British Actuarial Journal (2020), Vol. **25**, e9, pp. 1–15
doi:10.1017/S1357321720000124

ABSTRACT OF THE LONDON DISCUSSION

Silent cyber assessment framework

[Institute and Faculty of Actuaries, Sessional Research Event, London, 9 December 2019]

Abstract

This abstract relates to the following paper:
Cartagena, S., Gosrani, V., Grewal, J. & Pikinska, J. (2019) Silent Cyber Assessment Framework. *British Actuarial Journal.*

The Chairman (Mr S. M. Shepley, F.I.A.): Welcome to the Sessional Research Event on the Silent Cyber Assessment Framework. The word "Cyber" means a lot of different things to different people. I thought I would read the definition of cyber insurance used by a US insurer: "Cyber insurance is an insurance product designed to help businesses hedge against the potentially devastating effects of cyber crimes, such as malware, ransomware, denial of service attacks, or any other method used to compromise the network or sensitive data."

This is quite all-encompassing. It is also extremely topical in society, not least within the insurance industry. The increasing interconnectedness of what we all do, both commercially and personally, means that there are so many access points. If they are threatened, then it will have a consequence. Most of us should be thinking about how to mitigate this risk. Clearly, there is the potential for interference in commercial and financial endeavours, the political process, and also cyber attacks can be used, or seen, as weapons of war.

We are all familiar with increasing concerns around privacy and data security. Regulators and lawyers are playing an active part in establishing ground rules and the appropriate rules and regulations to help us navigate in this difficult area.

Clearly, a lot of the traditional underwriting considerations apply in this area. However, the nature of the risk is split between physical and digital elements. Some pundits would say 40%, globally, of that risk is intangible rather than physical in nature. If the insurance industry does not want to fall behind, it needs to evolve very fast to help people hedge and transfer some of those risks. I am delighted to say, from my experience that is happening, although the industry is definitely in the early part of the journey.

For many, the protection against cyber events is largely about being able to obtain post-event support and expertise to manage the consequences of being attacked. This may involve, for example, issues around the information technology (IT) infrastructure of the organisation, or around minimising the reputational damage to the organisation perhaps using suitable public relations.

Business interruption, clearly, is a major area of concern.

Forensic/legal support may be needed to protect organisations against potential lawsuits and counter-suits. These examples are much more about providing practical advice, guidance and support rather than a certain amount of money. That makes it quite an interesting and innovative insurance product. It is certainly constrained by some financial limits, but what the insurance product provides is service and priority access post-event.

Another facet here is that a lot of the risk is first party. It is not just third-party indemnity against liabilities. One needs to consider both the first-party and third-party aspects.

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

Notwithstanding that, cyber has been around for some time, whether we knew it or not. Existing portfolios are exposed to cyber. We are here tonight to focus on silent cyber, which is the cyber that is inherent within existing, more traditional policies. But clearly the world of affirmative cyber is growing up. There is beginning to be quite an attractive marketplace for that type of product. Whether you are a leading name in Lloyds or whether you are a large multinational, there is definitely a business opportunity for you as a risk carrier in that space.

There are many myths about cyber. I am not promising that we will explode those myths today. For example, small businesses may think: "Well, I don't need to worry about cyber too much because I outsource my IT." That view is not going to go down very well as a defence. Perhaps related to that, there is an expectation that cyber cover is going to be very expensive. That is not necessarily the case either.

There is huge concern in the population from the wide-scale, orchestrated cyber attacks on email and telephone fraud. As a consequence of that risk awareness, there is a definite need in the marketplace for appropriate products.

The US was at the forefront of developing cyber-related coverages, in part, perhaps, because the law and the regulations required boards to give active consideration under Enterprise Risk Management (ERM) for errors and omissions, and the consequences of any cyber-related attacks. Clearly, now, with General Data Protection Regulation (GDPR) across Europe, and more generally with regulatory awareness, there is a need for nearly all boards and companies to be actively thinking about how to describe, mitigate and manage this risk.

It is not a simple situation and there continue to be some relevant legal issues. For example, if you have a cover which is traditional in nature, and you have an affirmative cyber product, which responds first? In talking with a number of underwriters, as recently as last week, I think there is still a view that the legal debate in this area has yet to be resolved.

I am delighted to have Visesh Gosrani here tonight, on behalf of the Institute and Faculty of Actuaries' Cyber Risk Working Party to present a framework and some considerations as to how we think about non-affirmative cyber, the silent aspect of cyber within risk portfolios. Visesh (Gosrani) has spent the last 3 years focused on cyber risk. He started his cyber risk journey with Cyence where he focused on both assessing cyber risk at the risk selection stage, through the collection and analysis of data to supplement underwriting submissions, and also on a portfolio management level, where he assessed the aggregation of cyber risk and the evolving nature of both the threat and insured entities within a portfolio over time. Since leaving Cyence, he has assisted companies in assessing their exposure to cyber perils within the non-cyber insurance they have already written, and he is also putting together a cyber product for a niche market. Outside of cyber, Visesh is a qualified actuary with 20 years of experience in general insurance, mainly focused on risk management and Solvency II.

Mr V. Gosrani, F.I.A.: I am not going to focus on the background to cyber in any more detail than Stuart (Shepley) has today. That information is available within papers that we have already written and within the paper that accompanies this framework.

I am proud to say that we have managed to put this framework together quite quickly. We had the idea to put the framework together back in June because we were seeing that people were coming to us, as a working party, with questions about how they might assess their non-affirmative risk. We realised we had only limited guidance to give them.

In terms of the agenda for today, whilst I am not going to discuss what cyber is as a peril, I am going to spend some time talking about the difference between affirmative and non-affirmative risk so that we are sure we are talking about the same thing. I can't stress enough that taxonomy is really important within your organisation as you start to deal with this.

I am then going to move on and spend most of the time talking about the Silent Cyber Framework, with a fair bit of time thinking about scoping out that exercise. That is not because any of you will be new to scoping but because there are particular issues in scoping this exercise of which you should be

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

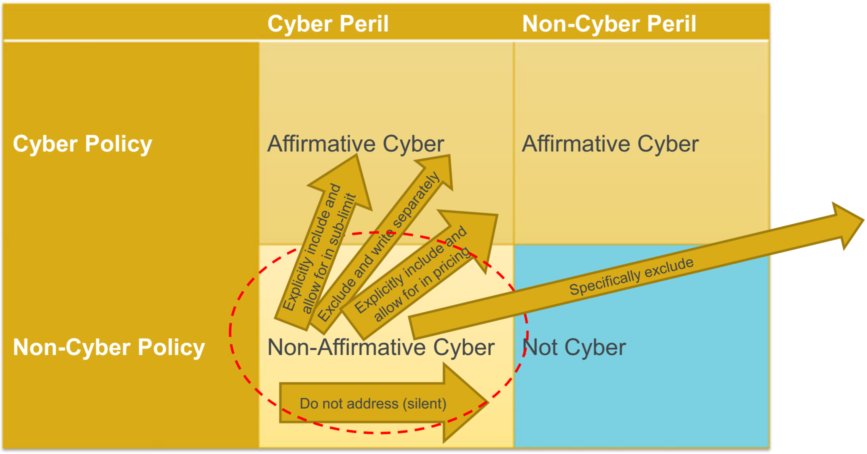


Figure 1. The part of your portfolio the framework is targeting.

aware. I will then spend some time talking about real-life example scenarios. I will move on to give thanks to the working party, and then I will open up for questions before I summarise.

