British Actuarial Journal (2024), Vol. **29**, e16, pp. 1–31
doi:10.1017/S1357321724000114

SESSIONAL PAPER

Cyber risk within capital models

[By the Institute and Faculty of Actuaries' Cyber Risk Investigation Working Party, 14 November 2023, Staple Inn Hall, London]

Jasvir Grewal and Simon Cartagena

Institute and Faculty of Actuaries, London, WC1V 7PP, UK
Corresponding author: Jasvir Grewal; Email: jasvirgrewal@yahoo.com

Abstract

The (re)insurance industry is maturing in its ability to measure and quantify Cyber Risk. The risk and threat landscapes around cyber continue to evolve, in some cases rapidly. 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 and 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 enterprise risk management (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. It is challenging for the capital models 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. 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.

Keywords: Cyber risk; capital models; insurance; capital modelling

Disclaimer: The views expressed in this publication are those of invited contributors and not necessarily those of the Institute and Faculty of Actuaries. The Institute and Faculty of Actuaries do not endorse any of the views stated, nor any claims or representations made in this publication and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this publication. The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this publication be reproduced without the written permission of the Institute and Faculty of Actuaries.

1. Executive Summary

Capital requirements in internal models in the (re)insurance industry for Cyber Risk are coming under greater focus due to the growth of the product line, interest from regulators, credit rating

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

agencies and boards themselves, in order to set risk tolerances around both the underwriting and operations risk that cyber poses. Cyber Risk impacts a range of risk categories in the internal model and each risk category may be linked to another.

There are a range of methods that can be used to model Cyber Risk within each risk category. Underwriting risk must focus on the emerging trends within the Cyber Risk landscape, both in terms of threat actors, vectors and policy wordings. Reserving risk equally has many challenges to parametrise different year of accounts and understanding the technographic and underwriting differences between these years is important. Operational risk is also a key area of focus to consider Cyber Risk generally by using scenarios and the correlation between each risk type is key to fully representing Cyber Risk across the internal model.

Third-party vendor models are available for companies to quickly understand potential extreme scenarios, but the expert judgements can be opaque, and this can cause difficulty in understanding a set of results at a particular time and also results over time. This also can create issues communicating the expected losses and movements between model version and management and the board.

Validation of Cyber Risk modelling is made more difficult by the changing nature of the risk and this is important to take into account when choosing the types of tests to prioritise.

Furthermore, it is important to embed Cyber Risk into the ERM processes including a clear risk appetite statement, translated into tolerances and limits which can be monitored.

2. Introduction

2.1. Aims and Terms of Reference

The Cyber Risk Investigation Working Party is a subgroup under the Institute's ERM committee. The group was established as a forum for actuaries to share insight and research and to respond to Cyber Risk developments within the industry.

The group aims to support actuaries working on realistic capital calculations and/or within enterprise risk management (ERM) for life and general insurers. In particular, the purpose of this paper is to provide a guide relating to how capital models can allow for and validate Cyber Risk both more holistically and more appropriately than may currently be the case.

- The scope of this paper 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.
- This paper does 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 a 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.
- The authors have written the paper primarily from a General Insurance Lloyds' and London Market perspective. This is primarily given the materiality of the London and Lloyds' Cyber market and the authors' own experience in this area. As part of the process in preparing this document, roundtables with industry experts were held to gather feedback on how capital teams in the market were approaching the modelling of Cyber Risk.
- Despite the London market experience that forms the basis of this paper, we consider it likely that the topics covered in this paper will also be relevant to insurers across all markets and regions where capital models are built with similarities to the Solvency II Directive.

2.2. Background

Past events have shown that cyber events have the potential to be a "capital event" whether due to operational Cyber Risk, non-affirmative Cyber Risk or affirmative Cyber Risk – for example, see Bloomberg (2019), Reuters (2018) or Bloomberg (2021). These recent events, and the uncertainty in rate adequacy as well as the lack of understanding around the potential loss distribution that such events have highlighted, have caused a variety of knock-on effects; these include double-digit rate increases for cyber insurance policies, limited growth due to concern by some regulators and stricter risk appetite management by some insurers.

Indeed, in recent years, companies are starting to increasingly appreciate the significant potential of losses from cyber events (whether operational, affirmative or non-affirmative) and their potential to be tail events and cause balance sheet shocks. In the survey results released in 2019 (Bank of England PRA, 2019), one of the feedback points provided was that some firms had assessed their non-affirmative cyber exposure "as being comparable with major natural catastrophes in the USA", which are some of the most material exposures for those operating in the Lloyd's of London General Insurance market.

However, this is where a capital model can be vital in an insurance organisation; beyond the regulatory need for setting capital requirements, a capital model's full power is unleashed when it is fully embedded within a business to help understand the range of potential outcomes, even if such results are accompanied by an appreciation of the limitations of key material assumptions due to limited data. Thus, not only is it important to fully allow for Cyber Risk exposures adequately in capital models for the sake of regulatory capital-setting purposes, business planning and associated processes, due to the ever-evolving nature of the Cyber Risk landscape, fully appreciating how Cyber Risks can aggregate with other (cyber or otherwise) risks and impact balance sheet volatility is a necessity.

Furthermore, the changing nature of cyber events is providing unease to the management and boards of companies around the adequacy of capital allocated towards potential large and systemic events. If a company is not fully appreciating its cyber exposures, then it is also potentially not adequately protecting its balance sheet from volatility so that fluctuations are within set risk appetite. Moreover, any risk mitigation factors may be inadequate in such cases and raise questions regarding the confidence that any purchased outwards cover (or other mitigating cover) provides true value for money and whether any underappreciated cyber exposures (whether underwriting, operational or both) have the potential to completely offset any profitable results or make worse the results seen elsewhere in the company.

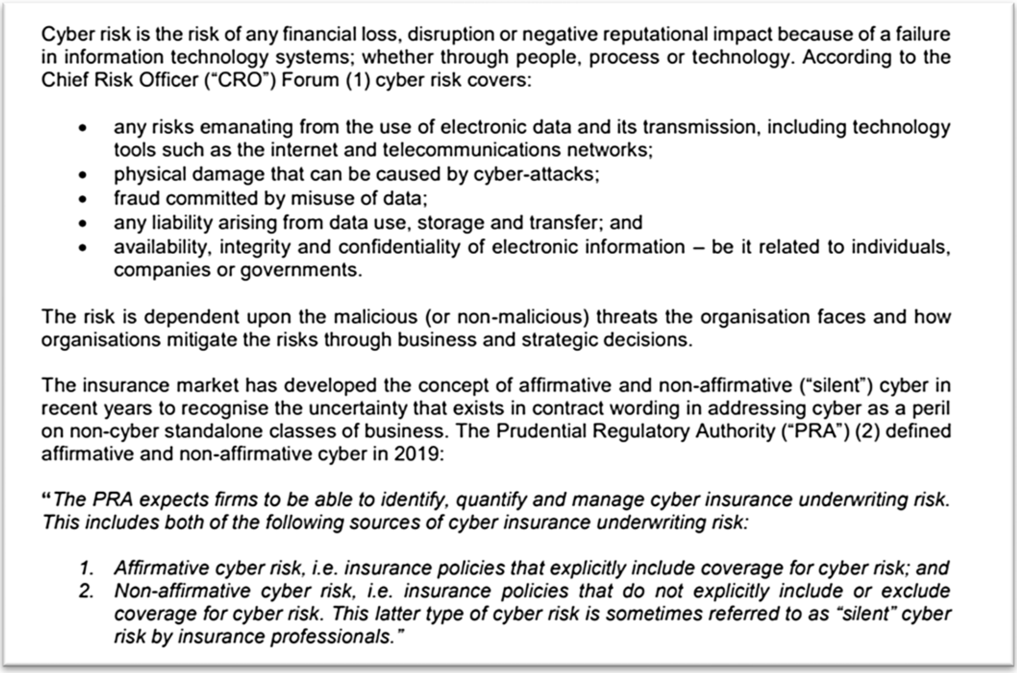
There have been strides made to improve cyber exposure understanding, risk management and pricing capabilities over the last few years; naturally, this also translates into better inputs into an insurance company's capital models. However, given the nature of the cyber environment – fast changing and dynamic – and the main use of the capital model (i.e. future projections of balance sheets), assumptions applied to bring exposures on to future bases also add a further level of complexity and uncertainty.

Nonetheless, providing a range of outcomes based on a set of assumptions – or an initial view of the world to be refined as further information becomes available – is an invaluable risk management and business planning tool, and this is precisely the power of using a capital model. Assumptions can then also be modified to further appreciate the sensitivity of results further and what business implications this could have and whether such outcomes are within risk appetite.

2.3. Definition of Cyber Risk

The scope of this paper 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 (see Figure 1 below).

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press



Cyber risk is the risk of any financial loss, disruption or negative reputational impact because of a failure in information technology systems; whether through people, process or technology. According to the Chief Risk Officer ("CRO") Forum (1) cyber risk covers:

- any risks emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks;
- physical damage that can be caused by cyber-attacks;
- fraud committed by misuse of data;
- any liability arising from data use, storage and transfer; and
- availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments.

The risk is dependent upon the malicious (or non-malicious) threats the organisation faces and how organisations mitigate the risks through business and strategic decisions.

The insurance market has developed the concept of affirmative and non-affirmative ("silent") cyber in recent years to recognise the uncertainty that exists in contract wording in addressing cyber as a peril on non-cyber standalone classes of business. The Prudential Regulatory Authority ("PRA") (2) defined affirmative and non-affirmative cyber in 2019:

"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:

1. *Affirmative cyber risk, i.e. insurance policies that explicitly include coverage for cyber risk; and*
2. *Non-affirmative cyber risk, i.e. 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."*

Figure 1. Definitions for affirmative and non-affirmative cyber risk.

The reader is referred to the working party's previous papers, Institute and Faculty of Actuaries' Cyber Risk Working Party (2021) and Institute and Faculty of Actuaries' Cyber Risk Working Party (2018), where more comprehensive definitions are given for each of the three categories above. The extract in Figure 1 is taken from the Silent Cyber Assessment Framework (Institute and Faculty of Actuaries' Cyber Risk Working Party, 2021), which describes Cyber Risk generally as well as providing definitions for affirmative and non-affirmative Cyber Risk.

Note that cyber underwriting risks (whether affirmative or non-affirmative) refer to the risks that an insurance company is exposed to, as a result of selling insurance contracts with Cyber Risk exposure. However, an insurance company can be exposed to cyber operational risks, regardless of whether or not it writes cyber (re)insurance contracts.

2.4. Scope of this Paper

The scope of this paper covers both the underwriting Cyber Risks (whether affirmative or non-affirmative) and the operational Cyber Risks that an insurance company may be exposed to.

Note that this paper does not consider the differences between different solvency capital-setting regulations. The experiences of the authors of this paper are based on the London General Insurance Market, and the considerations discussed are those that would be used within a Solvency II "internal capital model" (as opposed to a 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.

The reader is referred to the many available sources for additional background information on internal capital models, for example, ASTIN (2013), and their uses or comparisons with other capital-setting practices such as the use of the Standard Formula.

Section 2 of the paper covers the aims of the research and the scope of the paper. Section 3 considers methods available to use to capture Cyber Risk potential within a capital model, including parameterisation selections and Cyber Risk results within a capital model. Section 4 covers the Validation of Cyber Risk Modelling in Capital Models, and finally, Section 5 completes the picture by discussing how an effective enterprise risk framework would manage potential Cyber Risks.

