



DISCUSSION PAPER

Silent cyber assessment framework*

S. Cartagena, V. Gosrani, J. Grewal and J. Pikinska

Abstract

The (re)insurance industry is faced with a growing risk related to the development of information technology (IT). This growth is creating an increasingly digitally interconnected world with more and more dependence being placed on IT systems to manage processes. This is generating opportunities for new insurance products and coverages to directly address the risks that companies face. However, it is also changing the risk landscape of existing classes of business within non-life insurance where there is inherent risk of loss as a result of IT events that cannot be or have not been excluded in policy wordings or are changing the risk profile of traditional risks. This risk of losses to non-cyber classes of business resulting from cyber as a peril that has not been intentionally included (often by not clearly excluding it) is defined as non-affirmative cyber risk, and the level of understanding of this issue and the cyber peril exposure from non-cyber policies varies across the market. In contract wordings, the market has remained relatively “silent” across most lines of business about potential losses resulting from IT-related events, either by not addressing the potential issue or excluding via exclusions. Some classes of business recognise the exposure by use of write-backs. Depending on the line of business, the approach will vary as to how best to turn any “silent” exposure into a known quantity either by robust exclusionary language, pricing or exposure monitoring. This paper proposes a framework to help insurance companies address the issue of non-affirmative cyber risk across their portfolios. Whilst the framework is not intended to be an all-encompassing solution to the issue, it has been developed to help those tasked with addressing the issue to be able to perform a structured analysis of the issue. Each company’s analysis will need to tailor the basis of the framework to fit their structure and underwriting procedures. Ultimately, the framework should be used to help analysts engage with management on this issue so that the risk is understood, and any risk mitigation actions can be taken if required. In the appendix, we present a worked example to illustrate how companies could implement the framework. The example is entirely fictional, is focused on non-life specialty insurance, and is intended only to help demonstrate one possible way in which to apply the framework.

Keywords: Cyber Risk; Silent; Non-Affirmative; Actuarial; Cyber; Risk; Management; Aggregation

Disclaimer

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

*This paper was written by the Institute and Faculty of Actuaries’ Cyber Risk Investigation Working Party. Membership of the contributing authors from the working party is set out below.

© Institute and Faculty of Actuaries 2020. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

1.1 Aims and Terms of Reference

The Cyber Risk Investigation Working Party sits under the Institute's Risk Management Research and Thought Leadership Sub-Committee, which reports into the Risk Management Board of the Institute and Faculty of Actuaries (IFoA). The group was established as a forum for actuaries to share insight and research and to respond to cyber risk developments within the industry.

The working group aims to provide further insight on all areas of cyber risk relevant to actuaries within the life and non-life insurance industry including pricing, reserving, capital calculations and within enterprise risk management. The purpose of this research paper is to suggest a framework to develop actuaries' understanding of their companies' non-affirmative cyber exposure and equip them to engage with management on the issue, so that steps can be taken to better manage the risk from exposures to cyber perils within all lines of business.

1.2 Definition of Cyber Risk

Cyber risk is the risk of any financial loss, disruption or negative reputational impact because of a failure in information technology (IT) systems, whether through people, process or technology. According to the Chief Risk Officer ("CRO") (Forum, 2016), cyber risk covers

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

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

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

"The PRA expects firms to be able to identify, quantify and manage cyber insurance underwriting risk. This includes both of the following sources of cyber insurance underwriting risk:

1. Affirmative cyber risk, i.e. insurance policies that explicitly include coverage for cyber risk; and
2. Non-affirmative cyber risk, i.e. insurance policies that do not explicitly include or exclude coverage for cyber risk. This latter type of cyber risk is sometimes referred to as 'silent' cyber risk by insurance professionals."

It is the assessment of the second of the two sources of cyber risk, non-affirmative, listed above on which this paper is focused.

1.3 Background

Major cyber events continue to make international headlines on a regular, and increasingly frequent, basis. This has seen the topic of cyber security become a significant concern for company boards in recent years moving from an emerging risk to an active risk.

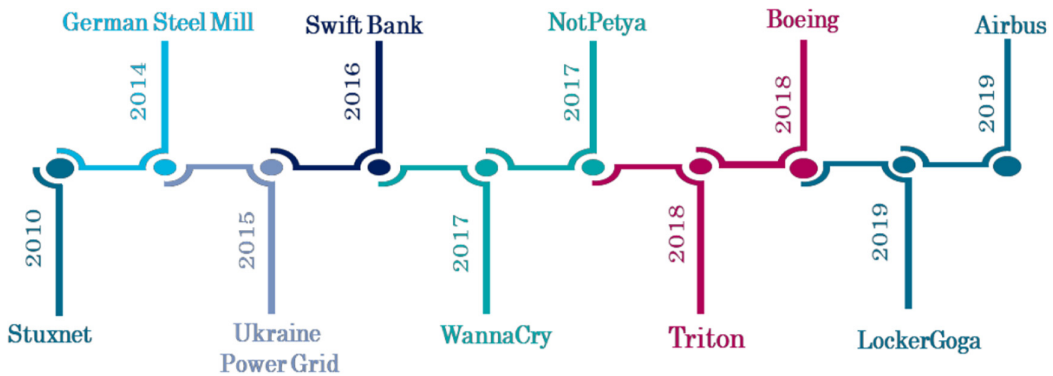


Figure 1. Notable cyber events timeline.

Cyber-attack profiles are not confined to a single geographical region or industry segment. The range and scale of the attack are generally a combination of the intent of the threat actors (e.g. theft/disruption) and the resources available to them (e.g. criminal gangs/state sponsored or lone wolf). The scale of a cyber attack poses a new risk to the insurance industry and the approach to managing accumulations.

Previously, accumulations of risk could be managed predominantly by geography but, as was demonstrated by WannaCry (Symantec, 2017a) and NotPetya (Symantec, 2017b), cyber attacks transcend geographical regions (despite NotPetya being aimed at Ukraine (Marsh, 2018)) and can cause losses across any region and/or industry. In the case of affirmative cyber coverage, companies are able to manage (to an extent) the risk they are underwriting (UW) as this will have been defined within their risk appetite, intentionally covered within a policy and supported by capital. However, cyber attacks have the potential to cause economic losses that trigger claims on non-cyber standalone lines of business. The timeline in Figure 1¹ outlines some known cyber events that have, or have the potential, to cause losses to traditional lines of business.