Many of you might have seen a matrix of the form shown in Figure 1 before. On the top row, you have the affirmative cyber, which is any cyber policy that has losses under it. That would be considered to be an affirmative cyber loss. What is more important is the non-cyber policies. Most of your losses under a non-cyber policy will not be cyber, and that is what you will be expecting. However, you may have cyber perils causing losses under that policy and that is what we are dealing with as part of this framework. The reason I bring this up is because, when you deal with them under this framework, they will move into other boxes. What you need to be clear about is what terminology you use for that new risk. You can exclude the cyber that is within those non-affirmative policies and write it separately, in which case it is clearly affirmative cyber. Or you can exclude it completely, in which case it is no longer a covered loss. You could explicitly include it and allow for it within a sub-limit or price it. In both cases, it is then affirmative cyber. If you do not address it and you do nothing, it is still silent cyber.

Another approach is to not address it and then have a loading to reflect the fact that you understand that there is an increased level of risk and it is just difficult to quantify.

As we move forward, we are talking about the box that is ringed in red in Figure 1, but we must not forget that we will have non-affirmative exposures and some affirmative exposures. When we are thinking about aggregations across the portfolio, it is important to consider both those exposures.

Moving on to the Silent Cyber Assessment Framework, we are going to start with thinking about scoping the exercise. Most of you that will be using the framework will be doing so amongst many other commitments and you may not have planned for this in advance. You need to work out what is achievable for you. Whilst I can use the cliché that you get out what you put in, what is more important is to do something and to start that journey. You need to temper your efforts such that you obtain some deliverables from the exercise and that you produce some messages so that you can plan the way forward.

That middle hexagon in Figure 2, “Senior Buy-In”, is important for many reasons, not least because you need to understand how concerned they are about their silent cyber exposures and therefore how much support they prepared to give you at the start of this exercise. Then you need to temper that with an idea of what is achievable. If we consider lines of business, there was a Prudential Regulation Authority (PRA) survey a year ago where, across the board, there were companies that thought that they had significant exposure to non-affirmative risk within

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

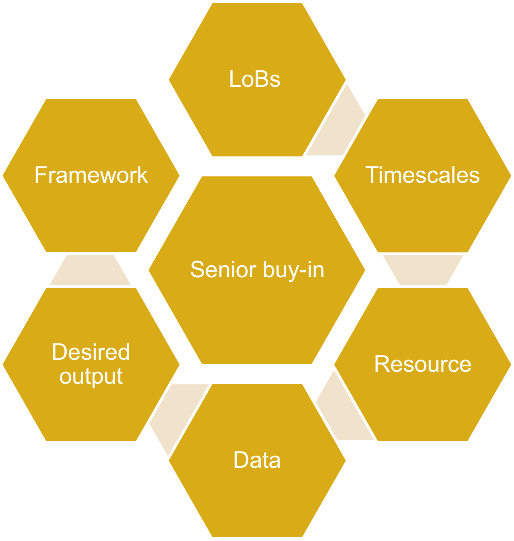


Figure 2. Scoping the exercise.

their non-cyber lines of business. However, that exposure is much greater in some lines of business than others, because of the greater number of perils and the greater potential impact that those perils can have.

It may be the case that when you start this exercise, you just start with a small number of lines of business that your underwriters think are going to be heavily exposed. That way, you limit the scope. One reason for that is when you do the exercise, you might have to do quite a lot of data manipulation because the classes of business have different recording formats. You might need to supplement and enhance the data to some extent. All that preparatory work is going to take up time before you can produce an initial result. Every extra line of business (LoB) may cause you a significant amount of additional time.

The timescales that you have are important, not just because of the length of the exercise but because, as you come to quarter renewals, it may be the case that there are particular lines of business that are exposed. You might be able to do something about them before the quarter renewals, or there may be other renewal dates that are important to your LoB. It is useful to have initial conversations such that you can target the exercise to produce something that the company can immediately use.

The resources required will not be just manpower. There will be manpower needed to do some of that data extraction and manipulation, but the main factor will be obtaining the necessary skill sets. What is hard with the cyber problem is that there is not one area of the business that comprehensively understands it. As you form a centre of competence within your organisation, you will be able to utilise the collective knowledge in order to be able to understand the nature of the perils and risks much better. You will need underwriting support, because you will need to understand, within your business, how cyber exclusions are being used. You will need IT support, in order to understand the nature of the existing risks and how they might manifest. There is an operational technology side of the risk which you must not neglect. It may be the case that you have some support from, say, your engineering departments, if they have some understanding of those issues. There may be other areas within the firm, or within your IT department, from which you can bring in some operational technology experience. You need to think about obtaining policy wording expertise from your underwriting or legal departments.

Data quality will severely limit what you can achieve. When you start thinking about what you are going to do, understanding what your recorded data have within it will help you to work out a sensible goal. For example, if none of your policies record whether a cyber exclusion is present,

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

that is already a piece of work that needs to be done. If they record a cyber exclusion but do not record which one is used, or whether there are any changes made to it, you are further ahead but there will be enhancements needed. The framework has ways to deal with these types of issues and to produce an output. But the more that you can do to enhance your data, or put in place programmes that will enhance your data over time, the more benefit you will obtain from these exercises.

You will find that, if your claims department has been recording risks that have resulted in cyber claims, then you can get a much better handle on how the claims you are seeing marry up to what you consider to be your exposure.

The output desired by management is likely to be in a number of forms. If they want to understand how the exposure to non-affirmative cyber risk compares to any prior estimates that they might have made, it is useful to have the benefit of some scenarios that bring it to life. You might have to develop a large number of assumptions to do that.

Therefore, it might be something that you need to scope as a separate exercise, but the framework can be used in partial forms. Why that might be helpful is because cyber perils can affect a large number of lines from a single event. To date, firms have not been confident about their quantitative estimates. As you bring this to life and show the assumptions and sensitivities you can potentially bring much more clarity to senior management.

Lastly, you need to confirm that this framework is suitable for your needs. We have designed it to be useful for many firms and to be very malleable, but it may be the case that you have a better tool that has already been developed in-house, or you can do something in a slightly different way using your systems. What we have is very open source, and so you can feel free to change it in any way you like.

