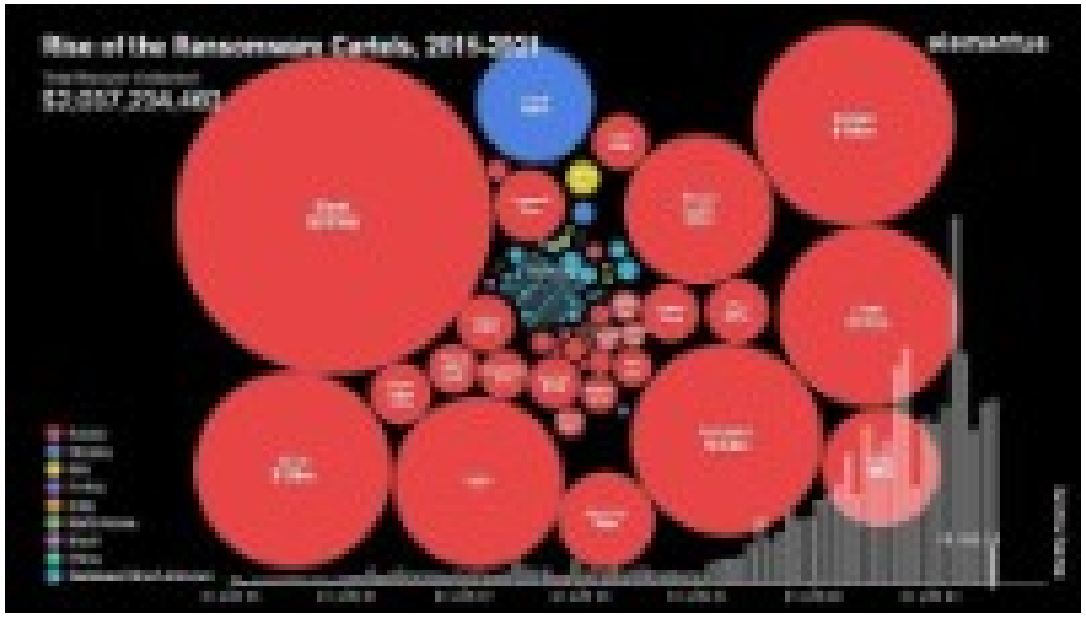
Technology

Capacity

Institute and Faculty of Actuaries

Threat Landscape Evolution



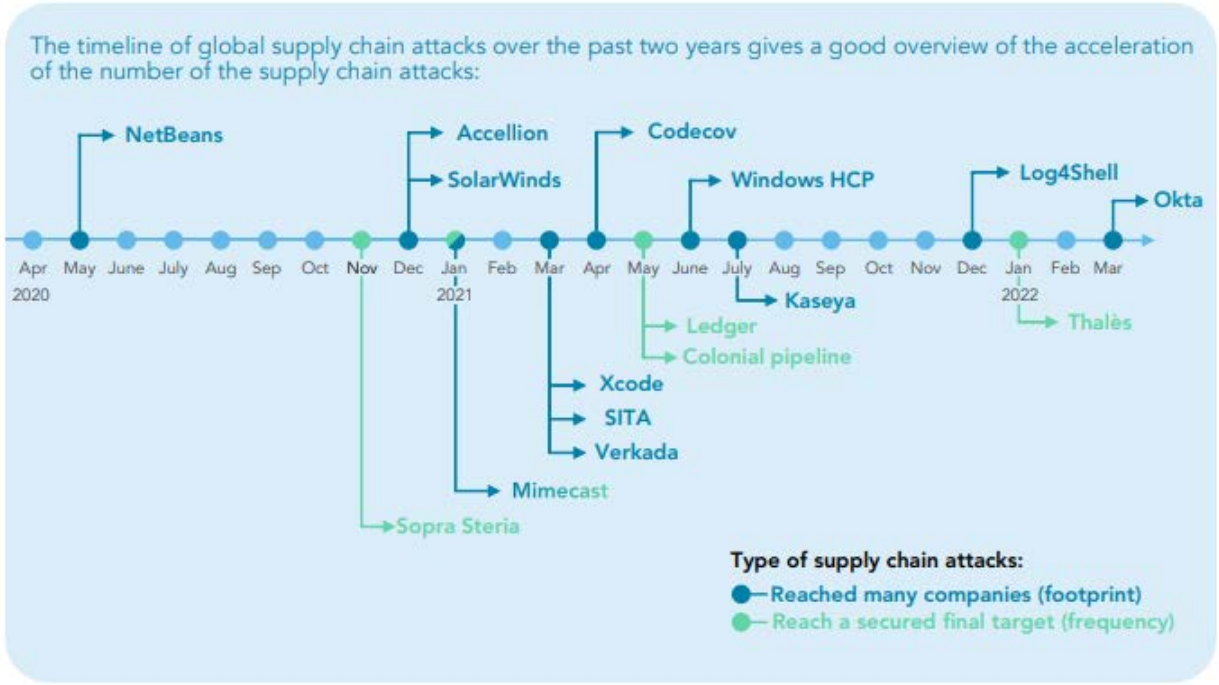


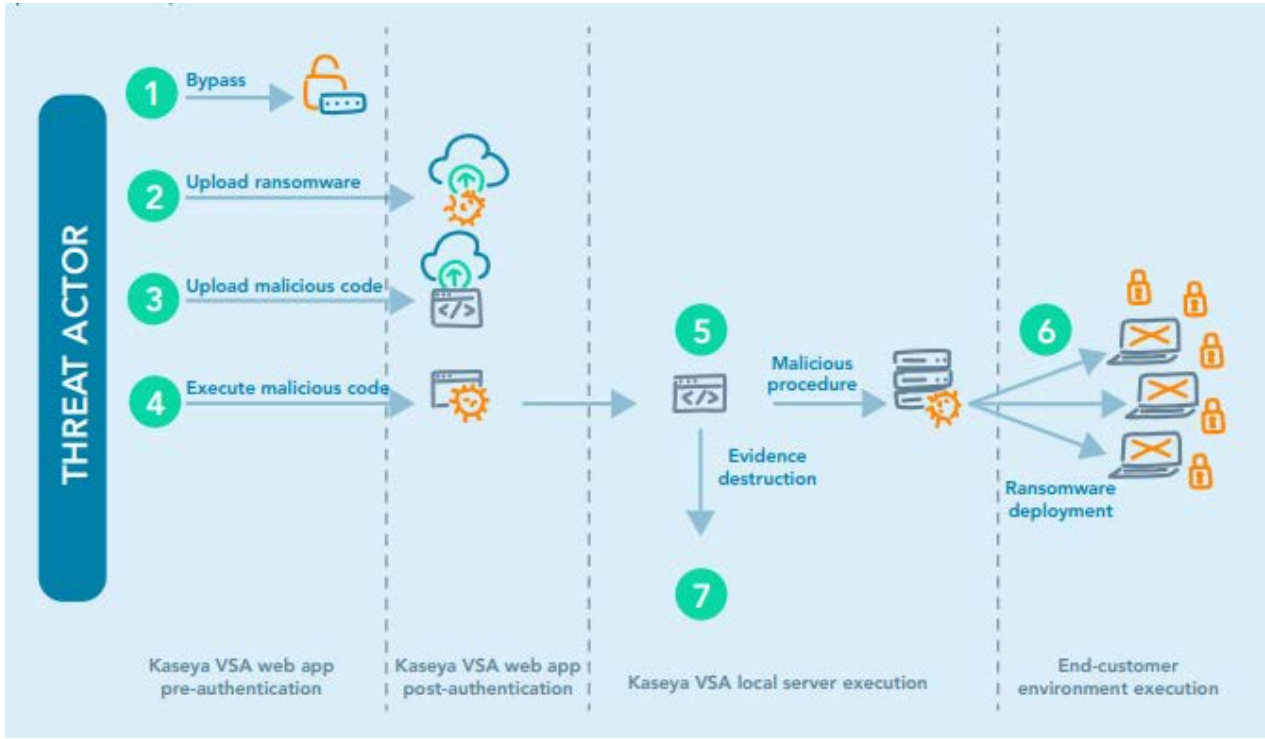
Sophos Cyber Security Report: The State of Ransomware 2022 Findings
From an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries.

https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

Institute and Faculty of Actuaries

Supply Chain Attacks





SCOR Expert Views - Cybersecurity of the supply chain: *https://www.scor.com/en/news/cybersecurity-supply-chain*

Institute and Faculty of Actuaries

2022 Developments

War in Ukraine

- Accelerated the Cyber Arms Race, the cyber war began long before the “land war”.
- **46** zero day weapons developed
- Focus of attacks has been mainly to **disrupt, confuse and disorientate** communications
- **Blackwired** anticipates a tidal wave of attacks on global targets when the conflict in Ukraine allows the resources of the bad actors to be focused elsewhere.
- Will this lead to increased frequency and/or severity of insurance claims in the coming months and years?

Weapons Developments

- Three significant weapons developed in 2022 that change the risk landscape forever:
  - **Click-less phishing:** evolution of attack whereby the mere delivery of the email is sufficient to deliver malware.
  - **Search poisoning:** attack method in which cybercriminals create malicious websites and use search engine optimization tactics to make them show up prominently in search results
  - **Supply Chain poisoning**: Most software contains proprietary and open-source components. If any of those components have vulnerable code, hackers can exploit the vulnerabilities to access networks

What does it all mean?