Following developments within the industry to monitor and manage affirmative cyber exposures over recent years, the insurance market's focus has moved to address the potential of non-affirmative exposure in light of recent events and near misses. The growing awareness of non-affirmative cyber exposure is bringing the need to address the potential exposure to the forefront. This is partly due to the increased awareness of the potential materiality of losses from the events, like those shown above, as well as the increased regulatory activity in this area requiring companies to address this.

2. Non-Affirmative Cyber

2.1 Cyber as a Peril

The term “cyber” is often used in the insurance industry to describe the concept of loss arising from an IT-related event. Such an event can cause loss on policies where the exposure was defined affirmatively, or where the exposure was neither affirmatively included nor excluded.

Many lines of business are now faced with the reality that IT developments are creating a new risk landscape for UW. Developments in IT may generally have a positive effect in reducing the likelihood of an event across many lines of business, for example

- satellite navigation systems enabling semi-automatic ship navigation reducing the risk of manual error;

¹For details and references of the events, please refer to Appendix 4.

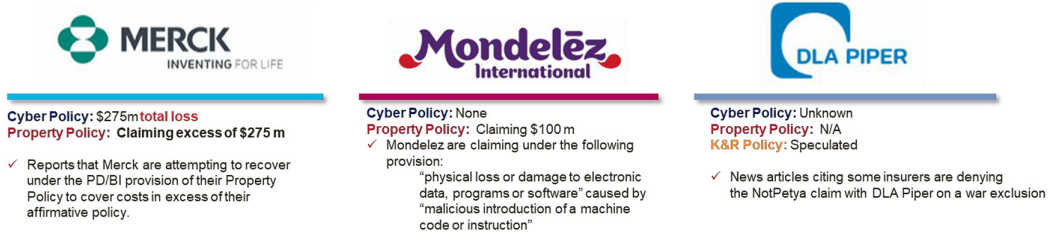


Figure 2. Notable non-affirmative cyber insurance claims.

- Supervisory Control and Data Acquisition (SCADA) systems creating safer working and operating environments for industrial facilities reducing the risk of injury and/or physical damage;
- cloud systems hosting platforms increasing the robustness of availability for companies to conduct business.

However, these developments simultaneously introduce new risks which are not well understood. The IT improvements themselves may introduce a greater systemic risk when failure occurs or drastically increase the event severity due to over-dependence on the system. This is an area that to date has not been well studied. Hence, the concept of considering “cyber as a peril” helps us define the situation where the loss is not concerning the coverage provided on a standalone cyber policy (i.e. data forensics, breach response etc.) but rather the event of physical damage, business interruption, and liability as a result of an IT-related failure that triggers payout on non-cyber lines of business. To a large extent, this risk is not new but is becoming increasingly more important as businesses have a growing dependence on IT systems.

It is also becoming increasingly clear that contract clauses designed to exclude losses resulting from “cyber as a peril” are not as robust as once thought. As these common clauses continue to be tested in the courts, there is growing concern and questions being raised by the market on the reasonability of their use. In Figure 2, we highlight a few events that are causing potential losses to insurance (SC Media, 2019) as a result of cyber attacks. The attacks generally caused disruption to servers and computers at the companies resulting in losses. The exclusions wording on property and other non-life insurance products are being challenged by these companies as they seek to recover losses from these events.

These events are a sample of known events at the time of writing and highlight that for this issue the insurance industry is largely at odds with its client base. When a company seeks insurance to cover the risk, their intention is to cover all financial loss as a result of physical damage. The insured is not concerned by the direct cause but rather the impact the event causes to their financial situation. Hence, as IT-related incidents continue to increase in frequency, one might expect the number of court challenges to continue to increase until more clarity is provided by the market.

2.2 Potential Scale of Silent Cyber

Non-affirmative cyber risk is a very real threat, and recent cyber events have highlighted how it has the potential to threaten the ongoing viability of an organisation; 90% of the Petya/NotPetya industry losses were classed non-affirmative losses (Reinsurance News, 2018).

Risk managers and actuaries should be aware of the various sources of non-affirmative cyber risk in a portfolio of business to ensure that exposures are being adequately priced for, as well as captured appropriately in capital and pricing models. Reputational costs (Mondelez/Zurich) as well as increased regulatory interest (from the PRA and/or Lloyd’s) also need to be considered.

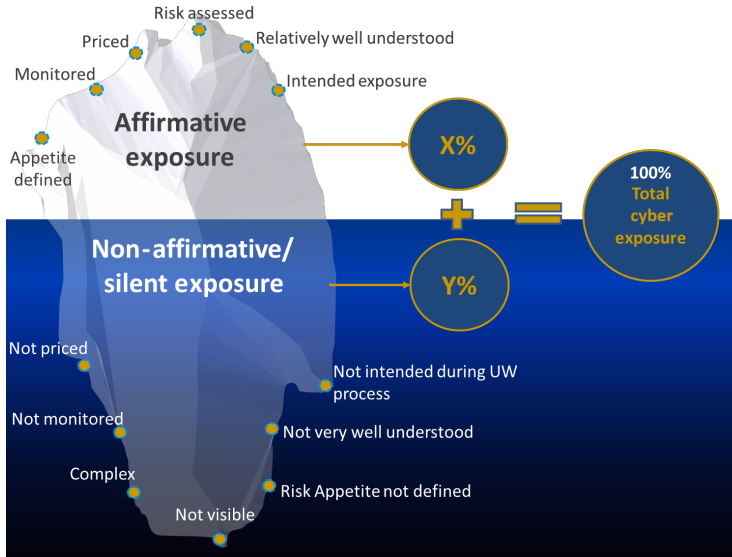


Figure 3. The hidden iceberg of non-affirmative exposure.