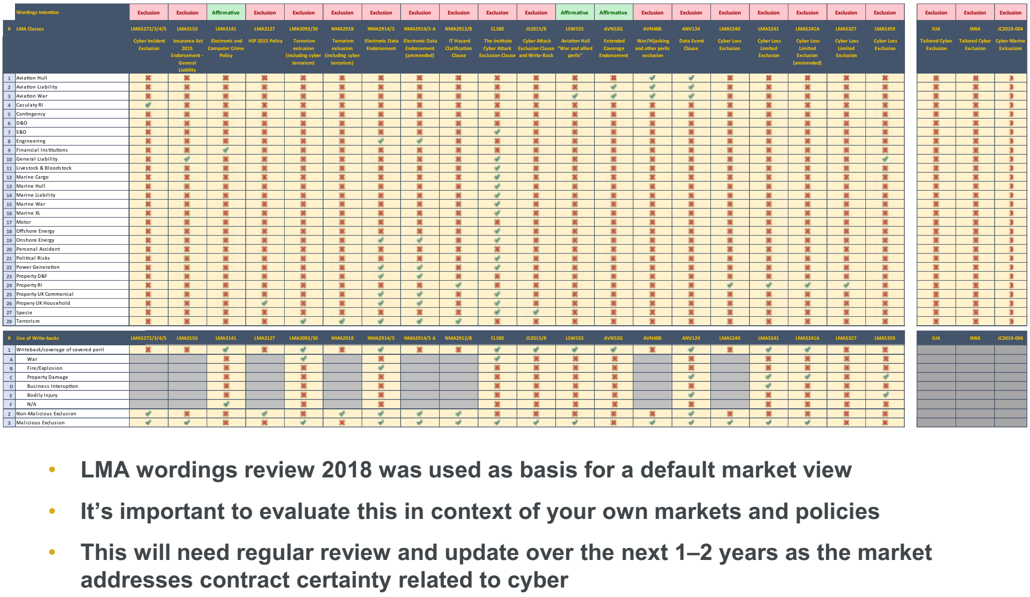
We feel that we have provided something that takes somebody from a very early stage to at least a medium level of understanding. I think that is going to be relevant for most firms. To obtain a greater understanding would require more specialist tools, for example, in order to understand what your exposure to cyber risk is from the cyber posture of the companies within your insured group.

I will now move on to the first of the two main parts of the cyber assessment framework. Populating the data is the bulk of the effort, but once you have done that you will have a better understanding of your non-affirmative exposure. We used the Lloyd's Market Association (LMA) Wordings review from January 2018 to populate the framework. You can see which clauses are applied across which classes of business, generally, within the market at any time, and therefore the clauses to which you may have exposure. You will need to do more work to find a better answer. You will need to work out the right measure of exposure for you, whether you have cyber sub-limits within your policies, how accessible those cyber sub-limits are in terms of being recorded into your policy database, and also the extent to which they might be effective. To understand the extent to which they are effective, you will need to assess your clause usage and confidence. At the end of this process, you will have a much better understanding of your portfolio and how the risk is managed within it.

You will understand the clauses that you are using by LoB, and also the extent to which those clauses are being amended in, maybe, an inconsistent basis to suit particular clients. You will have a level of confidence on the extent to which those clauses might work and hold in various scenarios.

One thing I can bring out here is the real-life example of NotPetya. When that occurred, the CL.380 exclusion clause had been used for quite some time. There were known issues with the wording, and the reason that Zurich is being taken to court by Mondelez is because there is a war write-back for CL.380. The US attributed Russia as having been the proponent behind the attack. If that argument fails, they have a second argument, which is that non-malicious attacks are not excluded within the wording and Mondelez was not the target but a bystander and collateral damage.

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press



	Wordings Intention	Exclusion	Exclusion	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Affirmative	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion
#	LMA Classes	LMA5272/3/4/5 Cyber Incident Exclusion	LMA3150 Insurance Act 2015 Endorsement - General Liability	LMA3141 Electronic and Computer Crime Policy	LMA3127 HIP 2015 Policy	LMA3092/30 Terrorism exlcusion (including cyber terrorism)	NMA2918 Terrorism exlcusion (including cyber terrorism)	NMA2914/5 Electronic Data Endorsement	NMA2914/5 A Electronic Data Endorsement (ammended)	NMA2912/8 IT Hazard Clarification Clause	CL380 The Institute Cyber Attack Exclusion Clause	JS2015/8 Cyber Attack Exclusion Clause and Write-Back	LSW555 Aviation Hull "War and allied perils"	AVN52G Extended Coverage Endorsement	AVN48B War/Hijacking and other perils exclusion	ANV124 Data Event Clause	LMA5240 Cyber Loss Exclusion	LMA5241 Cyber Loss Limited Exclusion	LMA5241A Cyber Loss Limited Exclusion (ammended)	LMA5327 Cyber Loss Limited Exclusion	LMA5359 Cyber Loss Exclusion	IUA Tailored Cyber Exclusion	IMIA Tailored Cyber Exclusion	JC2019-004 Cyber Marine Exlcusions
1	Aviation Hull	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
2	Aviation Liability	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
3	Aviation War	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
4	Casulaty RI	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
5	Contingency	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
6	D&O	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
7	E&O	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
8	Engineering	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
9	Financial Institutions	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
10	General Liability	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
11	Livestock & Bloodstock	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
12	Marine Cargo	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
13	Marine Hull	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
14	Marine Liability	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
15	Marine War	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
16	Marine XL	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
17	Motor	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
18	Offshore Energy	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
19	Onshore Energy	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
20	Personal Accident	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
21	Political Risks	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
22	Power Generation	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
23	Property D&F	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
24	Property RI	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
25	Property UK Commercial	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
26	Propery UK Household	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
27	Specie	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
28	Terrorism	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

#	Use of Write-backs	LMA5272/3/4/5	LMA3150	LMA3141	LMA3127	LMA3092/30	NMA2918	NMA2914/5	NMA2914/5 A	NMA2912/8	CL380	JS2015/8	LSW555	AVN52G	AVN48B	ANV124	LMA5240	LMA5241	LMA5241A	LMA5327	LMA5359	IUA	IMIA	JC2019-004
1	Writeback/coverage of covered peril	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗			
A	War			✗		✓		✗			✓	✗	✗	✗		✗		✗	✗	✗	✗			
B	Fire/Explosion			✗		✗		✓			✗	✗	✗	✗		✗		✗	✗	✗	✗			
C	Property Damage			✗		✗		✗			✗	✗	✗	✗		✓		✓	✓	✗	✓			
D	Business Interuption			✗		✗		✗			✗	✗	✗	✗		✗		✓	✗	✗	✗			
E	Bodily Injury			✗		✗		✗			✗	✗	✗	✗		✓		✗	✗	✗	✓			
F	N/A			✓		✗		✗			✗	✗	✗	✗		✗		✗	✗	✗	✗			
2	Non-Malicious Exclusion	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗			
3	Malicious Exclusion	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗			

- LMA wordings review 2018 was used as basis for a default market view
- It's important to evaluate this in context of your own markets and policies
- This will need regular review and update over the next 1–2 years as the market addresses contract certainty related to cyber

Figure 3. Clause usage and interpretation.

What is important about the overall exercise is the increased level of understanding it will produce. You should know what types of cyber losses might impact the policies, and also whether older clauses are being used, and therefore how this might impact on your exposure. If you are using older clauses, it may be difficult to immediately move to newer clauses, but at least with that information you can start to make that change. You will have estimates of your exposure by LoB and will also have it split between how much you think is affirmatively written versus excluded, versus silent, and also by coverage.

We have designed the framework so that, where you have inconsistencies within the treatment of policies, you can do a policy-level assessment. That is something that we would not expect you to do for the whole of your book unless you have serious concerns about your book as a whole. The purpose is to enable you to obtain a deeper understanding of the places where you think you have peak exposures. Figure 3 shows a matrix containing information about the initial population of how the clauses work across classes. It is intentionally compact and it is not necessary for you to be able to read it.

This enables you to have an initial view of the non-affirmative exposure that you have. Then within this part of the framework you can work with your underwriters to determine, for your classes of business, what clauses you are using. You can also see whether your underwriters agree with the LMA interpretation of what the classes cover and what they exclude. What is important is that the cyber market evolves quickly. As you repeat this exercise, there will be new wordings that will have come out. The matrix will not stay static. You will need to allow for the new wordings, and potentially for changes and new information about those classes of business.