3. Parameterisation Methods for Cyber Risk

In this section, we discuss a range of methods commonly used during parameterisation – the suitability of each and cyber-specific adjustments and limitations as well as other potential considerations.

We will start with a quick reminder for the reader of what a capital model is doing; at a high level, one simulation of a capital model typically simulates losses at each type of loss and risk level, before aggregating up to determine an instance of a balance sheet outcome that represents what an insurance company could experience. Then the balance sheet distribution is determined by generating lots of simulations; it is the ordering of these simulated results and selecting a return period (i.e. the 99.5th percentile if capital setting is determined at the 1-in-200-year point) by which capital can be set.

By parameterisation, we refer to the selection of inputs to be used when determining the simulated outputs, that is, inputs to use that will generate the Cyber Risk losses/profit to be used as part of the internal model balance sheet calculations.

There are a variety of Cyber Risk parameters that need to be considered, and these will vary for a company depending on its exposures. The main categories of parameterisation to consider are as follows:

- Underwriting risk
- Reserving risk
- Operational risk
- Reinsurance (RI) credit risk
- Dependency modelling

Note that for each type of modelled risk, there are also two further general categories of parameterisation to consider:

- The distribution types and/or method of generating losses
- The parameters/inputs to use within the selected distribution types/parameterisation approach

In this section, we will consider each of the above in turn. Note that when we refer to Cyber Risk losses, losses can be negative (i.e. gains/profit). Indeed, when simulating potential outcomes from cyber distributions that relate to underwriting losses, on average, an insurance company would typically expect to make a profit. That is, the loss distribution would be negative (i.e. profitable) at parts of the distributions but then likely positive (loss making) at later parts of the distribution. It is important to keep in mind that a capital model does also capture the upside potential of risk types.

The information provided in this section is intended to be a summary of the salient points for consideration rather than prescriptive guidance. The focus will be on providing the key parameterisation approaches currently employed by insurance companies and Cyber Risk related

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

discussion. Limitations will be mentioned alongside the methods, but the reader is also referred to Section 3 which explores the importance of validation in this context.

3.1. Underwriting Risk

Cyber underwriting risk refers to the risk that premiums collected on policies that include cyber exposures are not adequate to cover the potential losses. In this section, we consider each of the four main types of typical parameterisation methods that are currently employed for parameterising cyber underwriting risk: experience based, exposure based, scenario modelling and the use of third-party vendor modelling. In reality, firms will use a blend of multiple approaches depending on loss and risk type being modelled, the firm’s exposure and materiality of that risk, how long they have been writing that book of business/had exposure to that risk as well as their modelling capabilities, etc.

Generally speaking, now that non-affirmative Cyber Risks are being mandated out of contracts and insurance companies are explicitly pricing for them in contracts (Cartagena & Grewal, 2021), non-affirmative Cyber Risk exposures should be now reducing. However, given that these will typically fall under different classes of business, some companies may choose to model these in aggregate (or separately from) other cyber exposures. Non-affirmative Cyber Risk parameterisation methods will be similar to those employed for affirmative Cyber Risk parameterisation, although there will likely be further lack of data available for the former even relative to the latter. The key will be to understand the potential interconnectivities between losses from cyber underwriting losses – affirmative or non-affirmative – coming from different classes of business which may be triggered at the same time to provide significant aggregated losses; this will be discussed further in the dependency section.

A key consideration of parameterising underwriting risk is whether the historic data is a good guide to the future for modelling future exposure. It could be reasonably argued that the market understands the severity of the losses relatively well and that wordings have evolved so that there is much more certainty in this area. However, there is still a clear and difficult task to understand the frequency and scale of future events where the past is not likely to be a strong predictor for the future (Sophos (2022)). Recent events such as the Ukraine and Russian war further heighten this uncertainty and the challenge to parameterise the class of business. A clear view of the threat actor landscape and potential for future attacks is crucial to the estimation of loss and volatility inherent in the business. Hence it may be that models either need to re-parameterise in detail often considering the threat landscape or allow for more volatility than they might usually consider reflecting this unknown element.

What is clear is that threat actors are growing in ability and scale and therefore the threat landscape continues to evolve rapidly, and hence, considering the characteristics of the distributions selected is important, and more reliance may be needed on expert judgement for forward-looking risk assessment. Capital modellers should encourage their parameter providers for Cyber Risk to justify their selections clearly and demonstrate understanding so the output can ultimately be communicated to management.

As mentioned above, parameterisation involves a selection of a parameterisation method as well as parameters to use within methods.

3.1.1. Method selection

General parameterisation

The way that underwriting risk is modelled can vary significantly depending on the loss type being modelled. Underwriting risk is generally modelled through the following methods:

- **Modelling separate frequency and severity distributions**. That is, modelling the count of losses and, given a loss occurs, modelling the size of that loss separately. For example, a Poisson or negative binomial distribution for the frequency distributions and a lognormal or Pareto distribution for the severity distribution.
- **Modelling a block aggregate distribution**. This involves simulating one number from a modelled distribution which would represent the total aggregate loss number from that risk type over the simulated period, as opposed to generating the count and size of each loss separately. For example, this is commonly used to model total attritional losses in aggregation over a year.
- **Use of third-party simulated data** (or data generated outside of the capital model) such as Year Loss Tables (YLTs) or Event Loss Tables (ELTs). These consist of usually tens or hundreds of thousands of simulated years and possible associated events with associated losses. A capital model would then simply simulate a loss by selecting a loss that has already been generated by this table. This is an especially effective way of using information from teams such as exposure management or third-party software who may be able to provide more information relating to the size and range of potential losses; of course, all data would be subject to the usual rigorous validation processes and usually brought onto a projected future basis.

Cyber risk specific considerations

Capital modellers will commonly be faced with a lack of data to parameterise the extreme tails of the underwriting distribution of most classes of business; however, the cyber underwriting class brings further limitations. The changing nature of the class with its changing drivers, threat actors, loss trends, increasing interconnectivities between companies due to technological advances and ever-varying targeted industries make (the lack of) historical experience of limited use when trying to predict future loss potential. Moreover, there are also various data limitations associated with cyber beyond the lack of data available to use; for example, the industry is still working towards standardising cyber data and other issues such as changing categorisations (e.g. from the movement away from non-affirmative towards affirmative cyber), and unclear loss causation codes add to the difficulties of sourcing clean data to use within parameterisation processes.

Note the general parameterisation methods listed above. Insurers typically used block aggregated modelled distributions for modelling attritional losses, separate frequency and severity distributions for large and (some) cat losses and YLTs/ELTs for losses where there may be modelling already available. However, in the context of the cyber underwriting class of business, there may be uncertainty or variations between views of what a “large” cyber loss is and what is deemed to be “attritional”. Typically, a threshold is used which may be based on outwards reinsurance contract attachment points or a view given by the underwriting team for what they deem to be losses of notable size. Similarly, given the lack of historical experience, there may also be varying levels of appreciation of how big a cyber “cat” event may be.

It is important to appreciate that these categorisations can be important when parameterising a capital model. Some capital models may only allow recoveries from simulated large/cat losses (e.g. if there is an excess of loss outwards reinsurance contract in place), but also there may be different dependency assumptions being made between the different loss types; these factors can all have material impacts on capital model results in cases where material cyber underwriting losses are being written. This illustrates the importance of working towards a consistent approach in handling, storing and processing Cyber Risk data as part of parameterisation processes and for capital modellers to work closely with other teams – such as claims, underwriting, reinsurance purchasing and exposure management – to ensure that Cyber Risk distributions being modelled are appropriate.

Indeed, the point of separating the parameterisation of attritional and large cyber losses is to create more homogeneous sets of data – to be used within the parameterisation process – by the separation. Due to the ever-changing nature of the cyber class of business, including the changing

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

drivers of loss, the attritional/large split may need to be revisited frequently. Note that changing loss categorisations can have implications on year-on-year analyses of change reporting as well as validation. For example, if more losses were categorised as attritional rather than large due to a changed large loss threshold, say, but the overall parameterised level of loss remained the same, this could artificially trigger conversations regarding the need for a change in outwards reinsurance strategy that may or may not be appropriate.

Most capital models across the market are likely to apply standard frequency and severity methods to model the line of business consistent with other lines of business. However, in order to deal with the uncertainty in the threat landscape generated by the ever-evolving threat actors and threat vectors, it may be that capital modellers would consider new approaches to modelling the risk such as a risk driver and/or Bayesian framework. These methods could better represent the changes in the fast-moving landscape; however, their limitations include the level of parameterisation and data required to produce a robust model. Furthermore, they would require regular review and updates at a potentially granular level which many companies may not have the resources for. Each company will have to weigh up the pros and cons of any more complex approaches for their own risk exposure and the materiality of Cyber Risk to their capital.

If the company chooses to license one or more vendor models, then it is common to use the model to assess what adverse situations for your risk profile looks like and supplement it with your own scenario modelling before developing more sophisticated approaches (e.g. blending). You will then need to consider how this informs your view of risk and how to include this view in the capital model. The most common approaches would be to adjust an ELT/YLT to align to your view of risk or apply an uplift to bring the output into line with the company's expectations of loss at certain return periods and to ensure the tail is sufficient.

3.1.2. Parameter selection

Once a parameterisation method has been selected, the parameters to use within the method need to be determined and we discuss the main methods below.

3.1.2.1. Experience based.

General parameterisation

Generally, across most general insurance classes where there is deemed to be sufficient and relevant historically observed experience, experience-based methods, such as the method of moments or maximum likelihood estimation (Hossack *et al.*, 2003), are used to determine parameters for frequency and severity distributions and sometimes also distribution type selections; other standard best practices such as goodness-of-fit techniques and sense check discussions with the underwriting teams are also incorporated to assist with the parameter selection process.

Cyber risk specific considerations

In the context of cyber, where the true potential range of losses in the tail is still yet to be fully appreciated, there is uncertainty in the level of tail losses that need to be allowed for. Some insurers may opt for the usual approach, as with their other classes, of selecting distributions such as lognormal or generalised Pareto distributions for the loss severity curves; the reader is referred to further reading relating to extreme value theory (Paddam, 2001) to understand the various distributions that may be considered and associated distribution fitting exercises.

For the loss frequency curves, given that insurance experience data usually exhibit overdispersion, a negative binomial distribution may be considered amongst other distributions (Ismail & Jemain, 2007). Again, as with claims severity data, there may be an insufficient count of claims with which to meaningfully fit a frequency distribution. Furthermore, there is added uncertainty due to the ever-evolving cyber landscape, and this makes loss experience of limited use

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

within distribution fitting as a general increase in loss frequency has been experienced by some over recent years.

It is often a useful exercise to simulate the count of losses and size of losses separately, particularly for the larger losses, as this can trigger a deeper appreciation of losses in the final output distribution relative to when an aggregate distribution is used. For example, conversations move from *we expect a loss ratio of 110% at a 1-in-5 return period* to *we expect a loss ratio of 110% at a 1-in-5 return period and we expect a loss of size $5m once every 3 years with average 2 large losses a year*, say. This enables deeper validation and interrogation of the assumptions being made and makes frequency and severity assumptions explicit rather than implicit. Attritional losses are often modelled in aggregate with large and catastrophe losses modelled in a more sophisticated manner.

