British Actuarial Journal (2025), Vol. **30**, e12, pp. 1–12
doi:10.1017/S1357321724000230

Institute and Faculty of Actuaries

SESSIONAL MEETING DISCUSSION

Cyber risk capital

[Institute and Faculty of Actuaries, Sessional Webinar, Tuesday 14 November 2023]

Moderator (Mr P. D. G. Tompkins, F.I.A.): Welcome to this meeting on the work of the Cyber Risk Working Party paper. I am Peter Tompkins. I am a member of Council and the Risk Management Board. This is the third paper based on some major work done by the Cyber Risk Working Party over the last few years.

Simon Cartagena is a chief risk officer of Cincinnati Global Underwriting. He has worked in a variety of actuarial roles specialising in risk and capital, with an interest in cyber risk, and is involved with the Cyber Risk Working Party. He is currently a member of the IFOA's Risk Management Board.

Jasvir Grewalis is Head of Data and Analytics at the Global Facultative Broking Department of Willis Towers Watson. She has had a wide range of roles in this area and has also been a member of a number of working parties and of the Risk Management Board.

Mr S. T. Cartagena, F.I.A.: This paper was released earlier this year. Given that cyber risk is a growing area, the capital element of cyber risk has not been given sufficient attention and certainly not as much attention as, say, areas like natural catastrophes.

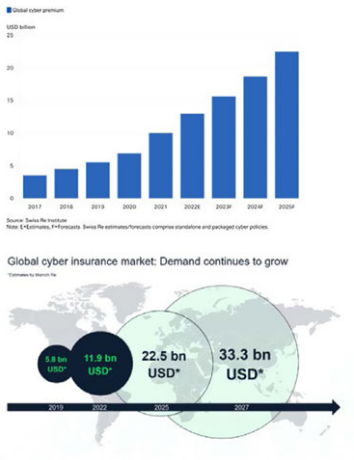
We use some definitions, that are common in cyber work, in this paper. "Affirmative" is the risk that you intend to write. "Non-affirmative" is the risk that occurs that you did not intend to write, that arises out of poor-quality wording or poor underwriting. Then, there is an operational cyber risk element that we will also cover.

For the purposes of this paper, we focused on Solvency II and the London market. But the work should apply to most other capital modelling approaches.

Figure 1 gives an overview of where Swiss Re and Munich Re see the cyber market going in the next few years. Most reinsurers and brokers are expecting cyber premiums to continue to grow, year after year. This is very heavily linked to the type of claims activity, or economic losses that companies experience. Capacity has been constrained in the last few years as companies have struggled to understand the risk, in particular the systemic element and how much capital might be required. This particularly affects reinsurers, who would ultimately pick up the really bad events. Munich Re is a very big player in this area and how they see the risk has potentially driven the market. But one interesting and positive development has been what Beasley did earlier this year, in terms of the first major insurance linked security (ILS) in this area, with the Cyber Catastrophe Bond bringing in alternative capacity into that market. So, that shows things are moving on and potentially confidence is growing.

In terms of capital and why it is uncertain, these are the main factors:

- Threat actors and threat vectors are constantly evolving, which makes it very challenging and unlike any other risk that we underwrite in general insurance. A one-year view of risk could look dramatically different.
- War is a huge element of cyber risk and recent wars have led to new weaponising of cyber approaches. At the moment that may still be confined to warring states, but eventually that



- According to Swiss Re, cybercrime is expected to cost $8 trillion in 2023.
- Both Swiss Re and Munich Re expect cyber premiums to grow significantly over the next 5 years.
- Cybersecurity Ventures, predicts that global cybercrime damage costs will grow by 15 percent per year in the near term, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015.
- Capacity in the cyber market has been cautious given the uncertainty, however more (re)insurers appear to be gaining greater comfort on the risks and entering the market/increasing capacity.
- 2023 saw Beazley securing a USD 45 million in reinsurance coverage through the industry's first dedicated and tradeable cyber catastrophe bond

Figure 1. Market outlook.

could spill out in a material way into the corporate and company market when there is no longer a war effort going on.