The second part of the exercise is developing the scenarios. What the framework does not do is give you a comprehensive set of scenarios, whereby you input a set of assumptions and you get an answer out. The hardest part of developing those scenarios is thinking of the most useful scenarios. We have heat maps and other tools within the framework that will enable you to assess the scenarios by LoB and coverage. You can then start to consider the types of event that could impact you and be a serious risk. Do not underestimate how difficult it is to assess the severity of those scenarios correctly. There are not many public sources of information that will enable you to understand how prevalent, say, software might be within organisations if you are thinking about

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

estimating mass vulnerability. There are a significant number of assumptions that you will not be able to easily assess. For example, how long it might take for the organisations within your portfolio to patch their systems, and potentially the extent to which an infection might spread before they do this. What is important is making what you think is a good estimate and then using other sources to provide you with some additional guidance. These sources could, for example, be the brokers that you use who have cyber departments or the regulators and the stress tests that they have put out.

For those of you working in the UK, Lloyds and the PRA have put out quite a few stress tests. The cyber model vendors have also put out various scenarios, trying to describe how attacks might occur, and how the impacts of them might be manifested. In a similar vein, risk research organisations and think tanks, such as the Cambridge Institute for Risk Studies, have put out cyber scenarios. There is a good paper from the Organisation for Economic Co-operation and Development (OECD) from late 2017. It has a chapter that gives a good introduction to the perils as they work in terms of cyber risk and also a good introduction to non-affirmative. Despite that paper being a couple of years old, it is still very relevant today. When you are thinking about silent cyber, the bad things that could happen will aggregate across your portfolio. There are lots of different ways in which that might occur. You may, for example, have a relationship, as an insurer, with a company. You sell them a number of different policies for different lines of business. It is possible that an event that occurs might impact more than one of those lines of business. Another example is that you might have a relationship with a group of companies. It may be the case that a particularly targeted company is not accessible because their cyber hygiene is quite good, but another company within that group has network access to that company and therefore is used as an entry route. Industry is regularly thought of as an aggregation point, but related industries can also have that aggregation issues. For example, it may be the case that related industries use similar sorts of software and therefore have similar vulnerabilities. There are particular dependencies in manufacturing. If you have an incident in one of the manufacturing companies you insure, they might be supplying to somebody else that you insure. This might create a business interruption loss in the second company because the originally attacked insured is no longer able to make the parts that are essential for them to continue their just-in-time manufacturing process.

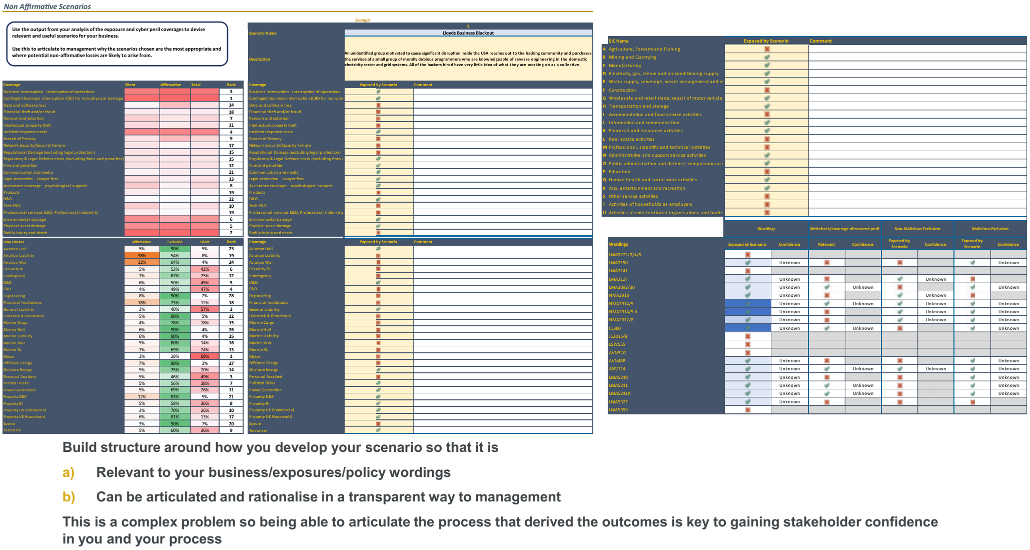
There are solution vendors who might implement solutions for a wide range of companies within an industry. If they have not thought about their cybersecurity properly, or if the consultancies that might often work to implement those solutions have not thought about them properly, and this is systemic across all the installations there might be claims under the Errors and Omissions (E&O) and professional liability policies.

You might also have knock-on impacts. A really graphic example is a dam bursting. There have been incidents whereby dams have been tampered with, and there have been intruders found in the system. It is not clear whether all the losses that have resulted have resulted from cyber, but the flooding that occurs downstream would not be covered by the dam insurance itself. Similarly, if you have a power outage as a result of an attack, you will have resultant contingent business interruption losses. You might have other cyber aggregation points. If you have a cloud outage, it may be that the companies in an industry with which you are concerned all use a particular cloud service provider because they host a particular solution on which they are all reliant. Lastly, within those scenarios, you need to consider reinsurance. Reinsurance does not always have the same treatment of exclusions as your primaries. There is a potential area of risk because your reinsurance may not react in the way that you expect.

What you see in Figure 4 is some of the exhibits within the framework itself. There is a heat map which splits between silent, excluded and affirmative risks. You have a similar heat map within the framework which splits between the coverages. You can see which lines of business have which types of exposures.

Moving on to the middle of Figure 4, once you have established which coverages are exposed, you can write down a rationale for why they might be exposed, such that you can then return to

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press



Non Affirmative Scenarios

Use the output from your analysis of the exposure and cyber peril coverages to devise relevant and useful scenarios for your business.

Use this to articulate to management why the scenarios chosen are the most appropriate and where potential non-affirmative losses are likely to arise from.

Coverage	Silent	Affirmative	Total	Rank
Business interruption - Interruption of operations				3
Contingent business interruption (CBI) for non-physical damage				1
Data and software loss				14
Financial theft and/or fraud				18
Ransom and extortion				7
Intellectual property theft				11
Incident response costs				4
Breach of Privacy				9
Network Security/Security Failure				17
Reputational Damage (excluding legal protection)				15
Regulatory & Legal Defence costs (excluding fines and penalties)				15
Fine and penalties				12
Communication and media				21
Legal protection – Lawyer fees				13
Assistance coverage – psychological support				8
Products				19
D&O				22
Tech E&O				10
Professional services E&O, Professional indemnity				19
Environmental damage				6
Physical asset damage				5
Bodily injury and death				2

LMA Classes	Affirmative	Excluded	Silent	Rank
Aviation Hull	5%	90%	5%	23
Aviation Liability	38%	54%	8%	19
Aviation War	32%	64%	4%	24
Casualty RI	5%	53%	42%	6
Contingency	7%	67%	25%	12
D&O	6%	50%	45%	5
E&O	4%	49%	47%	4
Engineering	8%	90%	2%	28
Financial Institutions	18%	73%	12%	18
General Liability	3%	40%	57%	2
Livestock & Bloodstock	5%	90%	5%	22
Marine Cargo	4%	78%	18%	15
Marine Hull	6%	90%	4%	26
Marine Liability	6%	90%	4%	25
Marine War	5%	80%	14%	16
Marine XL	7%	69%	24%	13
Motor	3%	28%	69%	1
Offshore Energy	7%	90%	3%	27
Onshore Energy	5%	75%	20%	14
Personal Accident	5%	46%	49%	3
Political Risks	5%	56%	38%	7
Power Generation	5%	69%	26%	11
Property D&F	12%	83%	5%	21
Property RI	5%	58%	36%	8
Property UK Commercial	3%	70%	26%	10
Property UK Household	6%	81%	13%	17
Specie	3%	90%	7%	20
Terrorism	5%	60%	36%	9

Example

	2
Scenario Name	Lloyds Business Blackout
Description	An unidentified group motivated to cause significant disruption inside the USA reaches out to the hacking community and purchases the services of a small group of morally dubious programmers who are knowledgeable of reverse engineering in the domestic electricity sector and grid systems. All of the hackers hired have very little idea of what they are working on as a collective.