Furthermore, despite the uncertainty inherent in modelling the ever-evolving cyber class of business, the consideration of absolute maximum loss potential can also be a useful exercise within parameterisation processes, for example, quantifying the maximum loss exposed and then subsequently comparing this against the parameterised loss distribution as a sense check of the associated return period. This can then trigger conversations regarding whether the absolute maximum loss exposed should be considered at a more, or less, extreme point on the parameterised loss distribution.

Within distribution fitting exercises, the use of a company's personal historical experience relevant to the book of business being written will always be preferred. Historical data may need to be adjusted for a range of reasons to bring onto the projected loss year's perspective; considerations might include regulatory landscape changes, adjustments to terms and conditions, changes to loss drivers (e.g. the recent Russian invasion of Ukraine might be considered to trigger increased cyber activity) and general allowance for claims inflation. Some companies may look to augment limited historical experience with other relevant data, such as industry data or proxy data (e.g. scenarios which are considered later). However, such relevant additional data may not be readily available, and in the case of cyber, there is a lack of credible industry data or classes of business similar enough in profile characteristics to be deemed as appropriate proxies.

In the case of cyber, it should also be emphasised that the threat landscape (i.e. dark web activity) is likely to be a much better indicator of the frequency parameterisation than any historical data available. At any given time, the threat actor activity and vulnerability/threat vectors that are exposed lead to a heightened or more benign risk outlook. For example, at the start of 2022, there was low ransomware activity largely attributed to the outbreak of the Ukraine–Russia conflict. However, consideration must be given to the fact that the war is producing many weaponised cyberattacks that whilst currently are focussed on war activity may be redirected to criminal activity. Hence capital modellers should be aware of the evolving threat landscape which may mean that cyber capital requirements are more volatile year to year than other classes.

3.1.2.2. Exposure based.

General parameterisation

In other cases, some classes of business may have insufficient or irrelevant historical experience; for example, if the risk profile being written has changed dramatically or if the class of business has just been entered. In such cases, there are range of alternative methods which can be considered:

- Some insurance companies may use exposure-based methods in such cases where there is information available about possible losses and associated likelihoods. For example, increased limit factors or information from underwriters/brokers may be used. However, such information obviously has its limitations and can be very subjective.
- Some companies may apply damage factors to exposed limits and associated likelihood to various parts of the book (overlaying further assumptions) to simulate possible losses via an

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

exposure-based method. A distribution fitting exercise can then be applied to the simulated losses to determine possible parameters to consider.

- Alternatively, some capital modellers when faced with limited historical experience to use within parameterisation may look to other classes to use as a proxy class until further experience is observed.

Cyber risk specific considerations

In the context of cyber, where there is limited information available and with the absence of a similar class of business with similar risk characteristics, given cyber has evolving risk profile with interconnectivity across industries and geographies, parameterising exposure-based methods can also be a complex process which requires the involvement of cross-departmental expertise, supplemented perhaps with external Cyber Risk expertise.

More specifically, a variety of data that is collected throughout general business as usual (BAU) processes could be utilised to help parameterise an exposure-based method.

For example, in the case of operational Cyber Risk, it is common to use the company's risk register as the data points to parameterise potential losses that could occur as part of capital modelling balance sheet simulations. This could be further enhanced by considering detailed scenarios, as per the discussion in the Cyber Risk Working Party's first paper (Institute and Faculty of Actuaries' Cyber Risk Working Party, 2018). Similarly, the silent cyber assessment framework as developed by this working party (Institute and Faculty of Actuaries' Cyber Risk Working Party, 2021) could be used to parameterise non-affirmative Cyber Risk.

For affirmative Cyber Risk, data collected during pricing and underwriting processes could also be incorporated into exposure-based methods to make parameterisation tailored to the risks being underwritten. Ideally, in the future, systems supporting Cyber Risk underwriting will evolve to incorporate real-time information (which will be collected for other purposes such as exposure management, risk management and business monitoring), and this information, whether dynamic or static, should also feed into capital modelling processes.

This is particularly important given mandated changes from Lloyd's (regarding making coverages clear and if cyber is included, then ensuring it is being priced into premiums explicitly). Captured information can be used to feed into parameterisation and understanding changes to the underlying exposures at risk.

3.1.2.3. Scenario modelling.

Related to exposure-based parameterisation methods is scenario modelling. Over the past decade, most general insurers with material exposures to cyber underwriting risks now will likely have created a range of potential loss scenarios as part of their risk management processes; such scenarios are likely to have been created, maintained and regularly reviewed by a cross-disciplinary team including exposure management, risk management, claims, underwriting and actuarial. These scenarios can provide invaluable information about the potential of losses and views around the potential likelihood of occurrence, especially in the absence of more credible and available data as is the case when considering cyber underwriting risk. Such scenarios are also designed to cover events that would not already be in the data (ENIDs).

In the Lloyd's of London general insurance market, there are also some regulatory prescribed realistic disaster scenarios (RDSs) (Lloyd's of London, 2021b) that consider cyber underwriting exposures. These include a "Major Data Security Breach", a "Business Blackout", a "Cloud Cascade" and a "Ransomware Contagion (Bashe attack)". Regulators, third-party model vendors (see below) and research organisations also continue to produce cyber scenarios events which may also provide a useful resource to understanding the potential impacts.

Other examples of scenarios that could be considered include those that would be generated, for example, by the Silent Cyber Assessment Framework (Institute and Faculty of Actuaries' Cyber Risk Working Party, 2021).

General parameterisation

In many cases, the scenario losses may contain a level of subjectivity (even, such as in the case of the last three RDSs mentioned above, where assumptions have largely been prescribed) and be sensitive to key assumptions such as data categorisation; it is not unusual for capital modellers to apply uncertainty parameters around scenarios to allow for this uncertainty. That is, the following approach could be taken to simulate from the scenario in a capital model:

1. Take the scenario loss and associated return period onto the projected period basis. That is, if the cyber underwriting risk book is anticipated to change (beyond that due to rate change) and/or the risk profile is anticipated to change, then would we need to adjust the underlying scenario assumptions, the assumed severity of the loss, the associated likelihood of loss or even all three?
2. In every simulated capital model year, simulate a loss to occur once every X years where X is the assumed return period selected.
3. When that loss occurs, the size of the loss is determined by sampling off a severity distribution which has a mean loss that equals the size of the selected loss, but a small coefficient of variation has been applied to allow for uncertainty; the distribution parameters of the severity distribution can be determined using a distribution fitting exercise based off the mean and coefficient of variation.

Cyber risk specific considerations

In the context of cyber underwriting risk, it is especially important that the scenarios being considered have been tailored to specific concerns/company exposures rather than being reliant on scenarios solely maintained for regulatory purposes. Scenario modelling may be very sensitive to the underlying assumptions being selected; however, if done in collaboration with cross-departmental teams, these can be invaluable in providing supplementary information about possible capital "tail" events that may not otherwise be included in the capital model. Similar practices may already be used for other classes of business such as liability classes or marine and aviation classes where there is a lack of modelled data available.

One of the more practical challenges of scenario modelling for cyber is how to attribute return periods to the events designed. To best develop, understand the impacts and communicate cyber scenarios, it's crucial that all areas of the business are involved as well as including cyber security experts where possible. The cyber scenarios are very complex and rely on a technical understanding of information technology (IT) infrastructure to fully understand and appreciate the likelihood and potential severity of any loss. Hence, it's crucial to include this expertise to ensure the losses estimated from this scenario process are reasonable.

3.1.2.4. Third-party vendor modelling.

At the time of writing, there are multiple vendors offering Cyber Risk modelling software and capabilities to the insurance market; it is not within the scope of this paper to compare and/or contrast the various offerings. It is important to note that there is a range of third-party support that could be considered and incorporated as part of capital modelling parameterisation processes, ranging from full quantification models (e.g. Cyrence (2021) or Willis Towers Watson (2021)) to cyber security information feeds which could also be useful (e.g. Fitch Ratings (2021) or Security Scorecard (2021)).

Third-party models can be used to supplement information available to be used as part of exposure-based parameterisation methods or to help develop detailed loss scenarios.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

Some third-party vendor cyber modelling capabilities have developed significantly over recent years and now can even provide outputs, similar to what would be expected from natural catastrophe models (i.e. ELTs with simulated losses by thousands of simulated loss years being developed).

The advantages of using third-party vendor modelling are that they can be used to help augment data which may be lacking in volume due to limited historical experience/internal data capabilities or sophistication. Third-party vendor models are also usually developed by Cyber Risk specialists and such specialist expertise may not be available in each insurance company otherwise. However, as with any external model, the data may need tailoring and may not be relevant; it is the responsibility of each company to understand the capabilities and associated limitations, process nuances and the assumptions of any model or information being used within any capital modelling parameterisation processes.

Validation of third-party vendor models or any external data is very important, and this area is discussed in further detail in Section 3. A couple of key considerations when working with third-party vendor models are as follows:

- Each cyber third-party vendor model may use a blend of factual information, combined with expert judgements. As with most models, models are useful in enabling conversations and appreciation for a potential range of losses and the potential sensitivity to uncertain assumptions, rather than being able to provide specific figures that can be used as figures that are perfect predictors.
- Stability and reproducibility of results is key. The volatility of results over time should be understood and using a refreshed version of a third-party's vendor model should not cause unexpected impacts on parameterisation, and thus capital, without any movements and/or changes to assumptions or methodology being understood. Note that some cyber vendor models may not always be opaque with their own modelling or parameterisation methodology citing concerns of their IP being lost to competitors (and, indeed, some third-party vendors may use interesting data sources such as the dark web!); as part of a Solvency II framework, such obstacles need to be carefully worked around as all sources feeding into capital modelling parameterisation processes need to be adequately validated.

3.2. Reserve Risk

The parameterisation of cyber underwriting risk captures the loss (and profit) potential of risks written in the projected business year as well as any unearned business from historical years. Cyber reserve risk parameterisation captures the risk that the cyber reserves, as at the internal model time = 0 date, are insufficient to cover their run-off.

There are a variety of methods that are commonly considered as part of reserve risk parameterisation – such as Bootstrapping or Mack's model – and the reader is referred to a useful paper on the "Practical Challenges in Reserve Risk" which contains good summaries of techniques (Chan & Ramyar, 2016). Given that many insurers and reinsurers may have limited cyber historical claims experience which would often be the initial starting point for any reserve risk parameterisation, reserve risk parameterisation faces similar issues as faced within the underwriting risk parameterisation. It is likely that many insurers currently have insufficient data to perform a bootstrap and thus must rely either on more market statistics or expert judgement in setting their reserving risk volatilities.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

Given the developing nature of the cyber class of business, the ever-changing nature will also be seen in claims patterns and reserve risk information which would typically be used as part of the reserve risk parameterisation process.

Changing aspects could include the following:

- Changing development patterns due to ransomware impacts.
- Changing the duration of the tail (in situations where there might be delegated authority/ claim disputes).
- Changing cyber categorisation (e.g. changes in Lloyd's risk code categorisation of business between the CY and CZ risk codes in light of mandated changes).
- Changing split of attritional, large and catastrophe cyber losses; this could be due to underlying drivers changing as threats develop (and mitigating strategies are developed).
- Changing severity of losses with the range of threat actors continually developing (e.g. from sole hackers to state backed attacks).
- Changing severity of losses due to inflationary pressures.
- Changes in the geopolitical landscape.
- Changing policy wordings, these are frequently updated and these changes may impact the type of losses being seen in portfolios (e.g. affirmative language and cyber war exclusions).