- Wording is a constant area of uncertainty. The Lloyd's Market Association (LMA) has done a lot to try and close that gap, so we are in a much better place now than we were two to three years ago, but there is still an issue.
- Cyberterrorism or cybercrime is a man-made peril and that makes it inherently difficult to model and understand.
- Technology is constantly evolving, which is what really enables threat actors and threat vectors and increases the underwriting risk element. It is difficult to move at the same pace as technology change and the rate at which cyber criminals are carrying out attacks. This is because your view of risk may be accurate, or at least as accurate as it can be. But a few months later it could have dramatically changed due to some zero-day vulnerability or ability of the threat actors to carry out something new and unknown. "Zero-day vulnerability" refers to a key vulnerability in a system or software that allows attackers to exploit it. "Zero-day" refers to the fact that the vulnerability is not yet known by the security teams and therefore remains exploitable by criminals.
- Capacity drives a lot of the uncertainty.

[At this point in the presentation, Mr Cartagena played and discussed a short video about the evolution of the threat landscape (Figure 2) and ransomware attacks. The video link is available at: https://youtu.be/L4Ti8H4y_YM].

There is an inflection point around 2019 where activity is quite low. But after that, it suddenly increases from about 500 million ransomware cost to about 3 trillion in the space of three years. Calibrating models using a view of risk based on 2019 and prior years would therefore be inappropriate. Now, I do not think this is necessarily a risk that we are used to assessing, especially when we are thinking about capital. With natural catastrophe (NatCat) risk we have a lot of history and a lot of ways to view that risk, and the risk landscape does not change quite so dramatically. The statistics show that ransomware is constantly evolving and growing as a threat.

There are quite a lot of other aspects to consider. For example, an outage of the cloud is potentially a huge systemic, catastrophic event. It clearly shows that the risk is getting bigger. But that does not mean it is necessarily uninsurable, it just means that the threat landscape is constantly evolving and changing.

The diagrams in Figure 3 show the areas of supply chain attacks that are also very difficult to understand, because attacking something in a supply chain has knock-on consequences to

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

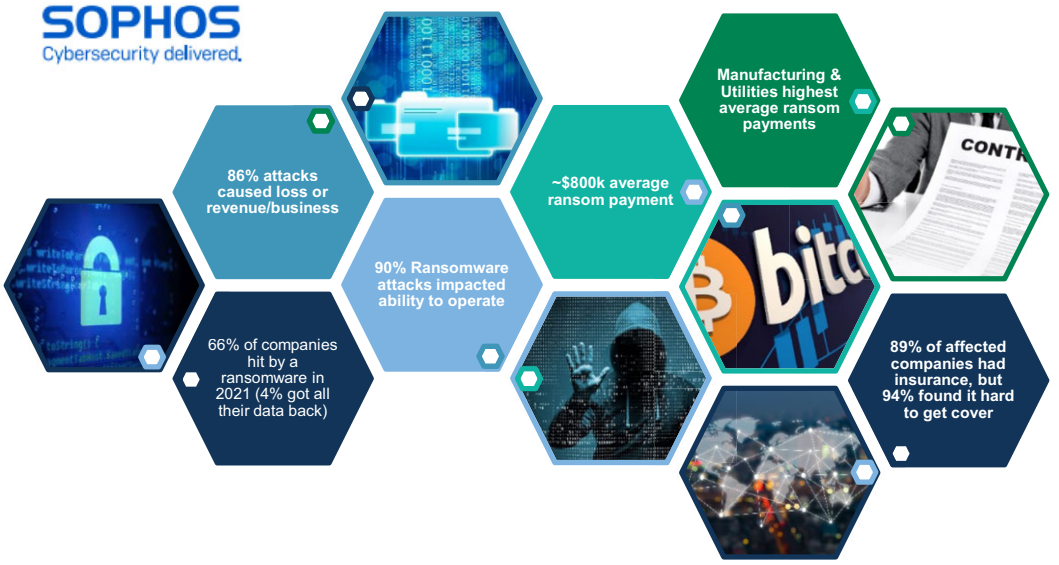


Figure 2. Sophos cyber security report: The state of ransomware 2022 findings.