One could reasonably expect an entity UW affirmative cyber risks to price, manage and hold capital for the affirmative exposure. Entities at present are less likely to be holding explicit capital for the risk of non-affirmative losses which are the significant but hidden part of the exposure as shown in Figure 3. Hence, given the potential severity of this type of event, entities should ask themselves if a severe cyber event causing non-affirmative losses would constitute a capital event for the company. This will depend primarily on the type of business underwritten and the capitalisation of the company. However, each entity has an obligation to understand and quantify their non-affirmative exposures, where possible, so that the management of the company can take educated decisions on the actions the company should take, based on the risk.

2.3 Regulators View

In January 2019, the PRA published a “Dear CEO” letter re-affirming their expectations of entities in respect of affirmative and non-affirmative cyber (PRA, 2019). The PRA expected companies to be able to demonstrate an understanding and appetite for non-affirmative/silent cyber. These key requirements outlined by the PRA include

- actively managing non-affirmative (“silent”) cyber risk;
- setting clearly defined cyber strategies and risk appetites that are agreed by the board; and
- building and continuously developing insurers’ cyber expertise.

At the time of writing, the European Insurance and Occupational Pensions Authority (“EIOPA”) is also in consultation with companies ahead of releasing a Quarterly Reporting Template (QRT) that would require Solvency 2 regulated entities to report cyber exposures as part of the regular reporting process (EIOPA, 2018). An entity must demonstrate its active management and strategy towards silent cyber to meet the expectations of regulators. Regulators recognise that this is a difficult topic and is committed to overseeing the market as it continues to develop the understanding and monitoring of silent exposures.

Following the July 2019 announcement from Lloyd’s calling for clarity around cyber coverage in all insurance policies (Lloyds of London, 2019), there is expected to be significant change during

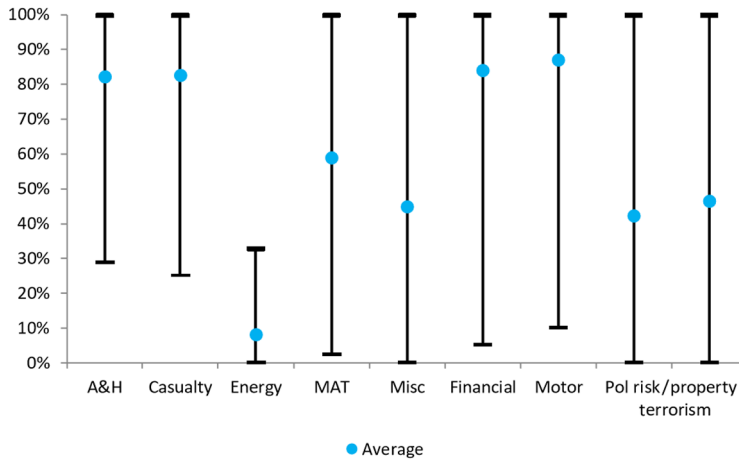


Figure 4. Percentage of total policy limit exposed to non-affirmative cyber risk as assessed by the companies sampled by the PRA review.

the 2020 renewal process for policies incepting 1/1/2020 onwards. The two specific statements made by Lloyd's were as follows:

- "... underwriters are required to ensure that all policies affirm or exclude cyber cover".
- "Define cyber risk as any risk where the losses are cyber-related, arising from either malicious acts (e.g. cyber attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets".

The action by Lloyds is likely to drive greater movement towards reducing contract uncertainty by giving both clients and (re)insurers clarity on what is being insured. The market movement on this will require close attention, particularly when large events occur, including any new clauses brought to the market and any clauses tested by the courts.

2.4 Current Approaches to Assessing Non-Affirmative Cyber

Some entities may have already developed sophisticated approaches to managing and monitoring non-affirmative cyber risk; however, the market remains inconsistent on its view of the "silent" potential in portfolios.

Figure 4 has been taken from one of the PRA's Non-Affirmative Cyber Risk Feedback (PRA, 2019) sessions. It shows the percentage of total policy limit exposed to non-affirmative cyber risk as assessed by the companies sampled by the PRA review. The spread of results illustrates that although firms agree that traditional lines of business have considerable exposure to non-affirmative cyber, views (and perhaps assessment approaches) can vary significantly. Furthermore, one of the PRA's key messages was that "*quantitative assessments of non-affirmative risk*" were not well developed and that "*stress tests suggest cyber events could have widespread impact across different CoBs*".

Responding to this uncertainty, this paper sets out a framework upon which readers can bring consistency to the way non-affirmative exposure is assessed and suggests a process for the subsequent generation of loss scenarios. It provides a common taxonomy to ensure that key aspects of silent cyber risk are considered and sets out examples of how to implement the framework.

Table 1. Common Clauses Used to Address Cyber as a Peril

Reference	Clause Title	Publication Year
LMA5272/3/4/5	Cyber Incident Exclusion	2016
LMA3150	Insurance Act 2015 Endorsement - General Liability	2015
LMA3141	Electronic and Computer Crime Policy	2016
LMA3127	HIP 2015 Policy	2015
LMA3092/30	Terrorism Exclusion (Including Cyber Terrorism)	2006 and 2010
NMA2918	Terrorism Exclusion (Including Cyber Terrorism)	2001
NMA2914/5 NMA2914A/5A	Electronic Data Endorsement	2001 2015
NMA2912/28	IT Hazard Clarification Clause	2010
CL380	The Institute Cyber Attack Exclusion Clause	2003
JSC2015/8	Cyber Attack Exclusion Clause and Write-Back	2015 and 2018
LSW555	Aviation Hull "War and allied perils"	2006
AVN52G	Extended Coverage Endorsement	2001
AVN48B	War/Hijacking and Other Perils Exclusion	1996
AVN124	Data Event Clause	2018
LMA5240	Cyber Loss Exclusion	2015
LMA5241	Cyber Loss Limited Exclusion	2015 and 2018
LMA5327	Cyber Loss Limited Exclusion	2018
LMA5359	Cyber Loss Exclusion	2019
IUA	Cyber Exclusion	2019
IMIA	Cyber Exclusion	2018
JC2019-004	Cyber Coverage Clause	2019

IUA, International Underwriting Association; IMIA, International Association of Engineering Insurers. The clauses listed above include only those known up to the end of September 2019.