3.3. Operational Risk

General parameterisation

The methods used to model cyber operational risk might be similar to the approach employed for modelling other operational risks. There are a number of good reference guides available which explore operational risk modelling best practices; for example, the reader is referred to the "Good practice guide to setting inputs for operational risk models" by the operational risk working party as a good general reference guide (Institute and Faculty of Actuaries Operational Risk Working Party, 2016).

Cyber risk specific considerations

Most insurance companies will maintain a risk register that will include a range of operational risks. Due to the occurrence of cyber events over the recent years, many risk registers will now also include cyber operational risks. This information will be an important starting point for any cyber operational risk parameterisation exercise (as is also the case with other types of operational risks).

Risk registers may only give loss estimates; however, conversations regarding the inherent uncertainty in that loss estimate will need to take place ahead of operational risks being entered into a capital model to capture the volatility required in the risk's parameterised distribution.

It is important that meaningful cyber operational risks are captured in the risk register that is relevant and appropriate for the insurance company rather than generic risk scenarios. To this end, the reader is referred to an earlier paper produced by the Cyber Risk Working Party which gives detailed guidance on this topic (Institute and Faculty of Actuaries' Cyber Risk Working Party, 2018).

When considering the cyber impact on their operational risk, companies should consider all sources of risks that drive the scenarios such as

- the company's IT infrastructure
- the cyber security posture of the company and what mitigations are in place (i.e. data backups, server redundancies)

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

- impact of a cyberattack on critical services, that is, claims handling/processing, BAU operations and premium collection
- the company's risk as a member of a corporate group/subsidiary operating in many territories
- risk of insider or "fat finger" losses and what mitigations the company has in place
- any legal and/or regulatory consequences of a cyberattack, for example, fines and reputational damage

These conversations should at a minimum include the chief technology officer of the company who should take ownership of the estimates. Operational risk scenarios are another example of where attaching a return period can be challenging and Cyber Risk events are potentially even more difficult given the lack of historical events and the changing landscape.

Companies need to attempt to be realistic wherever possible in their return period estimation; just because the event has not happened or previously seemed unlikely does not automatically mean that based on the current risk and threat landscape, the loss potential and return period remain static from year to year. Hence therefore it is crucial to engage with the IT team and/or external experts on cyber security wherever possible.

Another key consideration in operational risk is the obvious potential positive correlation of large or catastrophe cyber events whereby the company could also be impacted by an event which is driving losses to their portfolio which could have impactful consequences depending on the event and company defences.

3.4. Reinsurance (RI) Credit Risk

Finally, another area of the parameterisation of a capital model which must not be overlooked when considering the potential of Cyber Risk losses is RI credit risk. "The reinsurance credit risk is the risk of the reinsurance counterparty failing to pay reinsurance recoveries in full to the ceding insurer in a timely manner, or even not paying them at all" (Britt & Krvavych, 2009).

RI credit risk is particularly important when considering extreme events which may trigger losses across numerous accounts/classes of business/insurance companies/types of risk, given the high potential interconnectivity of Cyber Risk exposures.

Recent high-profile legal disputes over cyber policy coverages illustrate that disputes can occur (Bloomberg Law, 2022). An extreme cyber event could trigger recovery disputes as well as solvency issues in cases where reinsurance purchased involved a reinsurer who may have been significantly exposed to a cyber event – for instance, through accumulation risk within the reinsurer's own Cyber Risk portfolio.

For details of how RI credit risk can be modelled within capital models, the reader is referred to useful guides available through previous work done by members of the profession (Britt & Krvavych, 2009).

In particular, a number of insurers now also consider a cyber stress test analysis as part of their risk management/capital modelling validation processes. Here, not only the obvious parameters such as cyber underwriting risk and cyber operational risk parameters need to be considered but also RI credit risk assumptions (such as the probability of default assumptions and loss given default assumptions). In the context of cyber, it's important to remember that a reinsurer may be exposed to cyber operational risks which are correlated to the risk it faces through its underwriting activities, further stressing the potential for RI credit risk. Indeed, the 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 (Fitch Ratings, 2022).

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

3.5. Market Risk

Cyberattacks on financial institutions and financial market infrastructures are becoming increasingly common and of high value to threat actors. The International Monetary Fund (Kopp *et al.*, 2017) prepared a paper that considers the impacts of systemic Cyber Risk interacting with other financial stability risks and the regulatory frameworks and supervisory approaches. Whilst most companies are likely to take direction from the Economic Scenario Generator providers on parametrisation for market risk, it should not be ignored that cyber threats pose an emerging risk to financial market stability. The Swift cyberattack is an example of a potential attack that could have consequences and produce greater economic uncertainty. Companies should consider whether they consider the tail of their market risk distributions and/or any drivers of loss are materially impacted by the current Cyber Risk landscape.

Furthermore, geopolitical instability resulting in severe Cyber Risk attacks on critical and/or economic infrastructure could have serious economic impacts and should be at least considered and discussed.

3.6. Dependency Modelling

Dependency modelling within an internal capital model of an insurance company is commonly now achieved using copulas; it is beyond the scope of this paper to fully explore copulas, how to model them and why copulas may be used; however, the reader is referred to reading available for further information (Shaw *et al.*, 2010).

In this section, we explore the considerations specific to Cyber Risk exposures which would need to be factored into dependency modelling parameterisation processes.

3.6.1. Dependencies between risk types

An internal model may already allow for dependency modelling between different types of losses (i.e. between attritional and large losses, between cat and non-cat losses, between accident years, between classes of business, between types of modelled risk and so on). As with any risk, all such dependencies should be reviewed in the context of the risk in question. Given the nature of Cyber Risk coupled with the usual difficulties in parameterising dependency structures due to the lack of historical experience to parameterise the tails, particular care should be given to consider the potential for dependencies beyond what may seem obvious.

A good example of this was observed during the recent coronavirus disease 2019 (Covid-19) pandemic, when there were concerns that the working from home arrangements could trigger increased loss experience for both cyber operational and underwriting risks. Such concerns were prolonged by the recent invasion of Ukraine by Russia. These examples highlight the need to look away from obvious situations where losses may be correlated since the pandemic had the potential to trigger losses across a wide range of classes of business as well as other non-underwriting risks – some of which might have otherwise been deemed to be uncorrelated.

3.6.2. Appropriate copula type selection

The useful Figure below (Figure 2), which has been taken from a “On the aggregation of credit, market and operational risks” paper (Li *et al.*, 2015), illustrates the most well-known copulas and illustrates how copulas, such as the Clayton, can assist in achieving asymmetric dependencies at different ends of the distribution. The clayton copula can be used in situations where the modeller wants higher dependence in one distribution tail than the other – that is, when we want to model more dependence in an extreme stress event, such as those that might be modelled when considering Cyber Risk exposures.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

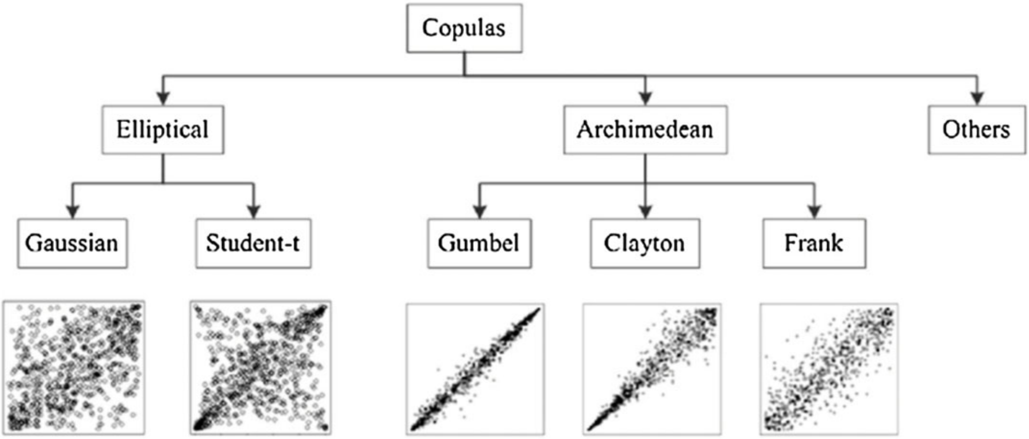


Figure 2. Examples of copulas and the distribution asymmetries that they can assist in achieving.

3.6.3. Other ways to model dependency/increase tail dependency where required

Finally, another approach that can be used to model dependencies – or even "top up" dependencies in models where increased dependency between variables is required at various points in the distribution is through explicit scenario modelling.

For example, if we wanted to model the potential for a pandemic to trigger losses across loss types, classes of business and risk types, then we could explicitly parameterise a scenario to occur with a specific return period in the simulations. For example, imagine that we expected a pandemic to occur once every 50 years, say, then the capital model could simulate losses for this pandemic to occur with a 2% probability (=1/return period of 50 years). When this loss is triggered in the simulations, then we could explicitly trigger this to cause losses – of an amount to be specified by the modeller – in the following loss distributions at the same time:

- Underwriting risk (various classes of business as required)
- Reserve risk
- Operational risk
- Market risk, etc.

This then creates manufactured correlations between the loss distributions, as required. Of course, volatility assumptions could also be applied to the severity and frequency assumptions to allow for uncertainty in the parameterisation process.

3.7. Capital Allocation

General parameterisation

The practice of allocating capital across risk categories is already commonly performed in many insurance companies for a variety of reasons such as business planning, portfolio optimisation and return on capital considerations at a class/department level (e.g. for the purposes of underwriter and staff remunerations purposes or business strategy decisions).

There are a number of sources available that discuss the advantages and limitations of a wide range of allocation methodologies; these are not discussed in detail here, and the reader is referred to the following sources for further information (Institute and Faculty of Actuaries Capital Allocation Working Group, 1999) and (Venter *et al.*, 2003). Figure 3 below outlines the key considerations.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

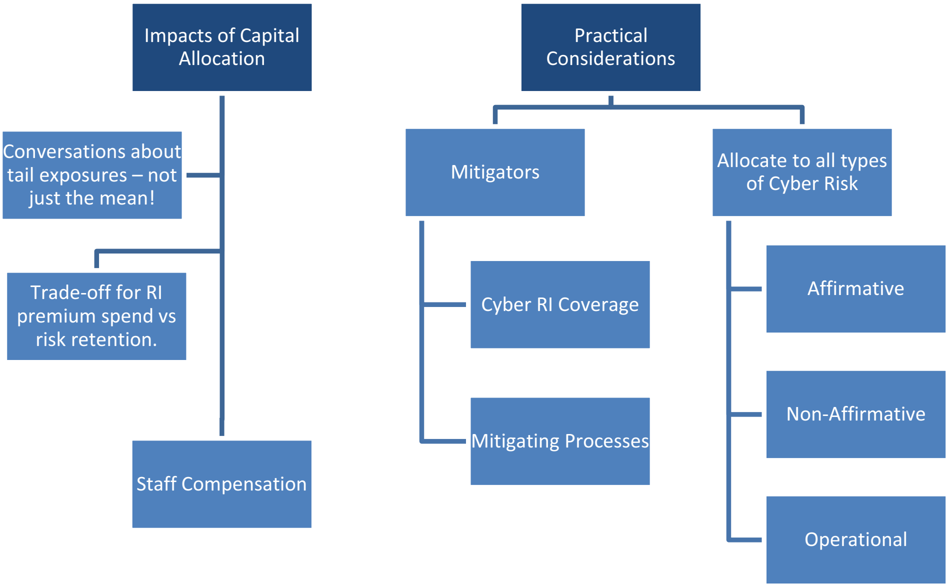

Impacts of Capital Allocation
Conversations about tail exposures – not just the mean!
Trade-off for RI premium spend vs risk retention.
Staff Compensation
Practical Considerations
Mitigators
Cyber RI Coverage
Mitigating Processes
Allocate to all types of Cyber Risk
Affirmative
Non-Affirmative
Operational

Figure 3. Key considerations when allocating capital.