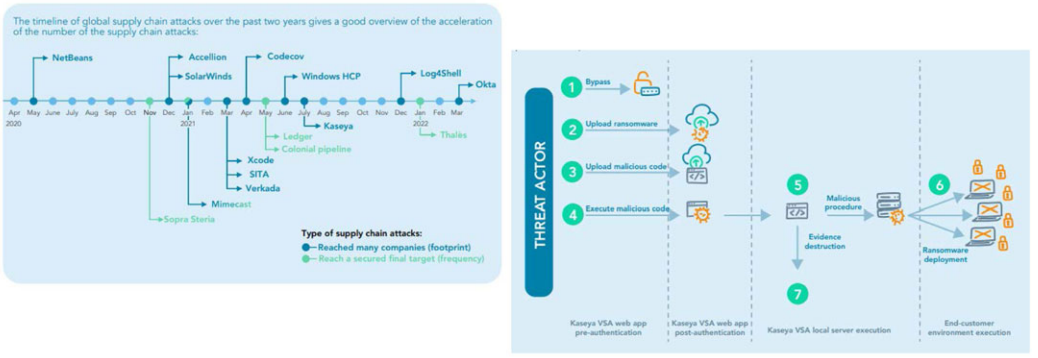


Figure 3. Supply chain attacks.

multiple companies. So, there is a single point of failure that could be crucial in understanding how cyber-attacks and cyber losses can occur on a mass scale.

The war in Ukraine has already led to new and different type of attacks being weaponised. I attended a really interesting talk explaining the types of attacks on the right of Figure 4. Some of them particularly scared me because they were new and evolving. They were potentially developed as part of a war effort but had not really been deployed because all of the relevant resources were being focused on causing disruption for the war. When the war eventually ends and those resources may start to be freed up, that could again dramatically change the risk landscape.

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

War in Ukraine

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

Weapons Developments

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

Figure 4. 2022/3 developments.

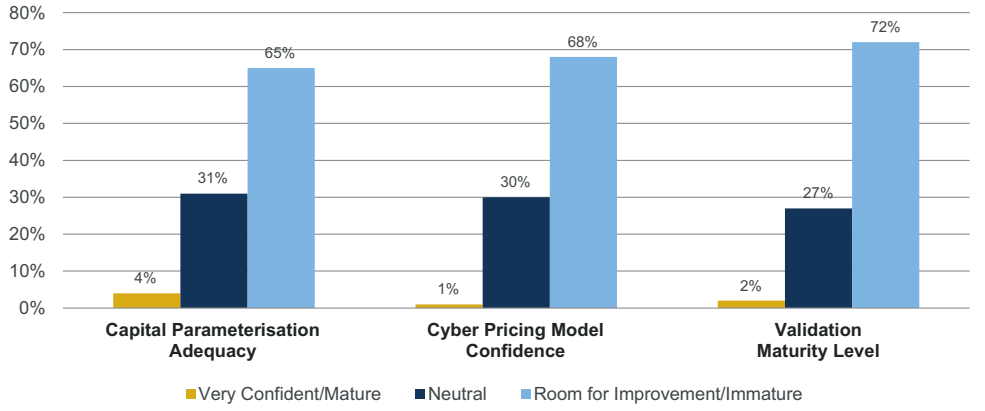


Figure 5. GIRO November 2022 audience poll results.

Miss J. K. Grewal, F.I.A.: In the first part, Simon (Cartagena) set the scene with regards to the cyber risk landscape. We are now going to move on to look at the capital considerations when it comes to cyber risk. The topics we cover could help you to reflect on the current sophistication and adequacy of cyber capital modeling processes. In general, we expect that some of the larger carriers of risk will have more sophisticated processes when it comes to cyber and capital. Then, of course, there will also be the smaller carriers who have smaller exposures to cyber risk and perhaps less sophisticated processes.

Cyber risk is an ever-evolving risk, and it is very dynamic, and that is one of the key characteristics. There are elements that are emerging, but it is no longer a truly emerging risk like it was a few years ago and we probably have not increased sophistication in our processes as much as we should have done, given the fact that this has been on our radar now for a quite a few years.

For this paper, the working party did three roundtables to give us a good sample size and a flavour of what is happening in the current market when it comes to cyber risk parameterisation processes. When we presented our work at GIRO in November 2022, we took the opportunity to do a quick poll of the audience. The results are presented in Figure 5.

We asked the audience three questions, garnering responses from between 50 and 80 people. The results were not surprising, but were interesting, and they emphasise the fact that we really do need to start paying attention to the level of uncertainty in cyber risk and how to quantify it to get better levels of comfort when it comes to dealing with that uncertainty.

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

The first question we asked, given the dynamic nature of cyber risk and the difficulties in setting capital, was about the level of confidence that the audience had when it comes to the adequacy of their capital parameterisation processes: "Are you very confident, are you neutral or is there room for improvement?" In Figure 5, we can see that the resounding answer was that there was room for improvement. Given our experience over the years with various markets, there is genuinely room for improvement in a lot of the cyber capital parameterisation processes.