- How do we quantify the uncertainty (especially in the tail)?
- Do our current approaches adequately capture and/or allow us to respond to the evolving risk?
- How effective are the latest wordings/clauses?
- Does it even matter?

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Capital Modelling

Jasvir Grewal

#GiroConf22

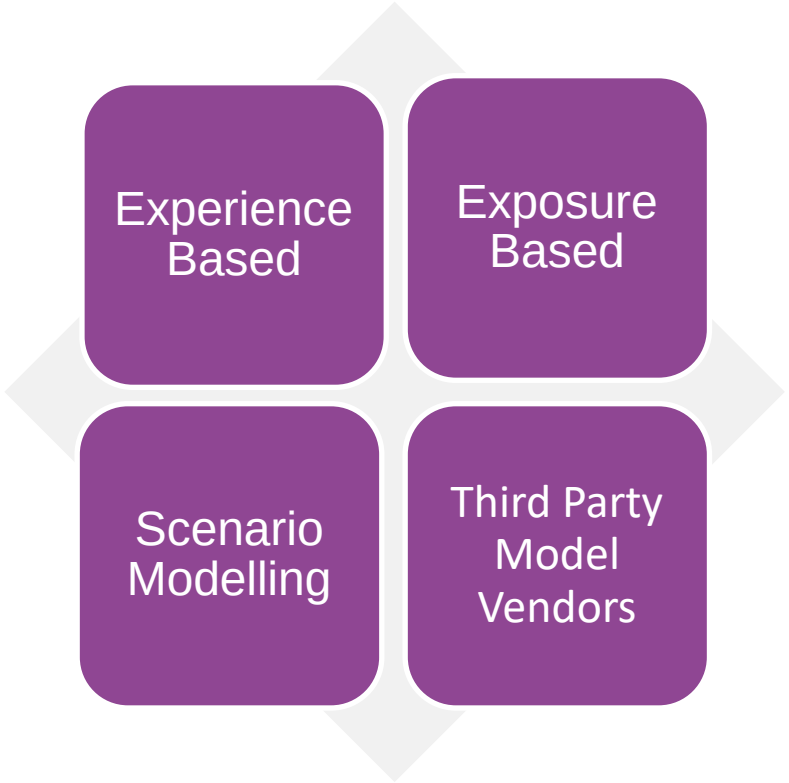
Some questions for the audience to get us started…

Institute and Faculty of Actuaries

Underwriting Risk

Key Considerations:

- **Data:** The industry is still working towards standardising cyber data and other issues such as changing categorisations (e.g., movement away from non-affirmative towards affirmative cyber), and unclear loss causation codes.
- **Stability** of parameterisation over time.
- Adequate allowance for **systemic risk.**
- **Changing nature of the class:** Changing drivers, threat actors, loss trends, increasing interconnectivities between companies, varying targeted industries.



Are we adequately allowing for the true extent of the changing cyber landscape within capital models?

Institute and Faculty of Actuaries

Other Risks: Key Considerations

Reserve Risk

Changing:

- development patterns, frequency and severity of losses, cyber categorisations.
- range of threat actors continually developing (e.g., from sole hackers to state backed attacks).
- duration of the tail (in situations where there might be delegated authority/claim disputes)

Operational Risk

Meaningful cyber operational risks that are relevant and appropriate for the insurance company rather than generic scenarios.

See earlier paper provided by the working party.

Market Risk

Adequate allowance for systemic risk where losses across occur across market risk and cyber risk distributions simultaneously?