Cyber risk specific considerations

In the context of cyber, capital allocation becomes particularly important and a useful tool to use in communications with senior management to demonstrate the potential for Cyber Risk losses which may not otherwise be perceived as material. Presenting a clear capital allocation, alongside the accompanying limitations of the analysis, assists in helping senior management move away from what they might expect the Cyber Risk potential to be (i.e. focussed at the mean and intuitively parameterised based on a lack of historical observations of the risk potential) to the loss potential that a more extreme event could achieve; this is an important distinction since a key responsibility of senior management is to manage balance sheet volatility to be within risk tolerances.

Capital allocation is also important in recent times given the rapid increases in Cyber Risk rates being charged in the market (whether operational Cyber Risk insurance or cyber underwriting risk reinsurance). Understanding potential capital allocations of cyber operational and underwriting risks helps senior management consider the premium budget versus risk trade-off between retaining the risk or potentially ceding it away to another (re)insurance organisation.

From a practical standpoint, when capital is being allocated, it’s key to consider the range of Cyber Risks being captured in the model and not just cyber underwriting risks. That is, allocate capital to the following:

- Cyber underwriting risks written through a cyber class of business.
- Cyber underwriting risks written through other classes affirmatively.
- Non-affirmative Cyber Risks.
- Cyber operational risks.
- Any mitigating impacts from cyber reinsurance or coverage that may have been purchased.
- Potential of any systemic Cyber Risk events to impact the macro-economic environment and thus drive losses in market risk.

Correlation impacts from Cyber Risk are an important consideration even if the company does not write affirmative cyber portfolio for these items listed. Hence, whilst it may not be deemed a

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

material risk and/or dependency in the model, it should be considered because potentially in some extreme events a cyber operational loss could impact other lines or areas of the business such as Market Risk.

3.8. Conclusion

The information provided in this section summarises the key considerations when parameterising cyber risk within capital models. Note that the working party interviewed various capital teams across the London Market when preparing this review and found that most teams were at very early stages of feeling confident in their modelling approaches. There is often an information asymmetry of the risk at the underwriting stage and how this translates to capital modelling. This is even more challenging for cyber risk. Hence, we encourage capital teams to deep dive and think holistically about the risk cyber poses to the business. For example, diversification across lines of business and across risk areas could be material impact capital, and this should be carefully considered in the parameterisation of the model.

4. Validation of Cyber Risk Modelling in Capital Models

4.1. The Importance of Validation

An important part of the capital modelling process is the validation process to enable other stakeholders to have the confidence that the way the risk has been modelled is suitable. It is vital to validate any model to ensure the predictive power of the model is sufficient to make conclusions given the known limitations of the model. Cyber Risk modelling remains in its infancy and will continue to develop, likely at a rapid speed to improve both its complexity and to remain relevant with the emerging Cyber Risks.

The validation of Cyber Risk in the capital model should cover not only the validation of Cyber Risk as a product but also as a peril across the entire business. Validators should ask the question as to whether all the risks that the company faces as a business arising from Cyber have been included in the distribution. This validation should include assessing how the impact of Cyber Risk on operational risk, dependencies between lines of business and dependencies between risk types allowed for. To some extent, all companies are exposed to Cyber Risk even if they are not writing cyber products, and hence, this assessment should form part of the validation process.

Furthermore, companies will need to demonstrate that board and senior management have sufficient understanding of the cyber models including the data required and their limitations. This will be a challenge given the rate of change and complexity of the risk to keep the board educated so that they are able to make informed decisions for the business.

4.2. Validation Approach

The validation should ensure there is the appropriate level of experience and expertise capable of validating Cyber Risk as well as a truly independent challenge. 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 is important that the challenge contains some expertise in the cyber security space so that any material issues are not overlooked.

When validating the approach to modelling Cyber Risk in the capital model, companies should consider the standard set of validation tools. However, given the maturity of the risk modelling, some of the more relied-upon validation tools will be less useful than for other risks. Figure 4 summarises the ordering of how useful different validation tools are when considering cyber risk.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

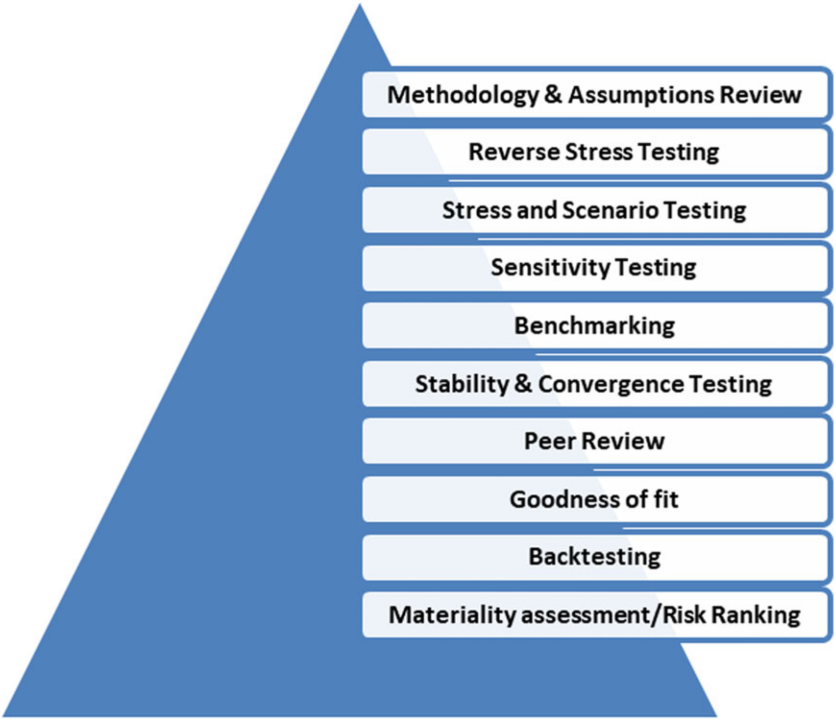

Methodology & Assumptions Review
Reverse Stress Testing
Stress and Scenario Testing
Sensitivity Testing
Benchmarking
Stability & Convergence Testing
Peer Review
Goodness of fit
Backtesting
Materiality assessment/Risk Ranking

Figure 4. Examples of validation tools that may be appropriate to consider for cyber risk modelling.

Methodology and assumptions review

From a validation perspective, a regular review of the methodology and assumptions applied in modelling Cyber Risk should be undertaken regularly. The company's validation cycle is likely to define a periodic review of all lines of business, but companies should consider if it's appropriate to review cyber on a more regular basis. The Cyber Risk landscape evolves rapidly, and hence, both frontline and independent assessment should be made at appropriate times to reflect the changing nature of the risk. In recent years ransomware has become more and more prolific with the threat becoming almost a "ransomware as a service" enabling many more threat actors to undertake ransomware campaigns attacking supply chains and/or more targeted attacks on large corporates. The validation process should ask the question if both the reserve and underwriting risk approaches reflect this new loss profile.

The level of detail of the validation and how often the line of business is reviewed will ultimately depend on its materiality to the entity. However, the potential impact across other risk areas should not be ignored. The approach to modelling cyber as a peril on operational risk as well as its potential impact on noncyber lines of business should be considered in any model. If the risk is not explicitly modelled, companies should be able to articulate how they have considered the risk framework and ultimately what capital implications it has.

Sensitivity testing

Sensitivity testing of assumptions being made in parameterisation and understanding the impact on capital is key. All material assumptions should be tested against expectations to ensure the model is performing as intended. When reviewing the results of these tests in respect to Cyber Risk, validators should be considering if the sensitivity of the variables is appropriate given the current Cyber Risk landscape. Depending on the granularity of the risk modelling, this may require regular assessment to conclude if the parameters are appropriately calibrated. For

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

example, a rise in ransomware frequency may be the result of a new ransomware campaign that exploits a vulnerability that is difficult to patch. How this step change in the risk affects the premium and/or reserve risk parameters should be justified.

Stress and scenario testing
Stress and scenario tests are a useful tool to test the model in extreme situations to test if the modelled output is in line with expectations. For cyber, engaging with cyber security experts to provide realistic scenarios that may impact portfolios would add greater credibility to the validation tests. Some useful scenario tests for Cyber Risk could include the following:

- Reserve deterioration due to previously unknown emerging cyber losses and/or events.
- Profitability stress whereby the loss ratio for the cyber market deteriorates due to a widespread ransomware campaign.
- Assessing whether the modelled return period of certain cyber events is aligned with expectations at various return periods.

Backtesting
Backtesting refers to the process of testing the predictive models on historical data to assess whether modelled losses are in line with experience. The assessment of how the implied (modelled) return period of events compared with observed data is a challenge for cyber losses. There are two main issues presented with backtesting for cyber lines of business. First, the product is relatively new and so too is the claims experience to the market. Second, the fast-developing risk landscape from the ever-increasing sophistication of threat actors undermines the validity of testing the model against potentially outdated experiences.

Hence care should be taken with backtesting and not to ignore the expert judgement of the forward-looking risk that incorporates the changing risk landscape. This is perhaps where cyber as a line of business is most differentiated from other property and casualty classes, in that the past experiences may have limited ability to validate the expectation of the forward-looking risk. Whereas weather patterns and the risk related to them remain relatively stable year to year, Cyber Risk can dramatically change from year to year and hence impact the claims profile for the particular year of account. Over time, we may identify more predictive variables in the cyber threat and vulnerability landscape, which may allow us to model the risk more accurately. However, given this breadth of data is either in its infancy or not yet available caution should be applied.

Benchmarking
Benchmarking is a useful tool for any company to compare itself to the market it is operating in. Particularly the capital allocated for cyber against its peers may provide insight to understand if the company has a prudent or optimistic view of Cyber Risk. This is important information for the board but may not be available easily without the help of consultants who have access to the approaches across the market.

A crucial area of benchmarking for cyber catastrophe is to compare multiple model vendors and benchmark portfolio losses across various modelling approaches. These should also be compared to any realistic disaster scenarios developed by the company or submitted for regulatory purposes. Comparing Probable Maximum Loss (PML)/Occurrence Exceedance Probability (OEP) and Aggregate Exceedance Probability (AEP) from different model vendors is crucial to understanding the strengths and limitations of the cyber modelling across the market. This should help inform which vendor is most suitable for the portfolio and modelling approach adopted by the company and whether model blending is an option to consider.

Goodness of fit
For Cyber Risk, the claims history is likely to be too limited or not detailed enough to provide a basis for the most appropriate parametrisation; hence the focus for Cyber may be more aligned to

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

the review of the appropriateness of the "Events Not in Data" (ENIDs) loading in the technical provisions. It may also be the case that as the risk continues to evolve, the ENIDs may start to appear and evolve within the data. Companies should stay aware that the cyber portfolio will continue to change over time and in some cases may drastically change in respect to exposure and risk. For instance, the threat actors present at any one period of time may drive a very different frequency and scale of loss, as well as latency in the loss profile. All these aspects of the Cyber Risk landscape should be considered.