The second question was on cyber risk pricing, where we asked "What is the level of model confidence?" Again, there were similar results, and it was deemed that there was room for improvement there as well.

Finally, we asked the question "What is the level of validation maturity that you deem to have in your frameworks?" From the responses it seemed that the validation maturity was very immature, and there is lots of room for improvement there.

This just gave a flavour of the level of cyber risk sophistication when it came to capital and pricing quantification, in general, and the associated validation. A similar survey today would most likely yield similar results.

When it comes to underwriting risk, one of the key factors is data and how there are data limitations specifically for cyber. There are market organisation bodies as well as market participants that are working to help with efforts in the areas of standardisation of cyber data, changing categorisations such as moving away from non-affirmative to affirmative cyber and unclear loss causation modes.

Now, I would argue that data for other lines of business can also be bad, but that does not stop us from augmenting that data and making our processes more robust. It is essential that we find a workaround to poor data in quantifying cyber risk, especially when it flows into capital models.

Practitioners tend to believe that only vendor models can help improve parameterisation for cyber risk. But there are other ways to increase sophistication that could prove cost effective even for smaller entities.

There are a number of organisations in the London insurance market that normally pick different distributions for attritional, large and CAT losses for property and will tend to take the same approach for cyber. That granularity does not always make sense for cyber. Property CAT losses such as a Japanese earthquake loss and a US hurricane loss are not comparable and do not fit in the same curve. Likewise, neither do ransomware and network outage. When we are looking at these different types of risk areas, we need to add that level of sophistication and granularity. Underwriting risk of course would be a first area of focus.

So, in summary, we need to consider whether we are adequately allowing for the extent of the changing cyber landscape within capital models. There have been a number of reports released over the last 12 months that echo these same sentiments. There was a Swiss Re research report released at the end of last year, which again echoed how cyber is ever evolving and questioned whether the quantification processes that we use to support that risk are developing sufficiently quickly (Swiss Re, 2022). At the start of 2023, there was a release by the Prudential Regulatory Authority (PRA) that stated that they had concerns about significant mis-estimation of scenario impacts on the cyber insurers. This again shows an inherent concern that there is a potential lack of sophistication and understanding of the potential size of cyber exposures and the risks with which they are associated (PRA, 2023).

Moving on from underwriting risk, the other key risk considerations are shown in Figure 6. More information on these considerations is given in the paper.

There are, of course, the different areas of cyber exposures that we need to allow for when we are looking for capital setting purposes, even though non-affirmative is now decreasing. We are not only looking at underwriting capital but there is also operational cyber as well. There are dependencies between these, and some of these have started featuring in capital models due to regulatory intervention that started a couple of years ago. But are we doing enough? An example to consider was during the COVID pandemic. With the prevalence of working from home, there is a

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

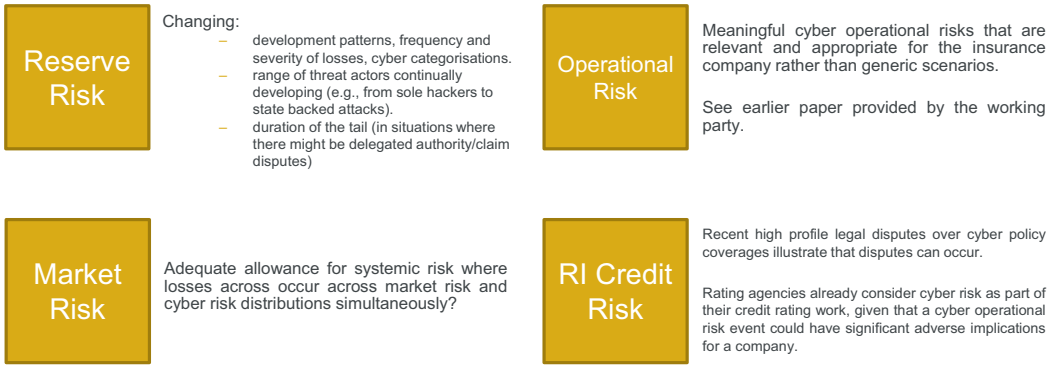


Figure 6. Other risks: Key considerations.

potential issue where lax underwriting processes trigger worse results from the underwriting risk component, but then there are also operational risks. There is a potential dependency there. Similarly, if there is a market downturn, the underlying companies that are being underwritten may not have enough money to spend on cyber resilience, and therefore we end up having correlation between market risk and underwriting risk. In 2022, there was concern that Lloyd's had been breached. Although it had not, hypothetically if a breach had occurred, that would not only have been an operational risk issue and a major event for Lloyd's but obviously also an issue for the carriers that operate within Lloyd's, and that would impact credit ratings. Credit rating agencies look at cyber-attacks and cyber resilience. An event of that scale would have impacted credit risk. These are examples of potential areas of dependency that we are not adequately allowing for in our capital models when it comes to cyber risk exposures.