3. Clauses

Table 1 outlines some of the common clauses used to address cyber as a peril in the London market. These clauses form the basis of the suggested framework. The framework proposed in this paper requires an understanding of the usage and confidence of wordings across all classes of business. As a reference point, we have included the results of the London Market Association ("LMA") Cyber Risk and Exposures Model Clauses Review (LMA, 2018). It is strongly advised that each individual entity performing such an analysis makes its own assessment which is directly relevant to the nature of the business it writes.

As one performs the review, one may come across broker specific wordings and amendments to standard clauses after speaking to UW and Legal teams. As far as possible, these should be reflected in the analysis if they are being used materially across the business. The wordings themselves are complex and do not all address the same issue. For example, some clauses intend to exclude cyber-induced losses, other are used to make it affirmative ("write-back" cover), while many simply only exclude cyber risks or events under certain situations, for example, malicious versus non-malicious events or physical versus non-physical losses. It is important to develop a company specific understanding of these clauses so that misleading information is not presented to management.

Some of the most common clauses are CL380 (for Marine and Energy) and NMA2914 and NMA2915 (for Property). All of these have come under growing scrutiny in their ability to effectively exclude cyber as a peril. In this paper, we will not discuss the complexities of contract wordings and why there is market debate on this; however, we encourage entities to engage in these discussions and form their own view. Lloyds Market Bulletin Y5258 published 4 July 2019 (Lloyds of London, 2019) was issued in order to ensure that clarity is provided for Lloyd's customers on coverage for cyber exposures. This specifically requires the clarification of whether affirmative provision of cyber coverage is provided from 1/1/2020 for first-party property damage policies and at later dates for liability and treaty reinsurance. Lloyds are engaging in pro-active change to better manage and address cyber as a peril; hence, regular monitoring and assessment of wording may be required until the market and courts are able to form a consensus on robust wordings.

4. Framework

4.1 Overview

This framework has been designed with the primary aim of helping actuaries, and risk managers approach the problem of quantifying and communicating the non-affirmative (silent) cyber risk in their company's portfolio. This has been sourced from the experiences and expertise in the working party. The below outlines the key stages of the proposed framework. Please note that it is not a requirement to perform every step or every detail within each step. The framework shown in Figure 5 is suggested best practice, and a proportionate approach is encouraged.

In the following sections, greater detail is provided on the key areas of the framework with additional information on where different subject matter experts (SMEs) should be consulted to maximise the quality of the analysis performed. The following tables summarise the proposed levels of input from SMEs across the framework using the key shown in Figure 6.

It is important to note that the framework distributed by the working party is populated with market views, and any users must review the appropriateness of all assumptions from their own company's perspective. Furthermore, the cyber risk landscape (whether affirmative or non-affirmative) is ever evolving, and this will result in changes, such as contract wordings, that users should be aware of and respond to accordingly in their analysis.

For additional clarity, a simple example of how the framework may be applied is prepared in an accompanying MS Excel file (see Appendix 3).

4.2 Exposure Assessment

This section of the framework details steps 1 to 4 outlined in Figure 5. This section aims to create a consistent base upon which to calculate a company's exposure and is the main objective of the exercise. The steps are outlined in Table 2, and it is key that UW has input to this stage.

Users should ensure that they do not interpret the data they are seeing incorrectly. Be wary of different classes of business having different data-recording standards across the business that may impact the assessment. Underwriters should be the main contributors and take ownership of the data being used for their class of business. Underwriters are likely to be the main source of the clause usage in their markets, and this should be parametrised in an appropriate and manageable way (see Appendix 1 for suggestion). If granular data on wordings usage are available, this should be prioritised but care taken also to confirm confidence in the data quality. Furthermore, if the company records details of each policy status in their data management systems, with regards to cyber, an assessment of the confidence in that data is important. Particularly, if the data process requires UW and/or technical assistants to record data, they may not be easily able to interpret (unless guidance has been provided).