Materiality assessment/risk ranking

The objective of the validation process is to test that all material risks are assessed in the internal model. Companies should perform a risk assessment of cyber both in terms of the line of business and as a wider peril on its business operations. IT teams should then recognise to what extent the risk is captured by the model and elements are not captured explicitly by the model. Furthermore, if a risk related to cyber is identified as not being covered, then an assessment of its' materiality must be made and communicated to management. Ultimately, the treatment of Cyber Risk must be proportional to the size and complexity of the business and must be considered alongside all other areas of risk as whether all material risks are captured by the internal model.

Peer review

The rapidly changing environment and potential re-parametrisation annually of the cyber line of business makes peer review an important validation tool. Obtaining an independent opinion of the model output and results and its impact on the company enforces the challenge process and represents robust governance.

Reverse stress testing

Cyber as a peril impacting both the line of business and across other lines of business and risk areas may become an important reverse stress test scenario. Companies should not underestimate the potential impact of a cyber catastrophe event impacting the market as well as its impact on its own operational functionality. Possible examples of relevant reverse stress tests could include

- A major natural catastrophe occurring at the same time as a major ransomware event, causing an operational strain due to the company being unable to access its systems to make claims payments.
- A data breach of a company, resulting in the theft of significant confidential personal data from customers during a global pandemic.
- A cyberattack on a major stock exchange, causing market turmoil and losses to financial lines.

The reverse stress tests scenarios involving cyber are endless and must be specific to the risk profile of the company. However, as the Cyber Risk globally continues to grow, the company must consider to what extent they are exposed to it as a company failure event.

Stability and convergence testing

As with any other risk area, the chosen modelling approach for Cyber Risk must be stable and converge. The level of complexity in the cyber modelling approach is likely to determine at which level of simulations will converge as well as how the company chooses to model its cyber catastrophe risk.

Separate assessments of the cyber catastrophe convergence (especially if a vendor model ELT is used) should be performed.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

4.3. Deep Dive Validation on Cyber Risk Modelling

Validating Cyber Risk in the internal model can be approached as with any other line of business. Most current capital models would break the loss profile into attritional, large and catastrophe losses which is currently not an unreasonable assumption given the current profile of claims seen across the market. However, the market has yet to see a true cyber catastrophe event in terms of capital strain/erosion.

Attritional and large loss

When validating the attritional and large loss models, companies will have to consider the lack of data during the parametrisation process for both underwriting and reserving risks. Even where there is some history in the portfolio, it's suitability to the risk in the present must be factored in. Cyber Risk a decade ago is very different from that of today, and hence the parametrisation process must consider this. Nonetheless, historical events give a good indication of the cyber losses we may expect, and backtesting should be used to assess the model results. Significant recent data breach events (e.g. Marriot) provide the pricing teams and validators examples of major large losses involving various coverage types.

Ultimately, the validation needs to conclude whether the loss ratio at the mean and the 99th percentile is appropriate for the portfolio. It cannot be ignored that a large part of this assessment will need to be qualitative and forward looking.

Coverages offered has also changes over time and may continue to change to meet the needs of the insured, so care needs to be taken in the parametrisation of both reserve and underwriting risks that this is appropriately considered.

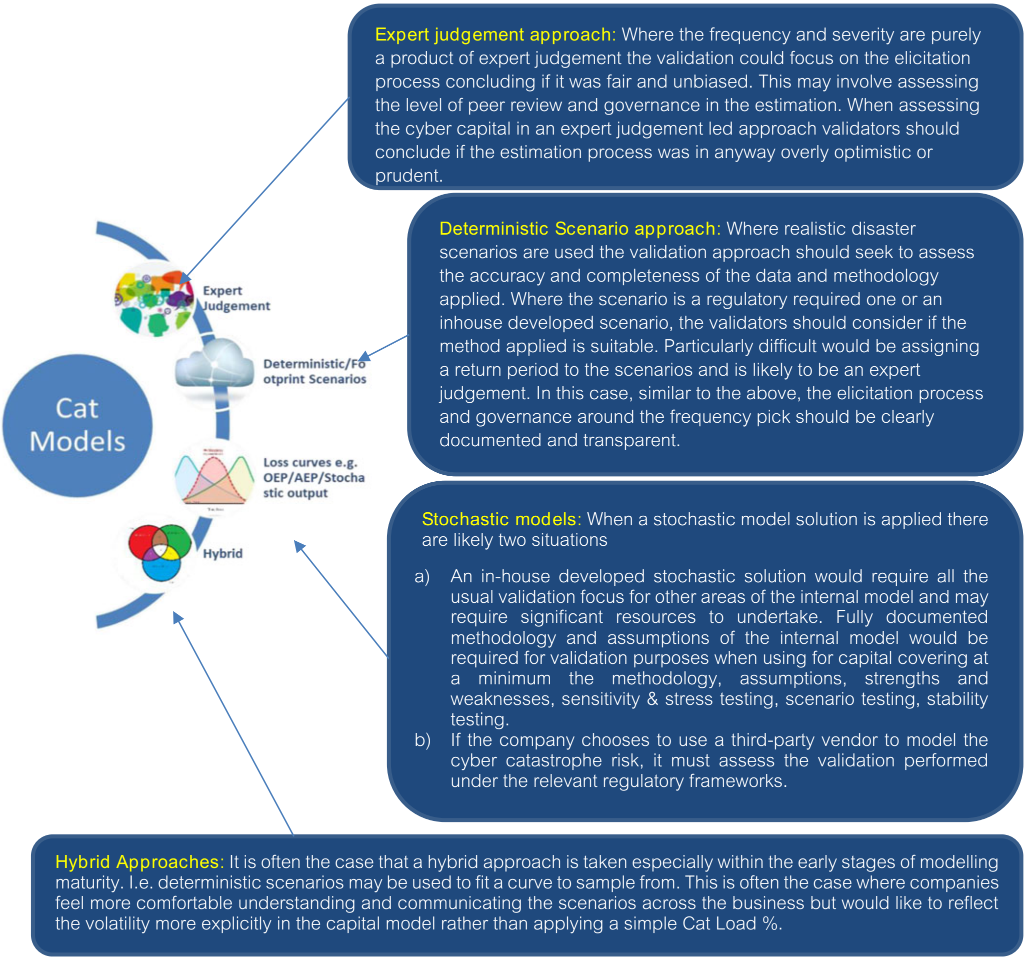
- How has the claims frequency and or severity changed over time?
- Have the cyber coverages offered changed?
- Has the companies risk appetite/strategy changed?
- Does the parametrisation process include an implicit/explicit cat load?
- How does the current threat actor and/or threat vector landscape 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?

Benchmarking or alternative assumption tests should also be considered by the validation team when assessing the parametrisation of premium and reserve risk. Market data such as the Lloyd's Market Association (LMA) data can be a useful tool to assess the cyber portfolio performance and tests alternative assumptions.

Catastrophe

The most challenging aspect of Cyber Risk is estimating the catastrophe risk element. Given that at the time of writing there were no true cyber catastrophic events to leverage from therefore makes the estimation of cat losses currently a theoretical exercise. This makes the validation of the catastrophe risk element of Cyber more challenging however not an unfamiliar concept for capital models. The level of cyber cat models across the market will vary significantly in complexity dependent on resources and materiality to the company. But regardless of what modelling approach is used the most important area to validate is how the return periods along the cyber cat curve are parameterised. Figure 5 summarises the key considerations for Cyber Catastrophe modelling validation.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press


Cat Models
Expert Judgement
Deterministic/Fo otprint Scenarios
Loss curves e.g. OEP/AEP/Stocha stic output
Hybrid

Expert judgement approach: Where the frequency and severity are purely a product of expert judgement the validation could focus on the elicitation process concluding if it was fair and unbiased. This may involve assessing the level of peer review and governance in the estimation. When assessing the cyber capital in an expert judgement led approach validators should conclude if the estimation process was in anyway overly optimistic or prudent.

Deterministic Scenario approach: Where realistic disaster scenarios are used the validation approach should seek to assess the accuracy and completeness of the data and methodology applied. Where the scenario is a regulatory required one or an inhouse developed scenario, the validators should consider if the method applied is suitable. Particularly difficult would be assigning a return period to the scenarios and is likely to be an expert judgement. In this case, similar to the above, the elicitation process and governance around the frequency pick should be clearly documented and transparent.

Stochastic models: When a stochastic model solution is applied there are likely two situations

a) An in-house developed stochastic solution would require all the usual validation focus for other areas of the internal model and may require significant resources to undertake. Fully documented methodology and assumptions of the internal model would be required for validation purposes when using for capital covering at a minimum the methodology, assumptions, strengths and weaknesses, sensitivity & stress testing, scenario testing, stability testing.
b) If the company chooses to use a third-party vendor to model the cyber catastrophe risk, it must assess the validation performed under the relevant regulatory frameworks.

Hybrid Approaches: It is often the case that a hybrid approach is taken especially within the early stages of modelling maturity. I.e. deterministic scenarios may be used to fit a curve to sample from. This is often the case where companies feel more comfortable understanding and communicating the scenarios across the business but would like to reflect the volatility more explicitly in the capital model rather than applying a simple Cat Load %.

Figure 5. Different approaches for validating catastrophe risk.

4.4. External Model Validation

External model vendor natural catastrophe models are well established following many decades of development. They are accepted across the market as effective ways to understand the risk posed from various perils, and the use of the models for capital purposes is fully embedded in the validation process given its materiality to many (re)insurance companies. Cyber models however are just at the start of this journey and continue to develop at a fast pace. The priority question for the validation to answer if the company is allocating capital with an external model should be "is the model aligned to our view of the risk".

Validation approaches should follow the example set by the validation of natural catastrophe models across the market and apply a similar framework in assessing the model's suitability and capital allocation. The Lloyd's External Model Framework provides a useful example for natural catastrophe perils to follow (Lloyd's of London, 2021a).

Demonstrate understanding of the model

The company should demonstrate that they have a good understanding of the modelling approach applied by the vendor and can articulate this. Some of the key topics to cover in demonstrating the understanding of the model involve the following:

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

- **Strengths and weaknesses** – The validation should acknowledge the strengths and weaknesses of the cyber models. Cyber modelling is evolving quickly, and hence, this may need to be regularly reviewed as part of the validation process. The vendor models currently have different philosophies for modelling Cyber Risk, and demonstrating that this is aligned to the company's view is crucial. Currently, a company may identify that the data augmentation process of a vendor model may have both strengths and weaknesses in its ability to model the risk. Similarly, the modelling methodology choice may be seen either as a strength or weakness by the company depending on their own view. For example, some vendors are striving for a detailed ground-up approach to estimating cat losses, whereas others are relying on a market share approach whilst data quality is improving.
- **Model parameters** – Having demonstrated understanding of the model usually the model will allow for various parameter selections. One such selection may be the severity of loss assumptions of certain cyber scenarios or the way in which the model handles missing data in the augmentation process. The company must acknowledge and assess the sensitivity of these assumptions to the model output.
- **Model output adjustments** – Ultimately, once the company has understood the model and made parameter selections, it must conclude on how comfortable it is with the model output. Depending on the company's assessment of the model, it should be clearly demonstrated what/if any adjustments are made so that the output reflects the company's view of the risk. Consideration should also be given as to how the output is to be incorporated in the model. Should the vendor model prepare a full ELT or YLT output? It is important to be clear to that the output is fully understood and used accurately by the capital mode. For example:
  - Is the ELT provided across all scenario/event types or just by scenario/coverage?
  - Does the ELT/YLT include cyber attritional/large loss as well as cyber cat losses?
  - Does the vendor model include a correlation structure between different cyber scenarios?
  - For cyber, it is unlikely there is any seasonality in the earning of the risk; hence, does the internal model reflect this?
- **Vendor validation** – Further work on assessing the quality and depth of the vendor validation should be performed across both quantitative and qualitative areas. Cyber data is sparse, and threat actor/vector assumptions can be very subjective relying heavily on expert judgements. The company should validate the vendor's approach in landing on the assumptions in the model and if they align with their own view.