In modelling dependencies there is the potential to tie different distributions to univariate variables. For example, the Clayton copula gives an asymmetric distribution with greater dependence in one tail versus the other tail. What I have noticed in terms of practice over the years is that picking distributions in the London market is an arbitrary process. The next step is to pick parameters for the copula.

These are assumptions, which will have material impacts on capital. So, ignoring the level of sophistication needed in parameterising the univariate distribution and choosing the copula will take away some sophistication when modelling dependencies, and that is if we assume we are allowing for enough dependencies to start off with.

Moving on to capital and capital allocation, there are lots of practical considerations and impacts to discuss, and there is a lot of subjectivity in the choice of method. Although it is out of scope, there are some relevant references in our paper. The key thing to highlight is the perception in the market that there is definitely too much capital being held for cyber. I am not sure I entirely agree with this, especially for some of the smaller players. What is interesting to note is the subjectivity in assessing the appropriate level of capital when it comes to cyber.

In the poll at GIRO, there was a question on the relative losses for a company from their NatCat exposures and their cyber exposures. It helps sharpen the focus of the level of subjectivity in our assumptions. It concerned FedEx, one of the largest delivery companies. Hurricane Harvey in 2017 was the costliest natural disaster to occur in that year and FedEx had losses from both Harvey and a cyber-attack. In a poll about what was the relative level of loss, only 7% of the audience got the right answer that FedEx had 40 times more loss from this cyber-attack than from its NatCat event. This just shows that if we are picking the underlying underwriting risk distributions, the dependency copulas and the copula parameters, all with subjectivity, our judgement may not be as good as we think it is, especially when it comes to cyber risk and tail events.

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

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

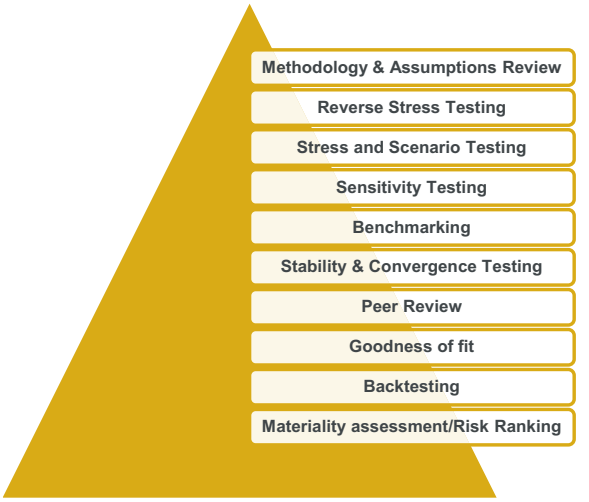


Figure 7. Validation focus.

Given all of this, when we are saying that there is too much capital being held for cyber, on what are we basing that statement?

Mr Cartagena: How do you even go about validating the amount of capital held and starting to get some kind of comfort when it comes to this very uncertain area that we perhaps do not fully understand? In capital and risk management, challenging the capital modelers on what they have done is an important role.

The pyramid in Figure 7 shows various validation tools/methods in order of usefulness. The methodology and assumptions review is ranked at the top in terms of usefulness for challenging the business on how they have set their assumptions and why they adopted a particular approach to modelling. Reverse stress testing is by far the most useful tool to test cyber assumptions within the business, and stress and scenario testing fall under testing at lower return periods and have been most informative.

Attritional and large loss deep dives fall into the methodology and assumptions reviews. It is probably important to do these more regularly than for other lines of business because of the changes in risk landscape. Catastrophe (CAT) risk validation is an inherently difficult area as currently we have not had any truly catastrophic events. There are some common approaches companies might be adopting for this, but whatever approach is chosen they have to own that risk and that is the part on which validation then focuses. For example, if an external model is used, the choice of vendor massively impacts what kind of capital you will ultimately be holding. None of the models are right, but none of them are wrong either. What matters is that you have formed and articulated how they fit your view of the risk. What is most important is why a particular model/ approach was chosen. Maybe the model picked is the one that gives the lowest capital? Maybe that is acceptable, provided there is also explanation of why that is acceptable and why that aligns to your risk view? It could be because that model has a better fit to the portfolio or to specific parts of the portfolio, for example a model for cloud outage is more suitable for your portfolio. What is needed is to articulate, rationalise, test and evidence your approach. It is not appropriate to just pick a model because, say, it is the most popular in the market, or because it gives you the lowest capital.