Coverage	Exposed by Scenario	Comment
Business interruption - Interruption of operations	✓	
Contingent business interruption (CBI) for non-phy	✓	
Data and software loss	✗	
Financial theft and/or fraud	✗	
Ransom and extortion	✗	
Intellectual property theft	✗	
Incident response costs	✓	
Breach of Privacy	✗	
Network Security/Security Failure	✗	
Reputational Damage (excluding legal protection)	✗	
Regulatory & Legal Defence costs (excluding fines a	✓	
Fine and penalties	✓	
Communication and media	✓	
Legal protection – Lawyer fees	✓	
Assistance coverage – psychological support	✓	
Products	✗	
D&O	✓	
Tech E&O	✗	
Professional services E&O, Professional indemnity	✗	
Environmental damage	✓	
Physical asset damage	✓	
Bodily injury and death	✗	

Coverage	Exposed by Scenario	Comment
Aviation Hull	✓	
Aviation Liability	✗	
Aviation War	✗	
Casualty RI	✗	
Contingency	✗	
D&O	✓	
E&O	✗	
Engineering	✗	
Financial Institutions	✗	
General Liability	✓	
Livestock & Bloodstock	✗	
Marine Cargo	✗	
Marine Hull	✗	
Marine Liability	✗	
Marine War	✗	
Marine XL	✗	
Motor	✗	
Offshore Energy	✗	
Onshore Energy	✓	
Personal Accident	✗	
Political Risks	✓	
Power Generation	✓	
Property D&F	✓	
Property RI	✓	
Property UK Commercial	✓	
Property UK Household	✓	
Specie	✗	
Terrorism	✓	

	SIC Name	Exposed by Scenario	Comment
A	Agriculture, Forestry and Fishing	✗	
B	Mining and Quarrying	✓	
C	Manufacturing	✓	
D	Electricity, gas, steam and air conditioning supply	✓	
E	Water supply, sewerage, waste management and re	✓	
F	Construction	✗	
G	Wholesale and retail trade; repair of motor vehicle	✓	
H	Transportation and storage	✓	
I	Accommodation and food service activities	✗	
J	Information and communication	✓	
K	Financial and insurance activities	✓	
L	Real estate activities	✗	
M	Professional, scientific and technical activities	✗	
N	Administrative and support service activities	✓	
O	Public administration and defence; compulsory soci	✓	
P	Education	✗	
Q	Human health and social work activities	✓	
R	Arts, entertainment and recreation	✓	
S	Other service activities	✗	
T	Activities of households as employers	✗	
U	Activities of extraterritorial organisations and bodie	✗	

	Wordings		Writeback/coverage of covered peril		Non-Malicious Exclusion		Malicious Exclusion	
Wordings	Exposed by Scenario	Confidence	Relevant	Confidence	Exposed by Scenario	Confidence	Exposed by Scenario	Confidence
LMA5272/3/4/5	✗							
LMA3150	✓	Unknown	✗		✗		✓	Unknown
LMA3141	✗							
LMA3127	✓	Unknown	✗		✓	Unknown	✗	
LMA3092/30	✓	Unknown	✓	Unknown	✗		✓	Unknown
NMA2918	✓	Unknown	✗		✓	Unknown	✗	
NMA2914/5	✓	Unknown	✓	Unknown	✓	Unknown	✓	Unknown
NMA2914/5 A	✓	Unknown	✗		✓	Unknown	✓	Unknown
NMA2912/8	✓	Unknown	✗		✓	Unknown	✓	Unknown
CL380	✓	Unknown	✓	Unknown	✗		✓	Unknown
JS2015/8	✗							
LSW555	✗							
AVN52G	✗							
AVN48B	✓	Unknown	✗		✗		✓	Unknown
ANV124	✓	Unknown	✓	Unknown	✓	Unknown	✓	Unknown
LMA5240	✓	Unknown	✗		✗		✓	Unknown
LMA5241	✓	Unknown	✓	Unknown	✗		✓	Unknown
LMA5241A	✓	Unknown	✓	Unknown	✗		✓	Unknown
LMA5327	✓	Unknown	✗		✗		✗	
LMA5359	✗							

Build structure around how you develop your scenario so that it is

a) Relevant to your business/exposures/policy wordings

b) Can be articulated and rationalise in a transparent way to management

This is a complex problem so being able to articulate the process that derived the outcomes is key to gaining stakeholder confidence in you and your process

Figure 4. Scenario generation.

that as you learn. Your views will change over time so it is important that you record your initial assumptions.

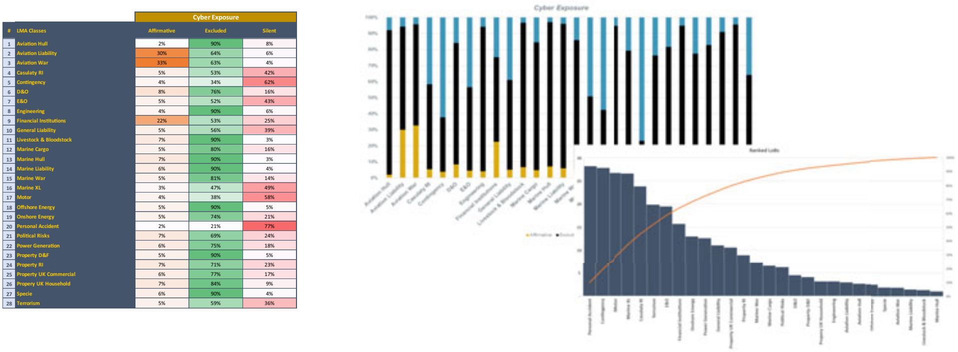
In the bottom-right of Figure 4, you see some more summarised data, in terms of industry, so that you can consider the issues at that level. Out of these scenarios, you will obtain an understanding of what the real vulnerabilities might be for your organisation and how you are managing them. This means that you can focus attention on what the right actions might be in terms of targeting particular areas of the portfolio.

This is going to be an ongoing set of exercises as you learn more and more. It is not just quantitative reporting that you need to communicate. You will have estimates of how the impact on various lines of business differs from those that might have been previously communicated within the organisation.

You will also understand what the impacts might be on stress tests that you have previously reported. They might generally be positive impacts because companies have erred on the side of prudence when they have been reporting the results of the tests. They have not necessarily adjusted the results to allow for the fact that they might be writing policies on companies that have a better level of cyber hygiene or they may have just assumed the worst within that reporting. You can, at least, start to build a picture of how those results might change before the next reporting deadline. What is important is not necessarily where you have the biggest areas of exposure, but where you have the biggest areas of exposure and do not have confidence in the clauses that are being applied. If you are happy with the clauses that are being applied to manage the exposure on some of your largest lines of business, you may wish to consider whether there are any fairly large lines where you do not necessarily have the control that you might expect. The initial thing you can do is to look at whether there have been any new wordings issued that would give you greater confidence.