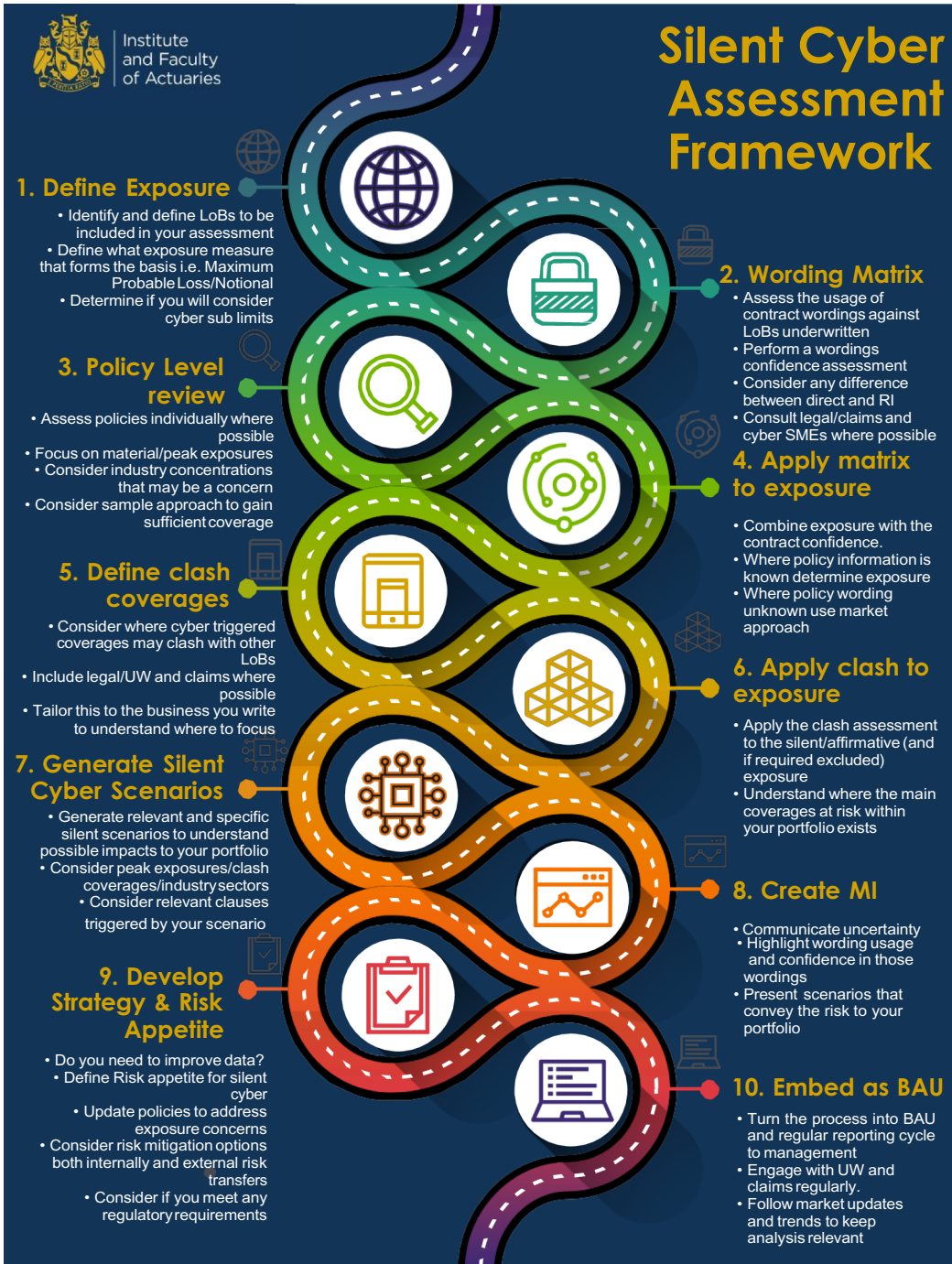


Figure 5. Illustration of the Silent Cyber Assessment Framework.

When performing the assessment of wordings used, users should consult the legal team to form a company's view of the strength of those wordings. This is crucial so that the company is able to form its own view of risk and can communicate this to management. Users may also decide to




SMEs Input Key	
Useful	
Important	
Crucial	

Figure 6. Level of input by SMEs.

consult claims teams to determine if the company has received any non-affirmative claims and how the clauses performed in these situations.

It is important to consider where it may be appropriate to supplement any analysis with specific policy-level assessment. Peak exposures or key lines of business may require additional analysis to confirm policy status, and the framework has been developed with the ability to flag these investigations within the analysis. Determining if peak exposures have clauses and/or sub-limits that contribute to the analysis is an important part of the assessment to be able to provide the clearest view to management.

4.3 Scenario Development

Once exposure has been defined and understood, the next question that many management committees will ask is to what extent they need to be concerned about any significant exposures resulting from the analysis. To do this, the framework proposes performing a scenario generation analysis that seeks to develop scenarios that are relevant to the exposure that has been defined as being at risk to non-affirmative cyber risk. Table 3 summarises the key steps and inputs suggested by this framework.

It is recommended that entities consider where potential coverage clash exists. To do this, they should define the common cyber coverage. This framework has proposed the CRO forum definition in order to construct a working example, but we encourage users to consider the most appropriate for them and consult with all relevant areas of the business. Furthermore, the assessment of where clashes of cyber coverages may be claimed on other classes of business will require discussion with underwriters and their teams as well as claims teams. Once this has been defined, the exposure clashes can be assessed to highlight where there may be areas of concern. It is expected that some organisations may have practical difficulties around obtaining appropriate data depending on how claims root causes/sources are recorded. This may result in changes to data-recording practices in order to capture claims data from cyber perils more appropriately.

Once peak exposures have been assessed, scenarios should then be considered that directly impact these areas. Assessments can be then made as to their potential severity. The assessment of potential silent exposure and potential clash coverages should enable entities to focus their analysis on scenarios that matter to them, enabling them to articulate to management if the exposure is a cause for concern or one that management can be comfortable is well mitigated.

Scenarios should also consider which clauses they could trigger and in turn what the company's confidence in those clauses might be. This will also help the company form a view for management if the exposure at risk is a cause for concern requiring action to help mitigate or control.

We consider this an important step in the framework to help make sense of the analysis performed and contextualise the numbers into a meaningful scenario. We encourage users of the framework to consider bespoke scenarios unique to their business rather than relying on any industry scenarios (although also important to consider) that may not adequately cover the risks they face.

Scenario development can be a detailed process, and companies will have to determine what resources they want to allocate to this area of the framework; however, it can be a very useful tool to communicate risk to management that is directly relevant to companies own exposure and UW experience.

Table 2. The Steps Within the Exposure Assessment Stage

#	Step	Purpose	Area	SMEs Key Input Stage				
				UW	Claims	Legal	Cyber	Management
1	Define exposure	Identify and define LoBs to be included in your assessment Define what exposure measure that forms the basis, that is, maximum probable loss/notional Determine if you will consider cyber sub-limits Determine what the most relevant exposure measure is	Exposure summary	●				
		Populate your policy database with insured contracts across all LoBs. Ensure full coverage is provided either at detailed level or aggregate depending on available data	Policy database	●				
2	Wordings matrix	Assess the usage of contract wordings against LoBs underwritten	Clause matrix	●		●		
		Perform a wordings confidence assessment Consider any difference between direct and RI Consult legal/claims and cyber SMEs where possible	Interpretation	●	●	●	●	
3	Policy-level review	Assess policies individually where possible Focus on material/peak exposures Consider any industry concentrations that may be a concern Consider sample approach to gain sufficient coverage	Policy database	●				
4	Apply matrix to exposure	Combine exposure with the contract confidence Where policy information is known determine exposure Where policy wording is unknown use market approach	Exposure summary	●				

Table 3. The Steps to Develop Scenarios

#	Step	Purpose	Area	SMEs Key Input Stage				
				UW	Claims	Legal	Cyber	Management
5	Define clash coverage	Consider where cyber triggered coverages may clash with other LoBs Include legal/UW and claims where possible Tailor this to the business you write to understand where to focus strategy	Coverages by LoB	●	●	●	●	
6	Apply clash to exposure	Apply the clash assessment to the silent/affirmative (and if required excluded) exposure Understand where the main coverages at risk within your portfolio exists	Exposure by Lob&Cov	●		●		
7	Generate scenarios	Generate relevant and specific silent scenarios to understand possible impacts to your portfolio Consider peak exposures/clash coverages/industry sectors Consider relevant clauses triggered by your scenario	Non-affirmative scenarios	●			●	●