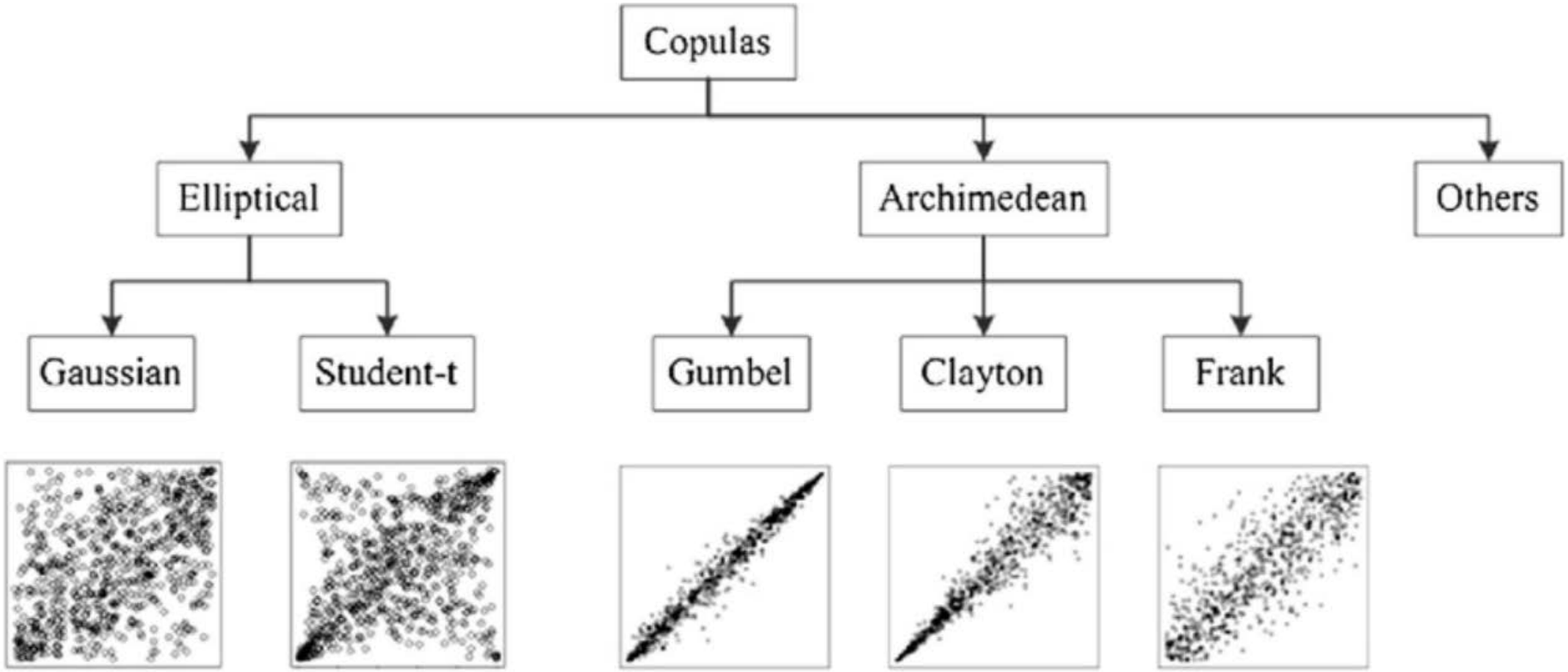
RI Credit Risk

Recent high profile legal disputes over cyber policy coverages illustrate that disputes can occur.

Rating agencies already consider cyber risk as part of their credit rating work, given that a cyber operational risk event could have significant adverse implications for a company.