Demonstrate model suitability to the portfolio

A very important part of any external model validation requires the business to provide an argument as to why the selected model is suitable for their portfolio. Given that cyber vendors currently have varying approaches to modelling each cyber scenario the business should consider first what are the material exposures in their portfolio. For example, are they mostly at risk of a cloud outage event or a ransomware campaign? This assessment will help in understanding how well the vendor model reflects the risk in the portfolio. The model outputs by vendor currently vary significantly, and hence, the capital required for the risk would be materially impacted by vendor model choice.

For some companies it may be that a multi model approach is required to approximately reflect the risk in their portfolios that meets their own view of the risk. This may be a combination of the vendor models as well as in-house models. Figure 6 highlights an example of validation testing performed across three vendors.

The results below show that each vendor has a different view of the risk and what drives the losses at the mean and the tail. It is crucial that companies can demonstrate that they have understood and aligned the vendor's view of risk to their own. This may mean making adjustments to the parameters and/or scenarios in the external model or output adjustments. Without their articulation and justification of the output, the company cannot demonstrate they

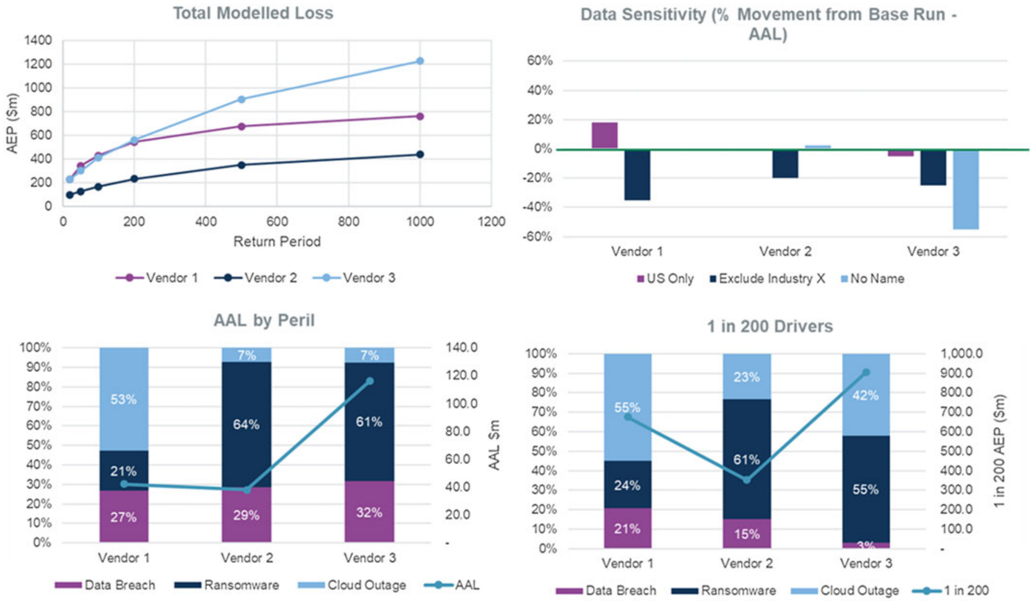


Figure 6. Example illustrations for validation testing.

understand the modelled risk output, and it is consequential impact on the capital. Furthermore, it's worth noting that when performing sensitivity tests, the models may also behave differently to the stresses which should further inform and support decisions on how to adapt external models into the internal model.

Independent validation

In addition to the model assessment, companies should still be performing independent validation to review a specific component of the model. For example:

- **Backtesting** simply involves testing the vendor model against historical data. In this case, testing the cyber model against recent major events such as NotPetya or SolarWinds may help to understand the suitability of the model to the portfolio. However, given the immaturity and lack of "real" cyber catastrophe event, the amount and quality of analysis here are limited, and the validation should not place too much reliance on backtesting to assess the model's ability to predict cyber cat losses. It can be debated that for cyber catastrophes that the forward-looking risk may never be a good fit for historical events given how quickly threat actors and evolve and change to exploit new weaknesses. Furthermore, the regulatory/legal environment changes in regard to cyber claims payments much also be carefully considered when backtesting.
- **Comparison to industry estimates** can be used to assess how the model output compares the market view of the risk. A suitable cyber comparison may not be easily found; however currently, sources such as Property Claim Services (PCS) have started developing market loss databases.
- **Sensitivity and stress testing** are perhaps one of the most crucial areas of cyber cat model validation currently. These tests should help to understand where the key assumptions reside. Companies may also choose to test the data augmentation process in some cyber models to understand the impact on capital and determine the importance of its own data collection at the time of underwriting.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

- **Stability testing** is an important area for any external model and understanding the convergence of the standalone capital at risk in the internal model should be no different from any other external model exercise.

4.5. Validation by Risk Type

In addition to the validation of cyber as a line of business, we need to consider the impact on other areas of the internal model. The validation should also assess how the risk has been modelled across the risk profile of the business in terms of

(a) Cyber losses and the correlation to other risk types, for example, RI credit.
(b) Cyber as a peril and its potential impact to other risk types, for example, market risk.

This is likely to be a challenging area of the internal model parametrisation and validation given how mature is the markets' understanding of Cyber Risk. Nonetheless, validation can be a useful tool in highlighting and challenging the business on its approach and understanding of the risk.

- **Operational risk:** Validators should consider whether Cyber Risk is modelled as part of an operational event for the business. All companies, to some degree, are exposed to this risk in the modern world, and hence, it cannot be ignored in the operational risk model. Validators should assess if the model explicitly allows for cyber operational events either malicious or non-malicious in nature within its outputs. The risk may be explicitly considered as part of scenario modelling or considered within an aggregate operational loss curve. Either way, this should be recognised and concluded as to whether the risk is adequately covered by the approach.
- **Market risk:** Cyber has the potential of causing global and local economic shocks with a precedent already set by the Swift attack. The risk that a cyberattack either directly or as a consequence of a major global outage causes market turmoil should not be ignored and the validation exercise should consider if appropriate consideration to this risk has been made. Many companies may consider this event beyond the 1 in 200; however, the Covid-19 pandemic illustrates how unforeseen events can have severe economic impacts.
- **RI credit:** Similar to natural catastrophe risk, cyber catastrophes have the potential to cause reinsurer default in extreme cases. Validators should assess if the cyber cat losses are well reflected by the RI default module.
- **Non-RI credit:** As with RI credit, cyber catastrophe (or even potentially large) losses may result in some non-RI credit defaults particularly in relation to broker and/or claims payments.
- **Dependency structure:** Perhaps one of the most challenging areas to parameterise with Cyber Risk is the interdependency of cyber as a peril across the company's risk profile. Truly catastrophic cyber events have the potential of impacting every risk type and being a serious threat to the company's viability. Validators should assess if the dependency of cyber as a peril across the business is aligned with the companies' view of the risk. The reverse stress tests may be the most suitable way to assess this area of the model.

4.6. Conclusion

The validation exercise cannot conclude that the chosen modelling approach is perfect and without limitation. The overall aim should be to be transparent on the strengths and limitations of the modelling. The risk evolves quickly, and modelling this risk poses a new challenge to the

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

industry; hence demonstrating how the company intends to manage with the known and any unknown certainties should be concluded in the validation. Validation should always focus on being “value-add”, therefore should seek to challenge and strengthen the key uncertainties in the modelling and ultimately conclude whether the allocated capital is adequate to support the risks, given the known uncertainties and limitations.

5. Embedding Cyber Risk Modelling into ERM Frameworks

5.1. Cyber Dynamic Feedback Loop

The role of the ERM framework in managing Cyber Risk should help to enable management to gain confidence that the risk is being actively and effectively managed. Promoting and embedding a strong risk culture is essential and one which consciously includes Cyber Risk is now critical as it not only impacts insurance risk but also other risk areas across the business.

Below (Figure 7) is an example of how Cyber Risk could be considered in the traditional ERM feedback cycle (American Academy of Actuaries, 2013). Ultimately, it is important to consider how embedded the capital team is in the whole process to understand if adequate and appropriate capital has been allocated for the risk. Does the capital team have an embedded process to engage with the underwriters, pricing, exposure management and reinsurance teams on a regular basis so that all teams are aware of the relevant evolution of the risk affecting their own disciplines? Furthermore, risk and reinsurance should also play a role in the process to provide challenge and oversight as well as considering if the wider Cyber Risk impacts are being reflected in the capital model, for example, operational risk. This should also not just be at the time of annual parameterisation updates for cyber (whether affirmative or non-affirmative). The potential for losses can be of a scale to cause serious damage to companies so the key aspect is to “connect the dots” between different business touchpoints. Hence a more dynamic feedback cycle would help pro-actively manage the risk and understand any capital implications from the changing risk landscape.

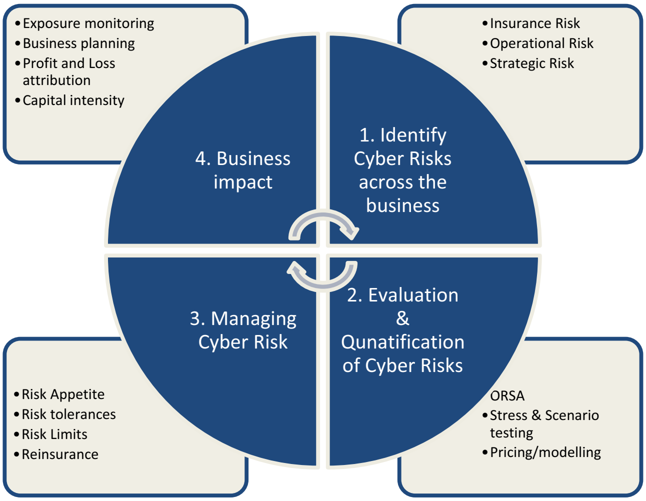


Figure 7. An example feedback cycle.

5.2. Identify Cyber Risks across the Business

In order to embed Cyber Risk into the company ERM framework, it must be first defined and understood. The scope of the potential impacts and losses should not be confined to known losses or recent experience but should consider the broader potential for emerging threats to the

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

business. These could be both malicious and non-malicious in nature. The company should seek to form its own view of the impacts across all areas of the business, for example:

- Insurance risk: Losses impacting both cyber products underwritten and the potential losses arising from cyber as a peril on noncyber policies.
- Operational risk: Potential for cyber incidents to impact the company such as ransomware attacks or data breaches.
- Strategic risk: Risk that Cyber Risk landscape makes achieving the company strategy more difficult or not possible.
- Reputation risk: Risk that, as a result of some cyber incident, the reputation of the business is severely impacted.