Table 4. Management Reporting and Governance

#	Sheet	Purpose	Area	SMEs Key Input Stage				
				UW	Claims	Legal	Cyber	Management
8	Create MI	Communicate uncertainty Highlight wording usage and confidence in those wordings Present scenarios that convey the risk to your portfolio	Risk reporting	●	●	●	●	●
9	Develop risk appetite and strategy	Do you need to improve data? Define risk appetite for silent cyber Update policies to address exposure concerns Consider risk mitigation options both internally and external risk transfers Consider if you meet any regulatory requirements	Silent scenarios	●			●	●
10	Embed as BAU	Turn the process into BAU and regular reporting cycle to management Engage with UW and claims regularly Follow market updates and trends to keep analysis relevant	Clause confidence	●				●

4.4 Management Reporting

Ultimately, the goal of this framework is to provide actuaries, risk managers or anyone else tasked with articulating to management how they have assessed the company’s non-affirmative cyber exposures a clear and structured process to achieve this. Examples of the output are shown in Table 4.

Simple and transparent management information (MI) packs should be developed in collaboration with all parts of the business. This MI should accurately and fairly represent the analysis and exposure. It is important that users communicate uncertainties in the data and analysis they perform to management. Given the complex nature of this topic, management should be able to understand and interpret output only at a level that is equivalent to level of complexity performed in the analysis. It is important to educate management on the clause strength interpretation so that they are aware that cyber losses may occur even where exclusions are currently being relied upon.

Ultimately, entities are required to develop a risk appetite and strategy going forward to manage their non-affirmative risk. The analysis performed should support this development by creating greater clarity to management so that they may make educated decisions reflecting the analysis performed.

Finally, users of the framework should consider upfront if the analysis performed should be one-off or easily repeatable. A developed risk monitoring strategy would enable the analysis to be performed regularly providing management with updates so that they can continually assess the risk. Consider whether embedding the analysis as a regular process is not possible or not and if this should be raised with management to rectify. This analysis should aim to raise awareness of the risk across the business and provide a regular view of the risk landscape so that if an event occurs entities are able to understand potential sources of loss and plan accordingly. Ultimately, this may lead to market pressures to re-define clauses, structure of reinsurance arrangements, pricing of cyber as a peril and the capital set aside to support the business.

4.5 Limitations

This framework is proposed only as a guideline on how to approach the problem and should not be used blindly as there are many limitations. Some of the key limitations include the following.

- Clauses used in the basis of this framework are subject to change and may be replaced.
- The cyber market is evolving rapidly, and coverages are continuously changing.
- The framework aims only to provide a high-level overview of the risk. Outputs should be interpreted in a consistent manner.
- Any and all data limitations identified will increase the uncertainty inherent in any outputs produced.
- The lack of claims data and the fast-evolving nature of cyber risk results in the need for extensive use of expert judgement.
- The framework provides only a deterministic snapshot in time of the potential silent cyber exposure. The actual range of estimates may vary significantly.

4.6 Level of Application of the Framework

Companies will inevitably be at different stages of their journey in assessing non-affirmative exposures. Hence, the level of use of this framework may vary. Figure 7 illustrates how companies of different maturities may choose to apply this framework.

The use may also depend on companies' availability and quality of data, that is, direct insurers are likely to have greater granularity of data than reinsurers with treaties across various classes of business. There will be value in applying the framework regardless of data quality, but it is important to communicate these additional limitations clearly to management.

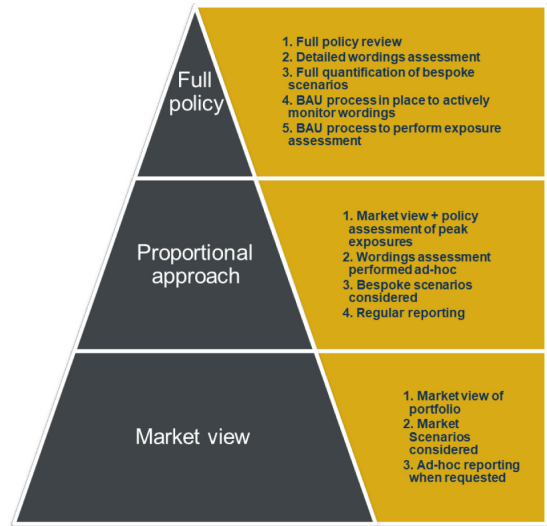


Figure 7. How companies of different maturities may choose to apply the framework.

Acknowledgements. Members from the Cyber Risk Working Party performing peer review of this paper are set out below: Rory Egan and Matthew Silley.

References

- CRO Forum** (2016) CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. Amsterdam: CRO Forum, 28, Concept Paper.
- PRA** (2019). Cyber underwriting risk: follow-up survey results. Bank of England Prudential regulation. January 30, available at <https://www.bankofengland.co.uk/-/media/boe/files/prudential-reghttps://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results>
- Symantec** (2017a). What you need to know about the WannaCry Ransomware. Symantec Security Response. October 23, available at <https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack>
- Symantec** (2017b). Petya ransomware outbreak Here's what you need to know. Symantec Security Response. October 24, available at <https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper>
- Marsh, S.** (2018). US joins UK in blaming Russia for NotPetya cyber-attack. The Guardian. February 15, available at <https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine>
- SC Media** (2019). The Cyber-Security source. SC Media. March 28, available at <https://www.scmagazineuk.com/update-dl-piper-insurance-dispute-nothing-war-exclusion/article/1580426>
- Reinsurance News** (2018). *Petya Cyber Industry Loss Passes \$3bn Driven By Merck & Silent Cyber*: PCS. November 7. <https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/>
- EIOPA. Understanding Cyber Insurance** (2018). A Structured Dialogue with Insurance Companies, <https://eiopa.europa.eu/Publications/Reports/EIOPA%20Understanding%20cyber%20insurance.pdf>
- Lloyds of London** (2019). Providing clarity for Lloyd's customers on coverage for cyber exposures. Market Bulletin Y5258. July 4, available at <https://www.lloyds.com/~media/files/the-market/communications/market-bulletins/2019/07/y5258.pdf>
- London Market Association** (2018). Cyber risks and exposures. Model clauses – Class of business review April, available at <http://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=a22f716a-9437-4ed8-bc24-d59eaea06dce&iFileTypeCode=PDF&iFileName=Cyber%20Report%202018>