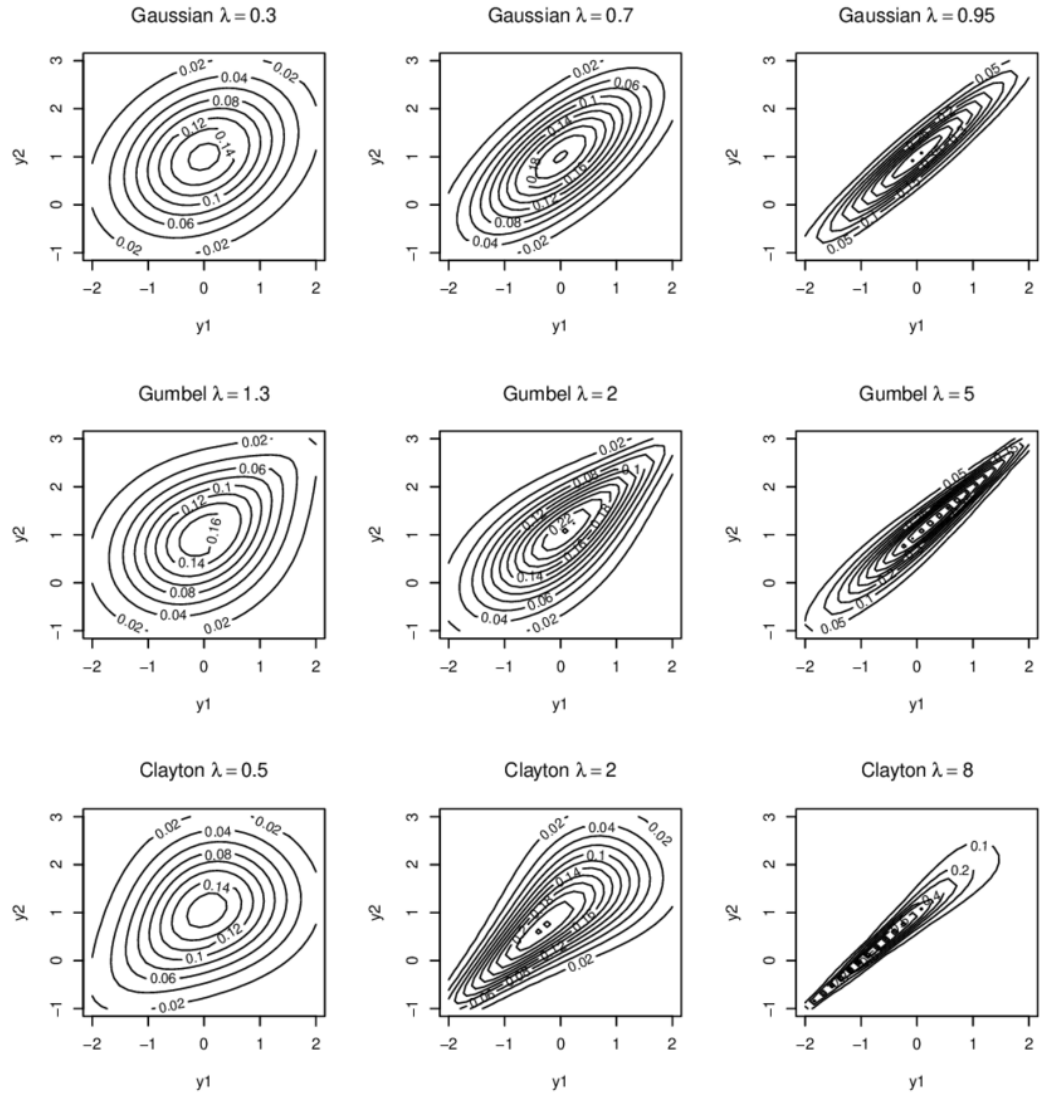
Institute and Faculty of Actuaries

Dependencies: let's parameterise together [1]



Institute and Faculty of Actuaries

Dependencies: let's parameterise together [2]



- Lack of data to accurately parameterise the tail.
- Some (re)insurers use dependency libraries to assist.
  - How effective is this approach in practice?
  - Affected by availability heuristic?
- There are alternative approaches!

Institute and Faculty of Actuaries

Capital Allocation

Impacts of Capital Allocation	Practical Considerations
Conversations about tail exposures – not just the mean!	Mitigators: Cyber RI Coverage and Other Mitigating Actions
Trade-off for RI premium spend vs Risk Retention.	Allocate to all types of Cyber Risk: Affirmative, Non-Affirmative, and Operational.
Staff Compensation	Strategic Risks

- Wide range of capital allocation methodologies – often this is a real discussion point within (re)insurance companies.
- Uncertainty in cyber capital modelling compounds the issues.
- Careful consideration of cyber capital loads is important, especially in the current market dynamic, where there is uncertainty in pricing adequacy, rapid increases in rates, and a shortage of underwriting talent.