There will be a number of lessons that you will be able to learn from this. What is important is to distil the knowledge and understanding into what might be important to communicate to senior management about the way that your view of the world has changed. You might identify brokers or delegated authorities that are bringing you business that is giving you much greater exposure to non-affirmative risk than you might want. This enables you to reconsider those relationships. You might identify underwriters who are systemically not using the right sorts of

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press



		Cyber Exposure		
#	LMA Classes	Affirmative	Excluded	Silent
1	Aviation Hull	2%	90%	8%
2	Aviation Liability	30%	64%	6%
3	Aviation War	33%	63%	4%
4	Casulaty RI	5%	53%	42%
5	Contingency	4%	34%	62%
6	D&O	8%	76%	16%
7	E&O	5%	52%	43%
8	Engineering	4%	90%	6%
9	Financial Institutions	22%	53%	25%
10	General Liability	5%	56%	39%
11	Livestock & Bloodstock	7%	90%	3%
12	Marine Cargo	5%	80%	16%
13	Marine Hull	7%	90%	3%
14	Marine Liability	6%	90%	4%
15	Marine War	5%	81%	14%
16	Marine XL	3%	47%	49%
17	Motor	4%	38%	58%
18	Offshore Energy	5%	90%	5%
19	Onshore Energy	5%	74%	21%
20	Personal Accident	2%	21%	77%
21	Political Risks	7%	69%	24%
22	Power Generation	6%	75%	18%
23	Property D&F	5%	90%	5%
24	Property RI	7%	71%	23%
25	Property UK Commercial	6%	77%	17%
26	Propery UK Household	7%	84%	9%
27	Specie	6%	90%	4%
28	Terrorism	5%	59%	36%

- **What do management need to know/understand about the silent cyber problem?**
  - **Peak exposures**
  - **Wordings usage**
  - **Potential vulnerabilities/single point of failures/industries at risk**
- **If a LoB is perceived as being excluded be clear with management on the confidence of that exclusion.**
- **There is a difference between single loss and systemic scenarios, for example, clauses may be more susceptible stand alone versus an accumulation event and vice versa. Make sure management is aware of the potential of both**
- **Is there a scenario your business should be concerned about?**

Figure 5. Risk reporting management information.

clauses. This will enable you to have conversations so that they understand the importance of using more appropriate clauses.

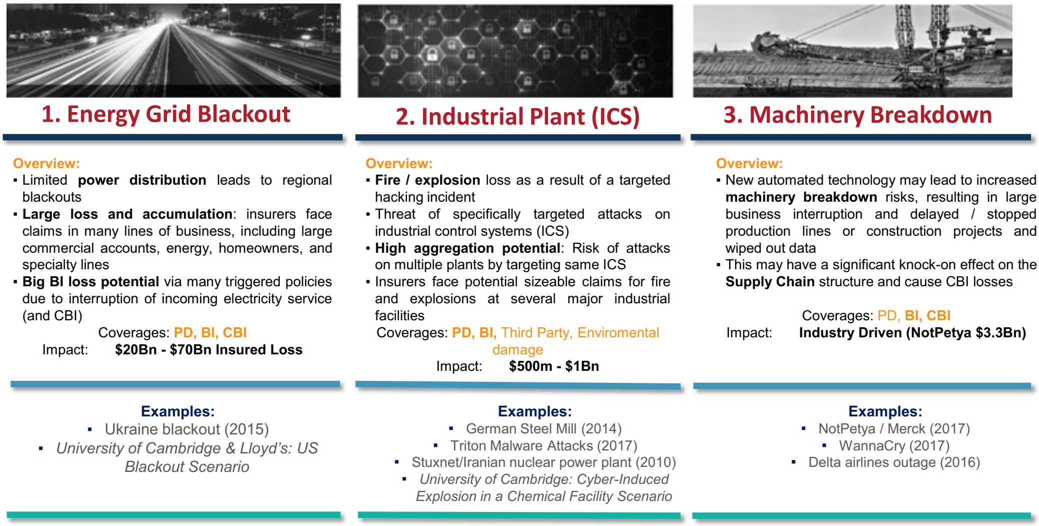
The pricing of cyber risk will vary amongst lines of business. You may have a good understanding of the risks and perils within a LoB that enables you to price the non-affirmative exposure appropriately. Or you may just have an indicative view which means that you can use some sort of loading to reflect that. Generally, firms communicated to the PRA that they were confident in their reinsurance. Confirming that that is the case, or potentially highlighting some issues that might exist, would also be important.

Once you have relayed these messages, there will be further steps that need to be taken. It is important to obtain buy-in from management so that you can have support for your proposed steps. You may have a range of options in terms of what types of further investigation you think is important. It is really important to have the resource and time to be able to do that work. Potentially, having the initial group that has been brought together being formally tasked with being a cyber centre of competence means that you can retain their knowledge and have a set of focused individuals working in the area. Also, your data will be important to the outcome of your exercises. You need to put processes in place such that your policies better record what exclusions are being used and whether there are any alterations made. You also should improve your claims records. You need to know whether there is a cyber peril and sufficient detail about the claim itself so you can understand your overall exposure and how that is translating into losses.

In Figure 5, we have some visuals that we have produced within the framework that enable you to start to communicate the quantitative types of messages. This should not detract from all the qualitative messages that need to be conveyed. A good way to start this communication is shown on far right of the figure. It shows the most exposed lines of business and a cumulative level of exposure.

However, it may be the case that some of your more exposed lines of business, in terms of your total non-affirmative exposure as part of your portfolio, do not have a significant number of cyber perils that will impact them. You may then have to clarify which lines are most exposed to cyber perils. There may be other lines where we do not necessarily have confidence in the clauses that are being applied as shown in the figure. Then just above that in the figure, you have a split between

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press



1. Energy Grid Blackout

Overview:
- Limited **power distribution** leads to regional blackouts
- **Large loss and accumulation**: insurers face claims in many lines of business, including large commercial accounts, energy, homeowners, and specialty lines
- **Big BI loss potential** via many triggered policies due to interruption of incoming electricity service (and CBI)

Coverages: **PD, BI, CBI**

Impact: **$20Bn - $70Bn Insured Loss**

Examples:
- Ukraine blackout (2015)
- *University of Cambridge & Lloyd's: US Blackout Scenario*

2. Industrial Plant (ICS)

Overview:
- **Fire / explosion** loss as a result of a targeted hacking incident
- Threat of specifically targeted attacks on industrial control systems (ICS)
- **High aggregation potential**: Risk of attacks on multiple plants by targeting same ICS
- Insurers face potential sizeable claims for fire and explosions at several major industrial facilities

Coverages: **PD, BI,** Third Party, Enviromental damage

Impact: **$500m - $1Bn**

Examples:
- German Steel Mill (2014)
- Triton Malware Attacks (2017)
- Stuxnet/Iranian nuclear power plant (2010)
- *University of Cambridge: Cyber-Induced Explosion in a Chemical Facility Scenario*

3. Machinery Breakdown

Overview:
- New automated technology may lead to increased **machinery breakdown** risks, resulting in large business interruption and delayed / stopped production lines or construction projects and wiped out data
- This may have a significant knock-on effect on the **Supply Chain** structure and cause CBI losses

Coverages: **PD, BI, CBI**

Impact: **Industry Driven (NotPetya $3.3Bn)**

Examples:
- NotPetya / Merck (2017)
- WannaCry (2017)
- Delta airlines outage (2016)

Figure 6. Counterfactual analysis.

what is silent, affirmative and excluded in terms of the risk. That can be useful to show the change in the portfolio over time. To the left of the figure, you have another heat map.