It is the same process for the CAT risk. The charts in Figure 8 are actual, real results from the three main CAT modelling firms and they show the relative differences between the ultimate capital requirements.

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

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

Figure 8. External cyber catastrophe models.

Operational risk is the most important "other" risk in validating the dependency or the link with cyber risk. There will be cyber risks on the risk register that need to be modelled and need to be reflected in operational risk, but the correlation between operational risk and cyber risk is potentially much larger, particularly in rating affirmative exposure, than for any other risk. So, if there is a major system CAT event, what is to say that you are not going to be impacted by the exact same event? For example, a major system CAT event that impacts 50% of your portfolio could also affect the business, in terms of ability to handle those claims and ultimately could cause additional stress to the business. It is difficult to assess whether, if a big insured event or underwriting risk event occurs, it is also expected to be an operational risk event. This is again where the reverse stress test (RST), a model validation tool, is very powerful. Again, for those in Lloyd's, there is also the impact of the market operational events to be considered.

Recognising cyber as an additional peril is also very important. Even if companies are not underwriting cyber risks, it does not mean they are excluded from them. We have called non affirmative cyber "cyber as a peril" in our paper and presentation. Even if you are not writing affirmative cyber, you could still have cyber events causing a loss on your portfolio. Hence, these events need to be given consideration even if it is only to say that we do not think the risk is material, and why this is the case.

The position about wordings for cyber has changed a lot in the past 12 to 18 months following an initiative from Lloyd's, and there is a lot more clarity. The choice of wording matters and may expose you to different types of risk and uncertainties, especially in the Lloyd's market and using the Lloyd's Market Association (LMA) wording. It cannot be assumed to totally eradicate silent or cyber exposure.

Moderator: Thank you, Simon (Cartagena) and Jasvir (Grewal). I am now going to ask Visesh Gosrani to come and make a first contribution to the discussion.

Mr V. Gosrani, F.I.A.: I would like to point out a few areas we have all been grappling with. We are all building our own capital models and parameterising them appropriately. But even before we do that, we often have challenges using external vendor models. The vendor models have varying levels of detail, and it requires a lot of engagement with vendors to obtain the detail that gives a full understanding of what is causing those models to produce their outputs. Ultimately, we need to be able to communicate internally to senior management as to why there is so much potential risk in those models. I would like to discuss the challenges that we have had in these areas.

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

Miss Grewal: One of the key issues I have found in the past was that vendor models were too much like "black boxes", when it came to validating and getting to a level of comfort with the results coming out of the model. One of the main issues was stability on refreshing quarter to quarter. There were cases when models would do things like saying that the cyber scenario has now increased by 100%. Although the issue of stability is now getting better, some of that is just due to filtering out the volatility from model users. Another issue has always been the transparency of the underlying assumptions and methodology. There are issues about vendor's IP, but if these models are truly going to embed into a Solvency II framework, we need sufficient transparency to know the assumptions that have been used in capital setting.

Mr Cartagena: I would concur with everything that was just said about vendor models. My experience has been very much the same. The vendors need to appreciate that model changes could materially drive the capital required for some companies. Some companies have very good diversification and so that issue does not impact them as much, but for other companies it could have a huge effect on the capital required. So, having the right level of governance around model changes from both sides is very important. We are mature in that respect for CAT risk but less so for cyber.

Producing cyber capital models is not a problem to be solved in isolation. Experts are needed in capital modelling and actuarial disciplines and in IT security. I have found that a major challenge when onboarding cyber capital models is having the right knowledge in the room to form an opinion as to whether or not they are appropriate for the business.

Moderator: You both described the fact that there are a variety of distributions with different looking tails, and a great deal of uncertainty about what the tails are going to look like in the future. Is there enough data to do goodness of fit statistics on different distributions? Do you have an analytical/mathematical way of justifying your choice of copula to management?