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

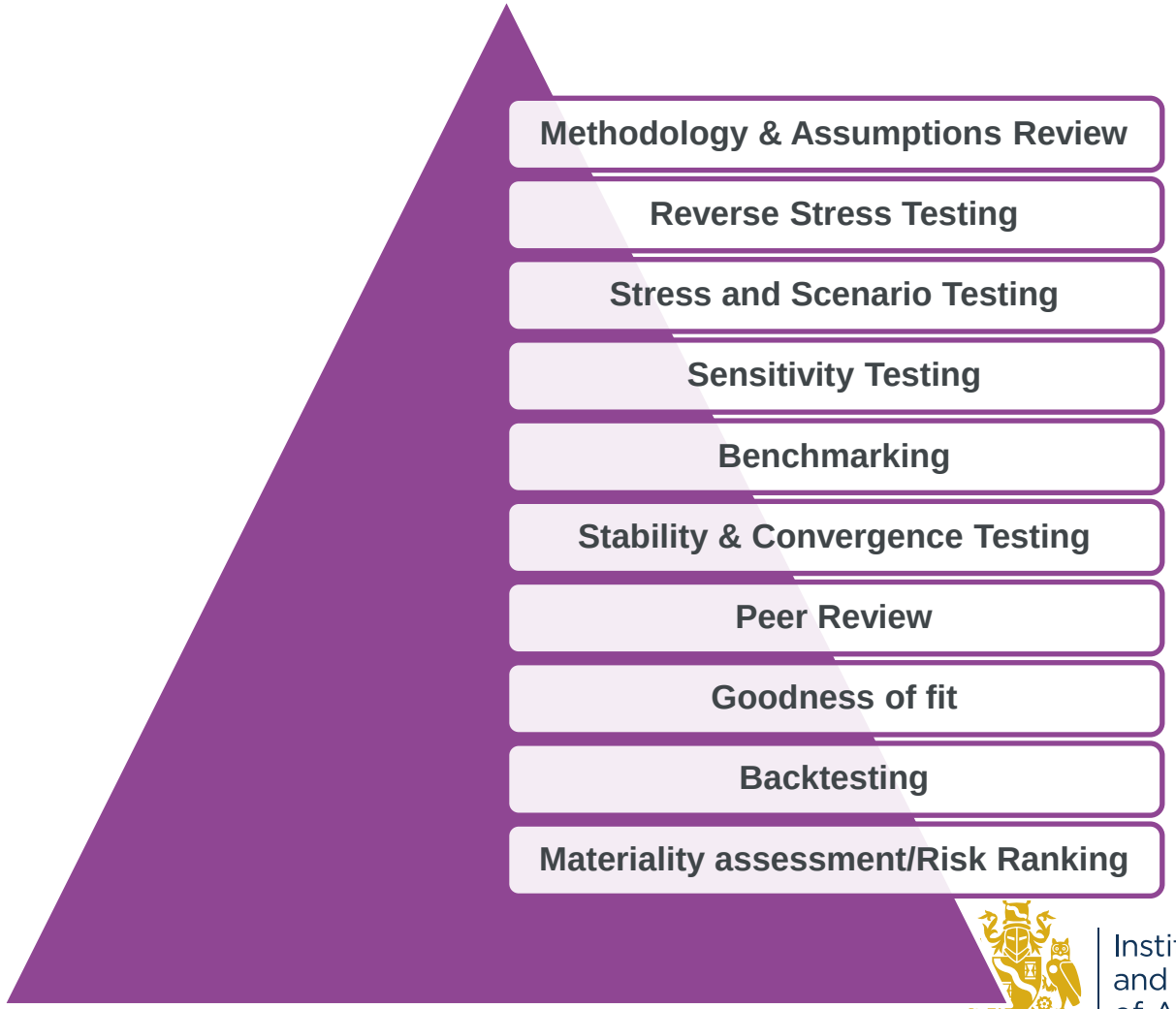
Validation & ERM

Simon Cartagena

#GiroConf22

Validation Focus

- Cyber risk is a complex issue that constantly evolves, and it has been a challenging task to communicate all the risks in cyber security into something measurable and quantifiable. Hence, it's important that the challenge contains some expertise in the cyber security space so that any material issues are not overlooked.
- Given the maturity of the risk modelling, some of the more relied upon validation tools will be less useful than for other risks.



Institute and Faculty of Actuaries

Attritional & Large Loss Deep Dives

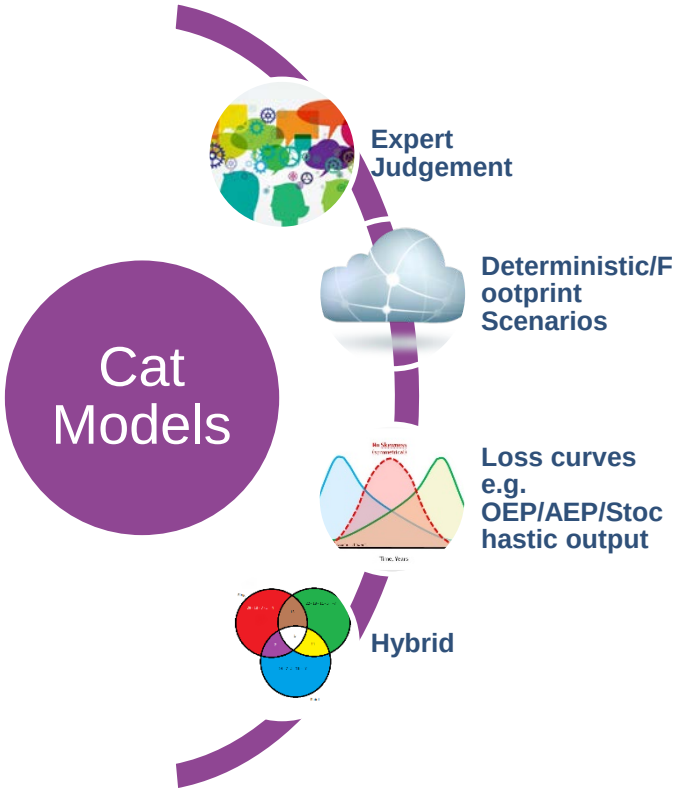
- How has the claims frequency and or severity changed over time?
  - Suitable volatility assumptions? Distribution selection process? Review and governance?
- Have the cyber coverages offered changed?
  - How does this affect your parametrisation? Is it performed on a regular enough basis to remain relevant?
- Has the companies risk appetite/strategy changed?
  - If so how has the parametrisation process addressed this?
- Does the parametrisation process include an implicit/explicit cat load?
- How does the current threat actor and/or threat vector landscape inform the view of risk going forward? For example, has the business considered the zero-day black market or commercial ransomware groups activity in estimating its loss ratios?

Institute and Faculty of Actuaries

Catastrophe Risk Validation

* "We don't expect syndicates to try to convince us that the chosen cyber model is perfect. We would prefer that the syndicates are open and honest about what all the limitations are in the cyber model and what they intend to do to cope with the uncertainty."