I am going to talk about some silent cyber, real-life scenarios and how they have played out. Figure 6 shows some examples of where these scenarios have occurred and also where others have come up with potential scenarios that could occur. There are three types of scenarios here and they are all focused on operational technology. There is a wide range of scenarios you can come up with: this is not exhaustive. This is just to give you a little bit more of an idea of what non-affirmative cyber risk can look like.

We initially describe the three that we have at a high level. The first one is a risk whereby you have a significant level of downstream business interruption. The next one is where plant machinery is attacked, typically maliciously when this occurs. The last one reflects the fact that more and more of the machinery that is in use has automated operation and therefore there is the potential for machinery breakdown. Typically, that will be non-malicious, but there are examples where that has occurred maliciously.

The first example, energy grid blackout, is reflective of the fact that to take the grid down you do not need to impact the whole grid. You just need to impact some specific points in the grid. The grid is quite susceptible to attack because the evolution of the smart grid means there is a much greater attack surface. This is now being increased further because of solar power installations and homeowners feeding their electricity into the grid, which needs to be managed.

Battery storage facilities are very sensitive to their operating conditions. There are a number of ways in which the grid can be attacked. The energy flow can be disrupted at the production stage and also at the transmission stage. This played out in real life in the Ukraine. Russia was able to disrupt the Ukraine's grid in 2015 and 2016. What saved the Ukraine in both instances, and meant that they were not down for significant lengths of time, was the existence of significant manual controls that existed from the old era to which they were able to switch operations.

Part of what the energy industry has been doing as a result of realising these risks is moving to a situation whereby they can use more of these manual controls. The losses that could occur from an attack on the grid are property damage to the energy infrastructure itself, but also the property damage for everything that is relying on the electricity. It could be as simple an example as refrigeration or a particular process that relies on an uninterrupted power supply. For example, if you

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

are running a steel mill, you end up not being able to control the processes within that steel mill. You can have a significant amount of damage as molten steel hardens within your machinery.

Moving on to the industrial plant side, I am assuming people may not understand the difference between IT systems and operational technology systems. IT is what you use to run your corporate networks. Cybersecurity has long been a high priority there. Operational technology is what you use to run your production environment and typically operational technology would not have been connected to the outside world. The main aim of operational technology was to ensure maximum uptime and reliability as opposed to being secure against risks. If you wanted to disrupt operational technology, you would typically have to obtain physical access to the installation and insert a USB stick into a hard drive or something of that sort. What is happening now is that more and more operational technology is being connected, not always intentionally, to the outside world.

By getting into the corporate IT network, somebody can then move over to the operational technology network and assess what damage they can do. There is the potential for aggregation of risk within industrial control systems. I will temper that by the fact that there are still lots of networks that are not directly linked to the outside world and it does require more effort to get into those networks. The case of NotPetya in 2017 was one in which the IT networks were impacted directly. NotPetya was ransomware and what it wanted to do was disrupt your operations by impacting your computers. Here you would have to first get into the technology network and then into the operational technology network. The operational technology network is one step removed and it is much harder for it to be accessed. If it is accessed, there is the potential for property damage from the loss of energy itself. Both business interruption and bodily injury could occur, for example, if there is a fire or explosion and some or all of the plant is out of action for some time. There is also third-party liability and environmental damage risk. For example, if you think about a water treatment plant, you are mixing chemicals to make sure that the water is treated correctly. If you can get into the network, you can change the way that those chemicals are mixed. It is also possible to tamper with the instrument displays such that they show something different from what is occurring in the water treatment plant.

Machinery breakdown is increasingly important to consider as an outcome of a cyber peril. This is due to the increased automation. An example of a non-malicious problem is the British Airways IT outage, which happened a couple of years ago. A contractor just pulled out a plug unaware of the importance of the system it powered. The Delta Airlines loss was somebody changing some lines of code and uploading it without fully testing it and taking down all their logistics. Then you have the ransomware attacks of 2017 which impacted the ability of systems to function and to control machinery within plant.

I am going to do some acknowledgements before I move on to any questions or comments that people have. I would like to give thanks to members of the Sub-Working Group, especially the Chair, Simon (Cartagena), who took it upon himself to push us to produce these deliverables quickly. The other members are Javir Grewal, Justyna Pikinska and me. Also to the reviewers within the Working Group, Rory (Egan) and Matt (Silley), who provided useful comments in terms of the usability of the framework such that we could enhance it further.

I would like to mention the importance of information sharing. It is a struggle to obtain the right information in terms of cyber perils. There is so much information out there because it is a hot new industry. Everybody wants a voice. What we have done is set up a group called "Cyber Risk + Actuaries". You are more than welcome to join that group. What we try to do there is share any relevant articles that we see and we ask that you share the same if you see any articles that might be use to the wider community. We are also trying to hashtag cyber risk to anything that we see as relevant.

In line with that we are also going to have a Chatham House session at some point, maybe the end of next quarter, for people who use the framework and want to discuss some of what they have

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

found as part of using the framework. You are more than welcome to contact us for an invitation to the session.

The Chairman: The discussion is now open to the floor.

Mr M. G. White, F.I.A.: A few thoughts were prompted starting with something right at the end. I am not willing to join LinkedIn because of personal risks. I am rather worried that the Institute and Faculty of Actuaries (IFoA) is encouraging us to do that.

Now, a couple of specific questions, which go beyond insurance. Firstly, looking ahead to how the cyber world might develop, is there any international punishment framework in the wings for cybercrime?

My second question is about customers. We have been talking from the perspective of the insurer, ensuring your business remains robust after you have understood potential exposures, managed and priced them, etc. Having done this to protect the insurance market, where might that leave the industry's customers? Will there be some gaps that the insurance industry just cannot cope with, such that the customers should be worrying even more than the insurance industry?

Mr Gosrani: In terms of the first question, the biggest problem with cybercrime is that it is difficult to attribute the events to those who may have caused them. It is possible to mask yourself and look like you are somebody else. That is made even worse by the fact that there are arsenals of cyber weapons that are being developed by nation states. Once they have been used, the code can sometimes be left out there and then repurposed such that a cybercriminal can use it for their own ends. If you take the example of the US arsenal that was leaked in 2017, there have been attacks that might look like they were US but actually they have Chinese or North Korean coding styles within them. But, at the same time, all the attributes of the attack might feel like they come from Russia. So that makes it very difficult to attribute blame.

When you move further down the scale in terms of the hobbyist, law enforcement is pursuing those who are at the less-skilled level. The biggest problem is that the skill sets that are needed for cybercriminal activities can be parcelled up. You will go to a particular person for one part of the attack. You will go to somebody else who will provide you another part of the attack.

There is a business environment that has grown up around this. All the participants know how to protect themselves from being identified. The best way is to identify them as a source of a particular skill.