Appendix 1

Clause Matrices

This is a pre-populated example of how companies should approach the issue of silent cyber. The LMA review (LMA, 2018) is used as the base of this example. Companies should be mindful to consider how appropriate using this general mapping and parametrisation is for their own analysis. It is strongly advised that companies take their own view that is specific to their business. Figures 8 and 9 can be seen in greater detail in the worksheet “Clause Matrix” of the workbook in Appendix 3.

Wording/Intention	Exclusion	Exclusion	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Affirmative	Affirmative	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	Exclusion	
# LMA Clauses	LMA5272/3/4/5	LMA3150	LMA3141	LMA3127	LMA3092/30	NMA2918	NMA2914/5	NMA2914/5 A	NMA2912/8	CL380	IS2015/8	LSW555	AVN52G	AVN48B	AVN124	LMA5240	LMA5241	LMA5241A	LMA5327	LMA5359	
	Cyber Incident Exclusion	Insurance Act 2015 Endorsement - General Liability	Electronic and Computer Crime Policy	HIP 2015 Policy	Terrorism exclusion (including cyber terrorism)	Terrorism exclusion (including cyber terrorism)	Electronic Data Endorsement	Electronic Data Endorsement (amended)	IT Hazard Clarification Clause	The Institute Cyber Attack Exclusion Clause	Cyber Attack Exclusion Clause and Write-Back	Aviation Hull "War and allied perils"	Extended Coverage Endorsement	War/Hijacking and other perils exclusion	Data Event Clause	Cyber Loss Exclusion	Cyber Loss Limited Exclusion	Cyber Loss Limited Exclusion (amended)	Cyber Loss Limited Exclusion	Cyber Loss Exclusion	
1	Aviation Hull	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	Aviation Liability	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3	Aviation War	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4	Casualty RI	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
5	Contingency	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6	D&O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
7	E&O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	Engineering	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9	Financial - Institutions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
10	General - Liability	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
11	Livestock & Bloodstock	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
12	Marine - Cargo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
13	Marine - Hull	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
14	Marine - Liability	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
15	Marine - War	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
16	Marine - XL	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
17	Motor	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
18	Offshore Energy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
19	Onshore Energy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	Personal - Accident	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
21	Political Risks	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
22	Power Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
23	Property - CB&I	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
24	Property - RI	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
25	Property - UK-Commercial	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
26	Property - UK-Household	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
27	Specie	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
28	Terrorism	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
29	Use of Write-backs	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1	Writeback/coverage of covered peril	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A	War	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
B	Fire/Explosion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
C	Property Damage	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
D	Business Interruption	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
E	Bodily Injury	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
F	N/A	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	Non-Malicious - Exclusion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3	Malicious - Exclusion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Figure 8. Clause matrix example.

#	LMA Classes	LMA5272/3/4/5	LMA3150	LMA3141	LMA3127	LMA3092/30	NMA2918	NMA2914/5	NMA2914/5 A	NMA2912/3	CL380	JS2915/8	LSW555	AVN32G	AVN48B	AVN124	LMA5240	LMA5241	LMA5241A	LMA5327	LMA5359	
1	Aviation Hull															Very High	Unknown					
2	Aviation Liability															Very High	Unknown					
3	Aviation War													Very High	Very High	Very High	Unknown					
4	Casualty RI	Very Low																				
5	Contingency																					
6	D&O																					
7	E&O									Low												
8	Engineering							Very High	Very High													
9	Financial Institutions			Medium																		
10	General Liability		Unknown							Low												Unknown
11	Livestock & Bloodstock									Very High												
12	Marine Cargo									High												
13	Marine Hull									Very High												
14	Marine Liability									Very High												
15	Marine War									High												
16	Marine XL									Low												
17	Motor																					
18	Offshore Energy									Very High												
19	Onshore Energy							High	High	Medium												
20	Personal Accident																					
21	Political Risks									Low												
22	Power Generation							High	High	Low												
23	Property D&F							Very High	Very High													
24	Property RI									Very High												
25	Property UK Commercial																Very Low	Very Low	Very low	Very Low		
26	Property UK Household			Very High				Very High	Very High		Very Low											
27	Specie										Very High	Very High										
28	Terrorism					Medium	High	Low	Low	Low												

Usage band	Up to
Very Low	5%
Low	25%
Medium	50%
High	75%
Very High	100%
Unknown	0%

Figure 9. Clause usage matrix example.

Appendix 2

A Note on Policy-Level Reviews

When performing a review of contract wordings, we strongly advise that legal teams are consulted. The use and interpretation of clauses is not a simple exercise, and the intent of wordings can vary significantly. Generally speaking, a contract (or “slip”) will include all policy terms and conditions relating to the risk. In addition, there will be clauses inserted, and some of these clauses may address cyber as a peril to the risk being insured, that is, insertion of CL380 or NMA2914. When performing analysis of individual risks, the clause needs to be identified, and this may be difficult if contract wordings are scanned and not easily readable/searchable. Hence, we recommend if possible, companies perform a full policy review if proportionate and possible. If this is the case, the need for the assumptions pre-populated in the framework is reduced and greater accuracy can be achieved.

It is our understanding that the insurance market generally has not adopted a philosophy of recording contract wordings in databases at the time of UW. Hence, any policy-level review may not be easily repeatable unless data-recording processes are changed. However, if companies have databased all policy contracts in a data warehouse, they may find it possible to use software that scan documents for specific pieces of text, that is, CL380. However, users should be aware that amendments and broker clauses may be used on risks so it is still very important to include underwriters in any automated assessment.