Emma Watkins
Head of Exposure Management & Aggregation
Lloyd's

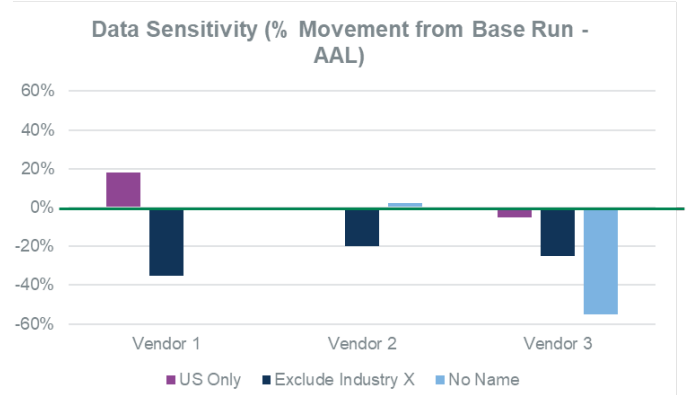


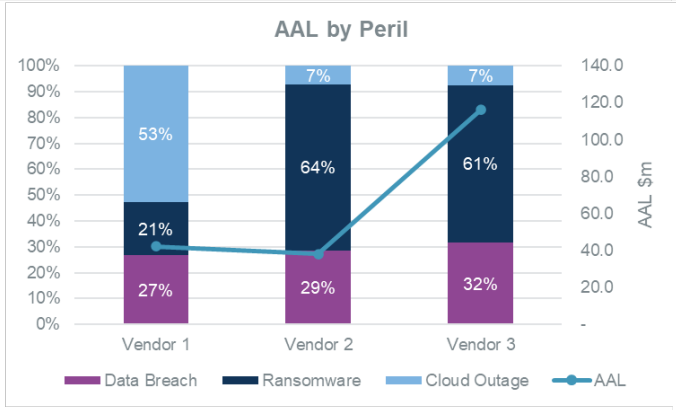
- There were no true cyber catastrophic events to leverage from
- The estimation of cat losses is currently a theoretical exercise
- What is your companies modelling philosophy for cyber?
- What are the key exposures and how might they aggregate?
- Can you communicate what type of scenarios are driving the tail? Do you agree with them?

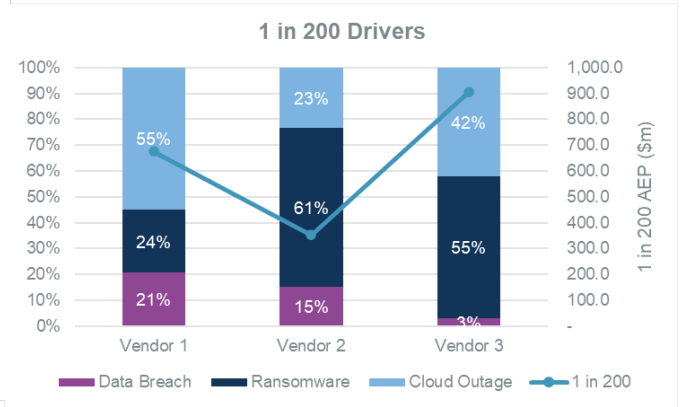
Institute and Faculty of Actuaries

External Cyber Catastrophe Models

- **Demonstrate understanding of the model**
  - Strengths and weaknesses
  - Model parameters
  - Model output adjustments
  - Vendors Validation
- **Demonstrate model suitability to the portfolio**
  - Scenarios suite a good match for the exposure
  - Multi-model approach required
- **Independent Validation**
  - Backtesting
  - Comparison to industry estimates
  - Sensitivity & Stress Testing
  - Stability testing