Mr Cartagena: This is a very personal opinion. Picking a distribution for modelling cyber is probably more difficult than for most other purposes. I think so much of the risk is forward-looking, and your data is potentially irrelevant. For example, for ransomware, your frequency assumptions, if based on 2020 or prior data, are just irrelevant. Using that data would have underestimated the capital massively. The challenge is to take a more forward-looking view and obtain data to give confidence around that view. The type of approaches that we use are probably not suitable, for instance fitting a log-normal distribution and simulating it 100,000 times. Much more complicated approaches are possible and probably would be used in Silicon Valley. These are approaches like neural networks, Bayesian frameworks or decision trees. The question then is whether the additional complexity is required. I do not think I know the answer yet, but what I do know is that assumptions need to be regularly reviewed and understood based not just on the data emerging but on what you think about the future of the risk.

Miss Grewal: I agree with everything that Simon (Cartagena) has said on the choice of distribution. For instance, using a log-normal, pareto or generalised pareto distribution does not really make a difference in the face of the level of uncertainty. There are so many levels of subjectivity. Rolling forward a set of assumptions that apply to a different class of business and waiting to see what happens in the actual market may not work for your exposure and your experience. We need a level of baseline thinking and then to update that thinking rather than use assumptions from other lines of business for cyber. Right now, we are confident about our lack of confidence when it comes to cyber rather than confident about the level of uncertainty in our figures, and the two are very different things. So, there is no right answer. Part of the role of those who work in capital modelling departments of insurers and reinsurers is to help inform the view of risk being taken by that company. There is no prescriptive answer to this issue. Cyber exposure will vary quite significantly depending on the online nature of the risk that is being taken, but we

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

do need to set our base assumptions and then refine them over time, rather than crudely applying approaches that are not fit for purpose when it comes to cyber risk.

Moderator: You mention in the paper that back-testing is hard to do, but have you seen examples of good back-testing happening?

Mr Cartagena: I have been doing back-testing at some companies, but it is hard to do. Back-testing may not be relevant in certain instances for a specific threat landscape and risk. Purely looking at the back-test would be ignoring the forward-looking view of risk, which could be dramatically different. I am of the school of thought around cyber risk that the forward-looking view of the risk is more valuable than the backwards-looking view. There is more to learn by thinking about what is happening. For example, looking at the dark web is probably a better indicator for your calibration than what happened three or four years ago.

Questioner: What I would say is more useful than back-testing is trying to look at some of the extreme percentiles and working out what is happening in these percentiles. We can then document the relevant underlying rationales, and these can be revisited in the future to test whether they still hold true and what we can learn from that.

Questioner: This is more of a big picture question. I suspect we are probably very early in thinking about what we are going to do to model cyber risk in capital models. Could you talk through the approaches you would take and why you would take them?

Miss Grewal: To answer the question I will make two points. One is just a follow-on to a point I made during the presentation. It is important to look at the correct level of sophistication and granularity even if you are using or looking at vendor models. Are you actually modelling only one general cyber curve? They may not be appropriate but this is done quite often in this industry unfortunately.

The next point is that no matter how big an entity you are, or how sophisticated your parametrisation processes already are, it is important to look at the dependencies. I touch upon this in much more detail in the paper itself. You can specifically force dependencies through triggering a scenario in capital models and allocating losses across different risk types. Think of the various risk types and understand that there could, realistically, not even in an extreme event, be dependency between those risks. If we recall the FedEx example, this shows how we could potentially underestimate the size of losses from an event. So, while thinking of scenarios and allocating losses, we need to make sure we adequately allow for the potential size of the loss.

Mr Cartagena: Materiality is key in this. When writing a small cyber portfolio, we need to achieve a tradeoff between resources and the capital allocated to this portfolio, given the capital may not be material to the entire business. If the sum of line sizes is less than a certain percentage of total capital, then we have to take that view. However, when starting to write significant amounts of premium and exposure, the natural question has to be whether the current method is an appropriate way to model that risk, especially if you are using a traditional approach. Would you be comfortable, should that result in you having to ask your capital provider to give you more capital because of underestimating the risk? In the worst case could it result in insolvency? Can we defend our current methods? For some companies the cyber issue is not material, and the approach used will not matter much at all. For other companies, it is going to matter materially and particularly for those companies that are using cyber as a diversification play. If they are writing equal amounts of property and equal amounts of cyber, what is the appropriate capital split? Are they assuming that the classes are totally independent so that they only need small amounts of capital to support that business? I would be concerned if some of the traditional

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

approaches to model risk are applied just like for like on cyber, especially while writing a large part of the market.