Ultimately, the choice to undertake a policy-level review will depend on proportionality, company philosophy and available resources. In such cases, the framework may be best applied at the first stage before a full policy review to understand where to focus resources.

Appendix 3

Excel Example of the Framework Applied

An Excel file has also been prepared that shows a simple example of how to apply the framework and should not be considered a template for entities to use with their own exposure. The Excel file is also available via the working party homepage at <https://www.actuaries.org.uk/practice-areas/risk-management/risk-management-research-working-parties/cyber-risk-investigation> with the specific link <https://www.actuaries.org.uk/documents/worked-example-illustrate-how-companies-could-implement-framework>.

It is designed to give users a clear example of how the components of the framework fit together. Hence, this file is populated with random numbers which have no significance and do not reflect any real portfolio of risks. The example is structured as a non-life specialty insurance portfolio, but this does not restrict the usage of the framework. It is intended to be applied to both non-life and life insurances and reinsurances, and users should ensure that they tailor the information within the framework to assist them.

In the “policy database” tab, a simple approach is proposed by which to turn the usage bands defined in sheet “Clause Matrix” into a weighted exposure measure. However, we encourage entities to apply the most appropriate method they see fit to derive their exposure.

Appendix 4

Historical Cyber Event Background

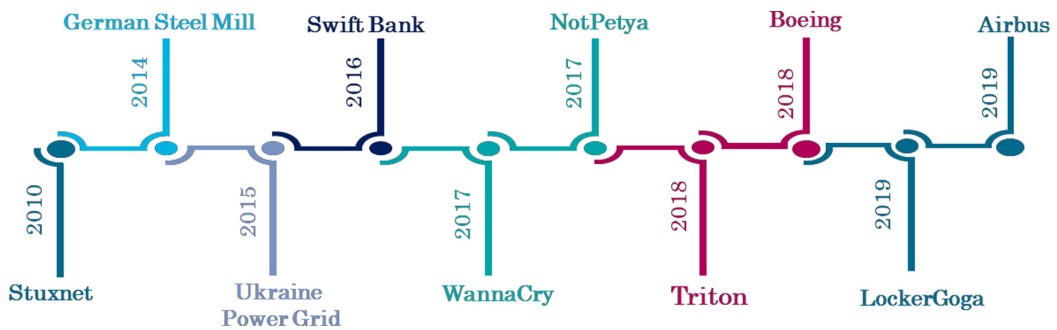


Figure 10. Notable cyber events timeline.

- *Stuxnet*. Stuxnet was a malicious worm targeting SCADA systems. The worm is thought to be the reason for causing significant damage to Iran's nuclear programme. It is widely considered to be a "joint state sponsored attack" (<https://www.bbc.com/timelines/zc6fbk7>).
- *German Steel Mill*. An attack on a steel mill leading to parts failing and the blast furnace malfunctioning causing damage to mill (<https://www.bbc.co.uk/news/technology-30575104>).
- *Ukraine Power Grid*. Power grid targeted by foreign nation causing mass blackouts in Western Ukraine using spear phishing methods (<https://www.bbc.co.uk/news/technology-35,297,464>).
- *Swift Bank*. Attacks using the SWIFT banking network exploited by cyber criminals resulting in millions of dollars stolen. Attack exploited vulnerabilities in bank systems allowing credentials to be obtained (<https://www.bbc.co.uk/news/technology-36129370>).
- *WannaCry*. Worldwide attack using a ransomware targeting Microsoft Windows operating systems. The ransomware encrypted data with a demand for payment in bitcoin to release information (<https://www.bbc.co.uk/news/technology-39901382>).
- *NotPetya*. Worldwide attack using a ransomware targeting Microsoft Windows operating systems. The ransomware infected the operating systems boot record preventing the operating system from booting and demand in bitcoin made to regain access (<https://www.bbc.co.uk/news/technology-40416611>).
- *Triton*. Targeted malware attack on critical infrastructure that was designed to manipulate the security systems. Intention suspected was to cause critical damage to industrial facilities (<https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/>).
- *Boeing*. Reported as potentially an impact of the WannaCry virus Boeings manufacturing equipment was compromised. The attack was contained not severe but potential impact to aviation production was significant (<https://www.bloomberg.com/news/articles/2018-03-28/boeing-hit-by-wannacry-ransomware-attack-seattle-times-says>).
- *LockerGoga*. A recent ransomware that has been detected attacking industrial companies and severely compromising their operations. Reportedly, the cause of the Norsk Hydro aluminium shut attack (<https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/>).
- *Airbus*. An attack on airbus in an attempt to steal intellectual property that came through the supply chain. Suspected that the attack was state sponsored. Attack took place over several months (<https://www.bloomberg.com/news/articles/2019-09-26/airbus-takes-steps-to-counter-cyber-attacks-targeting-suppliers>).

Appendix 5

Glossary

Affirmative cyber	Insurance intended to cover specific or multiple events resulting from cyber perils
BAU	Business as usual
EIOPA	Regulator responsible for prudential oversight at the European Union level
LoB	Line of business
Petya	Petya was ransomware propagated by infected email attachments. It was true ransomware in that payment of the ransom would recover your files
QRT	A reporting template prescribed by EIOPA for use in submitting regulatory returns
Spear phishing	The practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information
MPL	<i>Maximum probable loss</i> . The likely highest loss that would be incurred.
Non-affirmative cyber	The risk of losses to non-cyber classes of business resulting from cyber as a peril that has not been intentionally included, often by not clearly excluding it
NotPetya	Released in June 2017 and had similarities to Petya but used a different vulnerability to propagate. Similarly, to Wannacry, it was disguised as ransomware, rather than actually being ransomware. Its intention was to destroy data
RI	Reinsurance
SCADA	This is a computer system for gathering and analysing real-time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation
Silent Cyber	See non-affirmative cyber
SME	Subject matter expert
UW	Underwriter or Underwriting Department
Wannacry	Released in May 2017 and had similarities to Petya but used a different vulnerability to propagate. Similarly, to NotPetya, it was disguised as ransomware, rather than actually being ransomware. Its intention was to destroy data. It was only stopped due to a kill switch being discovered within its code and activated.
Write-back	Adding back a coverage which has been excluded.