In summary, there is not really a punishment framework. Only the least skilled of the operators are being caught. I cannot offer much optimism that the most sophisticated operators can be successfully targeted. The biggest thing that worries me is the geopolitical element, especially as tensions increase.

Coming onto the second question, the fact that insurers might not be able to provide the products that customers want and therefore customers are left with a protection gap. Part of the problem currently is that customers probably do not realise the extent of the cyber risk that they are facing. It is not so much that it is not possible to buy the products that you want, it is that there is insufficient demand in the market for customers to take those products. Large corporates are covering themselves because otherwise they might be negligent in their duties as a board.

As you move further down the scale towards the mid-market (mid-M) and Small- and Medium-Sized Enterprises (SME) level, it may not be clear to these companies that there is an amount of spending that needs to be done on cybersecurity, but even then there is an amount of cyber risk that you just cannot eliminate. There is some work to do in terms of producing

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

the right products, but there is also some work to do in helping consumers to understand what it is that they need. We need to move closer together.

Mr D. Lamb, F.I.A.: You talked about the first step of the framework being to define the exposure measure that forms the basis. You mentioned using either a maximum probable loss or a notional basis. In your experience, what are the pros and cons of taking one approach versus another.

Mr Gosrani: It depends mainly on the way that your organisation has recorded it in the first place. It may be that one measure is more accessible to your organisation than the other, or that one feels more appropriate to your organisation.

The Chairman: Have you any comments about whether fines are recoverable under such coverages for leakage of data or as regulatory penalties?

Mr Gosrani: If you are thinking about leakage of data, the answer is more on the affirmative. There are moves to ensure that fines are not recoverable under those coverages. The intention is to remove the moral hazard related to the fact that you have insurance to cover yourself if that is a risk. I do not think those initiatives have made their way into legislation at this point. However, there may be fines that result from the impacts on your non-affirmative books. For example, you may have liability to reimburse consumers for losses or for negligence if your product is tampered with and there is harm to customers or to the property of customers.

The Chairman: You mentioned in your presentation about the need for buy-in. From your experience, what do you think are the key factors for making progress in this space?

Mr Gosrani: It depends on what the tone is from the top. Different organisations are placing different levels of importance on the impact that cyber risk could have on them. If the organisation is already concerned about cyber risk, then your Chief Information Security Officer (CISO) and Chief Risk Officer (CRO) are likely to have bought into doing this exercise. You may already have done some form of the exercise. If it is the case that the lines of business that you are writing do not seem to be exposed significantly to cyber risk, you are going to have a harder time. You are going to have to work with the CRO and CIO and potentially CEO to obtain buy-in. It may mean that you have to be less ambitious in your objectives.

Mr White: Assume you are an investor in a company and you want to find out whether your board is well informed about this area. What sort of questions might you ask at the Annual General Meeting (AGM) to challenge them?

Mr Gosrani: One of the issues with cyber risk is that boards do not necessarily know enough to engage with the CISO and ask the right questions to ascertain what they have done to manage the cyber risk of the company. I am not sure that being at the AGM and asking the board about this area would necessarily show that there are gaps in their knowledge. They will have been given assurances that everything is all right and they will have relied upon somebody suitably skilled. There are ways of assessing a company externally in terms of the risks they might have, but the AGM is not going to be the right place to do it. The board itself needs to engage better with the CISO and be able to ask the right questions. There are already initiatives from brokers to try to provide them with suitable questions that have been developed by taking an outside view of the company. It is important to compare compatible companies. For example, it is not very useful to compare, say, a bank to a charity.

https://doi.org/10.1017/S1357321720000124 Published online by Cambridge University Press

The Chairman: In my experience, it depends how you govern underwriting. It depends on the size of the entity, but the underwriting committee at the very least should be conducting some exercises that are looking at stresses and scenarios. In certain contexts, the obvious thing to do is for the non-execs to expect the top three of those scenarios to be brought forward and presented. An important question is, how vulnerable are you operationally to a cyber attack? For this, you can put aside the customer-facing side of things. Another important question is, assuming you have assets to invest, how vulnerable are they to a cyber attack? If you ask those open questions, you will have a rich debate around the board table.

Mr O. F. Whelan, F.I.A.: Most of the discussion has been around malicious attacks, but two of the examples you gave at the end, BA and American, were accidental incidents. Do you think that we are focusing too much on malicious attacks?

Mr Gosrani: A fair amount of the risk is in malicious, but process error has a huge part to play. About 90% of the attacks that take place and impact the operational technology environment end up coming through the IT environment. This is generally because somebody clicks on a phishing link. That in my mind is an attack but it is also a process error because somebody does not determine the intention of the email. They do not identify that it is an email that is inappropriate. There is a lot to do around process and training. In terms of the coding environment, there is a fairly rigorous level of testing of code, but things can still slip through. Given this, it is important to assess what mitigation measures you have in place.

Miss V. J. Jaeger, F.I.A.: Going back to consumers, what should we be doing to improve consumer knowledge about the risks they are facing? I advise pension schemes and there is very little information available, for example, about informing the company about what insurance is available for trustees.

Mr Gosrani: As an industry, possibly we should be doing more. There are lots of other initiatives in place. The National Cyber Security Centre has initiatives around how to better protect yourself and what the risks might be. I do not see many examples portraying situations where losses have occurred and insurance has worked effectively to help a business. These would really bring things to life for a much wider range of people. When you look at the loss databases, there are quite a few losses occurring. They may not be severe but people do not seem to talk about their cyber losses. It obviously does not make for good dinner party conversation. As a result, it seems we underplay the level of risk to which we are exposed. I do not think resolving that issue falls just to the industry. There are wider initiatives and maybe the industry needs to work out how it engages with those initiatives.

I was also going to come back to Martin (White)'s earlier question about what he should be asking at the AGM. Disclosure of cyber incidents is not mandatory. It may be the case that you can ask the question, but they are not obliged to give you the full answer. Asking how they have tested their cyber defences and cyber posture might be a relevant question. Whilst they might not have the right answer, the richness of the answer that they give might show how much they have thought about it.

The Chairman: Thank you, everybody. Tonight we have seen a framework. We have a lot of questions, but they are in a structured form so thank you to you and your team. There are some suggestions for further research and certainly one or two that I will be taking up. The key emphasis for me is getting the risk carrying organisation to think about the possible scenarios. It is a classic underwriting problem. There is a business opportunity out there. However, nobody is going to come along and tell you how you make money out of it and how you provide the service. It is clear in my mind that the underwriting function or governance needs to own this project and topic. It is a business opportunity, but there is a big latency aspect associated with it.

The balance sheet is already exposed to a lot of this risk, even if the organisation does not know it. Now is the time to begin to develop scenarios. The outwards reinsurance side of things is an interesting one. As wordings change, you need to keep on top of the fact that the outwards reinsurance does not necessarily make sure that you do not have any gaps. It is quite a dynamic marketplace, so you need to find a way of being aware of developments. You need to have a process for adjusting your wordings or at least contributing to the industry discussions on any amendments to wordings because that is going to be key. You need some lawyers involved in that internal assessment.

It only remains to thank Visesh (Gosrani) and the Working Party for putting this framework together.

Reference

OECD (2017). Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264282148-en.

Cite this article: Silent cyber assessment framework. *British Actuarial Journal*. https://doi.org/10.1017/S1357321720000124