Moderator: We have got a comment here from the audience. We are essentially talking about the well-known limitations of quantitative models. We can improve the models by including qualitative or textual information, such as geopolitical data. But to do that we need different hybrid modelling techniques.

Questioner: Simon (Cartagena), you have put up some data for the growth of ransomware. How is this data sourced? A lot of this may be quite private, and there may be people who have been anxious not to see their exposure being revealed. What is the best approach to looking at the data and the evolving magnitude for potential risks, particularly when your own company or client's collection of data is quite limited?

Mr Cartagena: It is a very good point that some companies would not admit that they have had an event and paid a ransom. I think regulation is making that less possible in certain areas. The total amounts of ransomware costs are easy to find, although you cannot find them in the public news. A lot of ransomware groups or cartels advertise themselves, almost like companies, in order to recruit people to work for them. Although what they claim may not be fully authentic, it is corroborated by the amount of economic losses that are being made. I think there is no doubt that costs are on the rise. About the actual numbers, yes, there may be some uncertainty, but what is worrying is that they are definitely only going up.

Moderator: To what extent are regulators or other people cognizant of the work that companies are doing? What is the relationship with those regulatory bodies who are looking at what companies are doing about their capital models and reserves?

Mr Cartagena: I think the fairest thing to say about the regulators is that they are learning and trying to solve the same problem. To some extent, perhaps they are leaning on the market to solve it and ultimately give them the comfort that we have thought about it enough and done the right things. If I was a regulator, my concern would be whether enough capital was being allocated to a risk, and how companies have gone about doing that. If we consider the European Insurance and Occupational Pensions Authority (EIOPA), the standard formula does not even recognise cyber risk explicitly. So, if you are a standard formula company, you can write almost as much cyber as you want because you are not going to carry capital for it. It is calibrated for cyber in the same way as for general liability. So, there is a challenge for that regulator to get comfortable. There is also a challenge for the PRA. They have approved a lot of internal models, but have they approved the way that companies have modelled cyber, and how do they get comfortable with that? Overall, I think the relationship with the regulators has been collaborative, with everyone learning at the same time.

Miss Grewal: Yes. My view is that this is very much on the radar of regulators. A few years ago, Lloyd's was doing a deep dive into how cyber was being modelled in internal models. There was a PRA cyber sensitivity stress testing exercise that was released, at the start of 2023, which highlighted the concerns they had around cyber parametrisation and quantification (PRA, 2023). We have also had regulatory interest in the work that we have done.

Mr Cartagena: We had the US Treasury raise questions about some of this work, and they were coming from a point of zero knowledge and wanting to find out more from us. There is a lot of learning still to be done.

Moderator: Would either of you like to make any final comments before we finish?

https://doi.org/10.1017/S1357321724000230 Published online by Cambridge University Press

Miss Grewal: My final comment would be to consider current processes and what steps are needed to improve them. Cyber parametrisation, and also parametrisation processes for other classes, are very stagnant and they do not evolve as quickly as they should. I would say another key take-away is to think about where you want processes to have increased confidence. Even if there is uncertainty, how can you have a better handle on that uncertainty?

Mr Cartagena: My closing comment is that we need to consider regular reviews of modelling and assumptions, where they are appropriate, and what they mean. Ultimately, you need to give management and the board confidence that you have done all you can to get comfortable with the figure that you are proposing. I think that message is probably the same for any line of business, but cyber has an interesting element of constant change, and I think people need to consider this to a greater extent.

Moderator: Thank you. I found it fascinating listening to this discussion and seeing the paper. I think what this says to me is how much is dependent on the judgement of the individual. It is important to work with one's company and with their clients in terms of understanding what might be going on, looking forward as much as backward. It is also important to work well with people who are outside our profession to see the emergence of risks into the future. There is clearly lots more work to be done and each year will bring its own challenges, no doubt, when looking at these types of risks.

References

Swiss Re. (2022). Cyber insurance: Strengthening resilience for the digital transformation, available at https://www.swissre.com/dam/jcr:6fd9f6dd-4631-4d9f-9c3b-5a3b79b321c0/2022-11-08-sri-expertise-publication-cyber-insurance-strengthening-resilience.pdf (accessed 7 Sept 2024).

PRA. (2023). Thematic findings from the 2022 cyber stress test, available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf (accessed 7 Sept 2024).

Cite this article: Cyber risk capital. *British Actuarial Journal*. https://doi.org/10.1017/S1357321724000230