Institute and Faculty of Actuaries

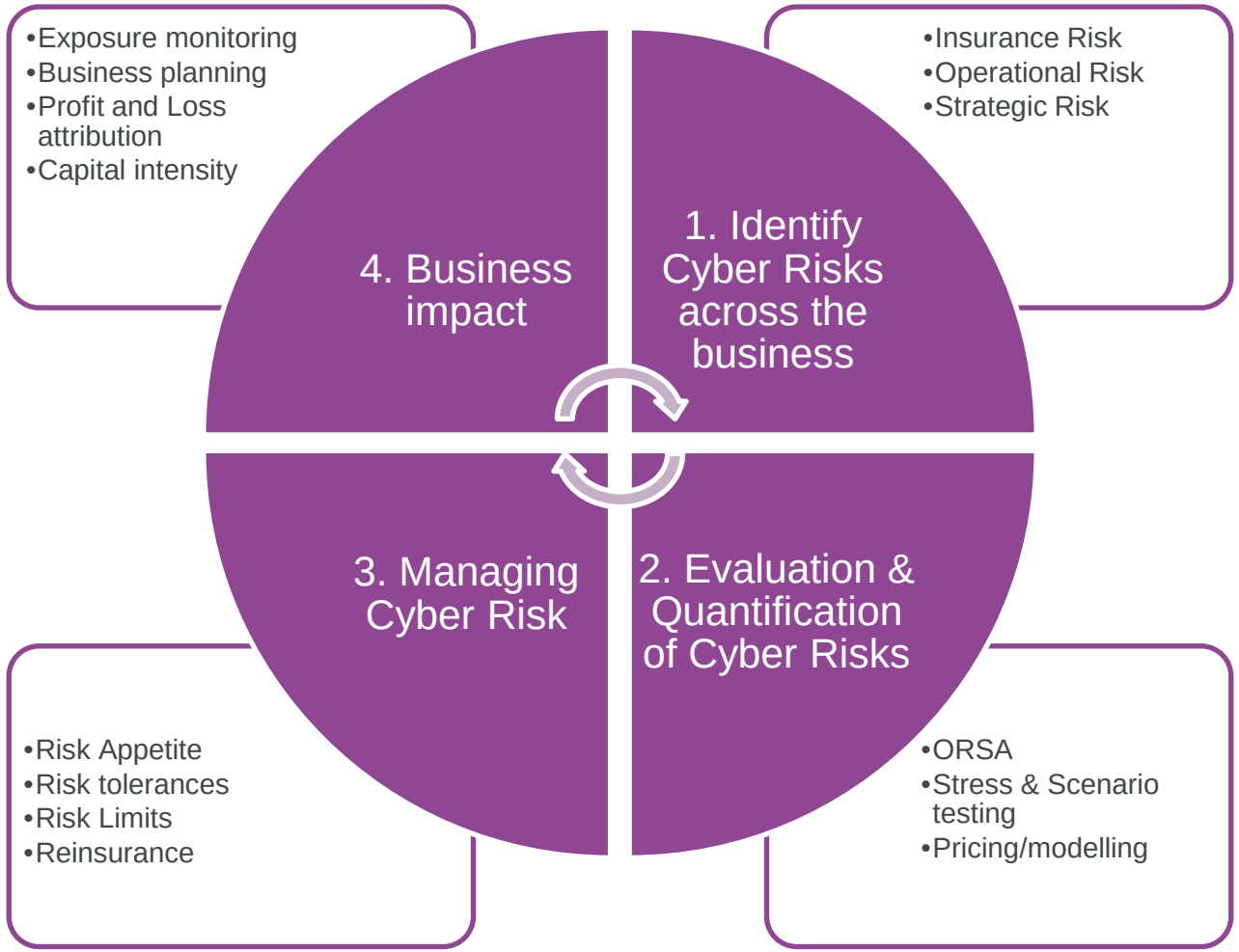
Theoretical results on an artificial portfolio performed for the ASTIN 2022 conference.
Data Sensitivity analysis performed by Gallagher Re

Other Risks

- Has sufficient consideration/testing been performed on other risk areas such as:
  - **Operational Risk:** Dependency testing in the tail should be performed to asses if there is sufficient correlation between cyber operational risk events and cyber cat events. Type 3 or RSTs can be useful in assessing this.
  - **Market Risk:** Do you consider that a Cyber event will cause market disruption? If so is it captured in your modelled output somehow?
  - **Credit Risk**: Do cyber events make credit risk any more likely?
  - **Cyber as a Peril:** Cyber can impact other lines of business, has the capital model allowed for this somewhere, either through explicit pricing/premium risk paramaterisation or via scenarios?

Institute and Faculty of Actuaries

Cyber Dynamic Feedback Loop



Institute and Faculty of Actuaries

Quick Note on Wordings

"Is there clarity around coverage in the London market? Are we comfortable with quantifying impact from developments to the tail risk/capital?"

Clause coverage		LMA5564	LMA5565	LMA5566	LMA5567	Munich Re/Marsh/Aon	Beazley
War and Cyber Operations in the course of war		X	X	X	X	X	X
Cyber Operations that have a "major detrimental impact" on the functioning of a state security defence or essential services		X	X	X	X	X	X
Cyber Operations that are retaliatory between specified states (G7)	leading to 2 or more specified states becoming impacted states	X	X	X	X		
	without leading to 2 or more specified states becoming impacted states	X	X	X			
Effects on by standing cyber assets		X	X	X			
Other losses due to cyber operations not set out in all of the above	without specified coverage limits	X	X				
	with specified coverage limits	X					

Institute and Faculty of Actuaries

Thank you

#GiroConf22

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.

Institute and Faculty of Actuaries