Crucially this stage of the framework in respect of cyber should aim to be comprehensive and cover all material and emerging Cyber Risks to the business. To produce this output, workshops with relevant stakeholders will be required, whereby companies may seek out cyber security expertise either internally or externally to provide technical insight and bridge the information asymmetry gap that can arise when trying to understand Cyber Risks. Crucially cyber security experts may be able to educate the company on what are the material risks and probable risks. This process should be continuous and regularly considered if the risk profile has changed.

5.3. Evaluation and Quantification of Cyber Risks

The evaluation of the Cyber Risks to the business can take a variety of forms. For insurers writing cyber policies, one of the most important areas will be in the pricing team. However, quantification of loss potential should involve reserving, exposure management, cyber security experts, claims teams and possibly also legal to understand the clause environment. Modelling of Cyber Risk is developing and maturing; hence various methodologies and approaches exist.

Stress and scenario testing is likely to be a key tool to help companies understand Cyber Risks in the first instance and then building on these to develop more complex stochastic models and help inform the capital requirement for the risk. The capital models will need to leverage from the work performed by pricing actuaries and accumulation management to model the tail risk. However capital teams will also need to leverage expertise across the business to assess dependency between other risk areas particularly operational risk.

Within the ERM framework, the quantification approaches for Cyber Risk will need a regular review of appropriateness of both the modelling methodology and parameterisation. Given the rapid change in the threat and security landscape, the risk requires constant review both on identification and also in regard to modelling approaches. It may be that blended model approaches are required to capture the full scope of the risk identified.

5.4. Managing Cyber Risks

An effective ERM framework will leverage from the quantification approaches and develop effective management of the risk to the company by embedding the following:

- **Risk appetite statement** outlining the specific risk that the company has chosen to expose itself to, such as underwriting only certain types of companies with a certain cyber security score, etc. This will need ongoing monitoring and a defined cyber data standard to adequately monitor and report. In addition, companies should seek to define the level of Cyber Risk they are prepared to accept, not just within insurance risk but more broadly across the business such as in operational risk. This may also define certain risk areas to avoid those that are deemed as high-profile cyber targets for criminals.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

- **Risk tolerances and risk limits** that define the overall aggregate Cyber Risk that the company is prepared to accept that are monitored against exposure management modelling approaches of tail events.
- **Reinsurance** will play an important role in managing the overall exposure to Cyber Risk. Furthermore, the company may also need to purchase its own cyber cover to cover operational incidents.
- **Cyber risk metrics** may be developed to produce early warning risk indicators to management of either insurance or operational Cyber Risks that may be merging so that pro-active action can be taken to mitigate the impact. This may lead to defining triggers for model re-parametrisation for the pricing and capital model for cyber. This triggering of re-parameterisation needs to be more sophisticated for cyber than perhaps other classes of business as the cyber landscape moves so dramatically and quickly. For example:
    - RDS increases by a specific risk tolerance triggers capital review.
    - Increase in threat landscape metrics triggers a review of pricing parameters for ransomware risk.
    - Increase in a specific industry or peak exposures above a threshold triggers review of reinsurance appropriateness.

5.5. Business Impact

As the company evaluates the risk and monitors its exposure to the risk against its tolerances and metrics, an evaluation of the business impact needs to be made such as the impact on the profit or loss of the business. The profitability combined with exposure metrics risk monitoring should then inform the next business/strategy planning of the risk.

Geo-political and macro-economic factors may also impact the company's evolving view of Cyber Risk and the decision on strategy. For example, increased tensions between nation states may lead to more cyber-criminal activity which may result in a threat landscape that is beyond the risk appetite of a company to write insurance.

5.6. Conclusions

Ultimately following the quantification and monitoring of the risk the impact the risk has on capital consumption needs to be reviewed and fed back to the stakeholders in the ERM framework process. The return on capital for Cyber Risk will be an important metric for companies to consider when developing their approaches. It should be compared to their expert management view at the board level to determine if the return on capital derived for the risk is in line with expectations and if not, can it be reasonably communicated and justified.

The development of the modelling and monitoring of the risk could result in return on capital that looks favourable because the modelling approaches are simplistic and inadequate; hence more development may be required. Conversely it may be that the approaches receive heavy investment and ultimately produce return on capital metrics that are not in line with expectations but can be justified through the modelling.

Communication of the modelling approaches and what this means for capital is crucial and requires regular review whilst the risk continues to evolve and mature.

Acknowledgements. The authors would also like to thank the general Cyber Risk Working Party for their contributions to discussions in wider roundtable and, in particular, to Matthew Silley, for his contribution to scoping the content of the paper. The authors would also like to thank Mairi Russell for her contribution in finalising this paper.

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

References

American Academy of Actuaries (2013). Insurance Enterprise Risk Management Practises, available at https://www.actuary.org/sites/default/files/files/ERM_%20Practice_Note_July_2013_0.pdf (accessed 5 November 2021).

ASTIN (2013). *Making Use of Internal Capital Models*, available at https://www.actuaries.org/ASTIN/Colloquia/Hague/Papers/Krvavych.pdf (accessed 20 January 2022).

Bank of England PRA (2019). *Cyber Underwriting Risk: Follow-Up Survey Results*, available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results (accessed 10 January 2021).

Bloomberg (2019). Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?, available at https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (accessed 1 January 2022).

Bloomberg (2021) Hackers Breached Colonial Pipeline Using Compromised Password, available at https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg (accessed 1 January 2022).

Bloomberg Law (2022) *Merck's $1.4 Billion Insurance Win Splits Cyber from 'Act of War'*, available at https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war (accessed 22 June 2022).

Britt, S., & Krvavych, Y. (2009) *Reinsurance Credit Risk Modelling – DFA Approach*, available at https://www.actuaries.org/ASTIN/Colloquia/Helsinki/Papers/S5_16_Britt_Krvavych.pdf (accessed 11 November 2021).

Cartagena, S., & Grewal, J. (2021). The silent treatment. *The Actuary Magazine*, available at https://www.theactuary.com/2020/04/14/silent-treatment (accessed 30 September 2021).

Chan, K., & Ramyar, M. (2016). *Practical Challenges in Reserve Risk*, available at https://www.actuaries.org.uk/system/files/field/document/Chan%2C%20Ramyar%20%282016%29%20-%20Practical%20Challenges%20in%20Reserve%20Risk.pdf (accessed 31 December 2021).

Cyrence (2021). Guidewire, available at https://www.guidewire.com/products/cyence/ (accessed 31 December 2021).

Fitch Ratings (2021). *Fitch Ratings Analyzes Global Insurers Cyber Risk*, available at https://www.fitchratings.com/research/insurance/fitch-ratings-analyzes-global-insurers-cyber-risk-14-10-2021 (accessed 31 December 2021).

Fitch Ratings (2022). *Exploring Bank Cybersecurity Risk – FAQS*, available at https://assets.ctfassets.net/03fbs7oah13w/5eEcUG918sIq4O2mvTwcPg/d7c7258821bb4b23910ff4950f76d721/Fitch_Ratings_Exploring_Bank_Cybersecurity_Risk_-_FAQS.pdf (accessed 22 June 2022).

Hossack, I. B., Pollard, J. H., & Zehnwirth, B. (2003). *Introductory Statistics with Applications in General Insurance*. Cambridge: University Press.

Institute and Faculty of Actuaries' Capital Allocation Working Group (1999). *Preliminary Report of the Capital Allocation Working Group*, available at https://www.actuaries.org.uk/system/files/documents/pdf/capitalall.pdf (accessed 5 November 2021).

Institute and Faculty of Actuaries' Cyber Risk Working Party (2018). *Cyber Operational Risk Scenarios for Insurance Companies*, available at https://www.actuaries.org.uk/system/files/field/document/Sessional%20paper%20-%20Cyber%20operational%20risk%20scenarios%20for%20insurance%20companies_0.pdf (accessed 1 January 2022).

Institute and Faculty of Actuaries' Cyber Risk Working Party (2021). *Silent Cyber Assessment Framework*, available at https://www.actuaries.org.uk/system/files/field/document/FINAL%20Sessional%20paper%20-%20Silent%20Cyber%20Assessment%20Framework_0.pdf (accessed 1 January 2022).

Institute and Faculty of Actuaries' Operational Risk Working Party (2016) *Good Practice Guide to Setting Inputs for Operational Risk Models*, available at https://www.actuaries.org.uk/system/files/field/document/FINAL%20PAPER%20FOR%20WEBSITE.pdf (accessed 1 October 2021).

Ismail, N. & Jemain, A. A. (2007). Handling Overdispersion with Negative Binomial and Generalized Poisson Regression Models. *Casact.org*, available at https://www.casact.org/sites/default/files/database/forum_07wforum_07w109.pdf (accessed 1 January 2022).

Kopp, E., Kaffenberger, L. & Wilson, C. (2017). *Cyber Risk, Market Failures and Financial Stability*, available at https://www.imf.org/-/media/Files/Publications/WP/2017/wp17185.ashx (accessed 22 June 2022).

Li, J., Zhu, X., Lee, C. F. et al. (2015). On the aggregation of credit, market and operational risks. *Review of Quantitative Finance and Accounting, [e-journal]* **44**, 161–189, available at https://doi.org/10.1007/s11156-013-0426-0 (accessed 23 June 2022).

Lloyd's of London (2021a). *External Catastrophe Model Validation Illustrative Validation Document No. 1 US Windstorm, High Materiality*, available at https://assets.lloyds.com/assets/pdf-model-validation-validation-of-external-catmodels-illustrative-example-for-us-windstorm/1/pdf-model-validation-Validation-of-External-CatModels-illustrative-example-for-US-Windstorm.pdf (accessed 5 November 2021).

Lloyd's of London (2021b). *Realistic Disaster Scenarios (RDS)*, available at https://www.lloyds.com/conducting-business/underwriting/realistic-disaster-scenarios (accessed 31 December 2021).

Paddam, P. (2001) *A Short Introduction to Extreme Value Theory*, available at https://www.actuaries.org.uk/system/files/documents/pdf/paddam.pdf (accessed 20 January 2022).

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press

Shaw, R. A., Smith, A. D. & Spivak, G. S. (2010). *Measurement and Modelling of Dependencies in Economic Capital – A Discussion Paper*, available at https://www.actuaries.org.uk/system/files/documents/pdf/sm20100510.pdf (accessed 23 June 2022).

Reuters, 2018, *Capital One to Pay $80 Million Fine after Data Breach*, available at https://www.reuters.com/article/us-usa-banks-capital-one-fin-idUSKCN2522DA (accessed 1 January 2022).

Security Scorecard (2021). *Cyber Insurance & Security Ratings*, available at https://securityscorecard.com/resources/cyber-insurance-security-ratings (accessed 31 December 2021).

Sophos (2022). *The State of Ransomware 2022*, available at https://www.sophos.com/en-us/content/state-of-ransomware (accessed 1 November 2022).

Venter, G., et al. (2003). *A Survey of Capital Allocation Methods with Commentary*, available at https://www.actuaries.org/ASTIN/Colloquia/Berlin/Venter2.pdf (accessed 6 January 2022).

Willis Towers Watson (2021). *Cyber Quantified*, available at https://www.wtwco.com/en-BM/Solutions/products/cyber-quantified (accessed 31 December 2021).

Cite this article: Grewal J and Cartagena S. (2024). Cyber risk within capital models. *British Actuarial Journal*. https://doi.org/10.1017/S1357321724000114

https://doi.org/10.1017/S1357321724000114 Published online by Cambridge University Press