EIOPA report on cyber risk for insurers: Challenges and opportunities

Key findings with respect to cyber risk as an element of an insurer's own operational risk profile

Claire Booth, FIA, CERA
Emma Hutchinson, FIA

Milliman

Introduction

On 17 September 2019, the European Insurance and Occupational Pensions Authority (EIOPA) published a report titled 'Cyber Risk for Insurers – Challenges and Opportunities.' The report assesses cyber risk from both the perspective of insurers providing cyber coverage and the perspective that insurers are susceptible to cyber threats themselves.

Aiming to improve understanding of the vulnerabilities of the European insurance sector towards cyber risk and the challenges facing insurers of this risk in the European cyber insurance market, the paper reports on data gathered from 41 large European insurance and reinsurance groups. Respondents from the United Kingdom include Aviva, Prudential, Legal & General, Standard Life and Royal London, amongst others.

In this paper, we discuss the key findings of the report with respect to cyber risk as an element of an insurer's own operational risk profile, and provide supplementary insight from our own experience of assisting firms in this area. According to EIOPA, insurance groups are key targets for cyberattacks, given the volumes of confidential personal and financial data that they hold, and cyberattacks are likely to result in significant financial impacts, potentially irreversible reputational damage and business interruption. Moreover, the increased use of cloud services by insurers is compounding cyber vulnerabilities for firms.

We will shortly be publishing a second paper covering the report findings that relate to cyber risk as part of underwriting risk.

Defining cyber risk

EIOPA referenced a Financial Stability Board (FSB) Cyber Lexicon definition when it asked participating insurance groups to supply the definition of cyber risk they used. The FSB defines cyber risk as '*the combination of the probability of cyber incidents occurring and their impact*,' while cyber is defined by the FSB as '*relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems*.'

The responses showed that:

- Half of the participating groups used the FSB wording or similar definitions
- Several others used the International Association of Insurance Supervisors (IAIS)[1] definition
- Other definitions of cyber risk differed substantially from the FSB definition and, in some cases, were more aligned with the FSB definition of a cyber incident[2]
- Some groups did not have a definition but stated that they were in the process of developing one

EIOPA recommended that having a shared set of definitions with respect to cyber risk would help insurers, regulators and other stakeholders to have meaningful conversations on cyber risk and thus encourage the development of effective solutions to cybersecurity challenges.

In Milliman's experience, establishing common terminology for cyber risk is an imperative first step to improving the ability of firms to understand, assess, quantify and manage their cyber risk exposures.

One common problem we encounter is the use of the term 'cyber risk' to refer to what in fact is a threat, rather than a risk. The risks caused by cyber threats are of types that are already known—for example, reputational damage, business interruption, theft and fraud. However, the cyber threats themselves happen in ways that firms are not yet good at anticipating.

Clear definition and use of new, cyber risk-related jargon such as 'threat actors,' 'threat vectors' and 'attack surfaces' should help to avoid misinterpretation, confusion and hesitation, and so increase the potential for efficient and effective communications and decision making.

[1] The IAIS definition of cyber risk is "'Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information − be it related to individuals, groups, or governments".' See https://www.iaisweb.org/file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity.

[2] A cyber incident is defined by the FSB as a cyber event that "'(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not".'

Assessing cyber risks

All participating insurance groups bar one provided their own assessments of cyber risk. In terms of how high-risk they rated themselves as a target for cyber threats, 28% of the groups evaluated themselves as high, 63% as medium and 10% as low.

Although it is likely that the groups considered have varying levels of cyber risk exposure and resilience, the discrepancy in responses may also be partly due to the fact that cyber risk is relatively new and complex, and so difficult to accurately assess and quantify.

In particular, with the advancement of technology, interconnectivity and the pathways into firms are growing exponentially. Collateral damage from mass cyberattacks is becoming more likely in addition to direct attacks on individual firms. This makes it very hard for firms to identify and monitor all of their weak points and effectively assess the likelihood and potential consequences of any particular threat hitting them.

Though most companies are conducting assessments and some type of measurement of cyber risk, most still fall short of meaningful quantifications. However, in light of the continued regulatory focus on cyber risk and increasing industry awareness of the need for effective cyber risk management, we anticipate that the market will gradually converge towards standard 'best practice' approaches, which should help to reduce unexplained variances in reported cyber risk exposures over time.

Identification of cyber risks was carried out through a number of methods, although all participating insurance groups used self-assessments. Self-assessments encompassed the use of expert judgement using internal data or, in some cases, quantitative models. The report found that the complexity and number of cyber events used to assess cyber risks varied: for example, some groups only focussed on common types of events such as malware, website defacements, data breaching or denial of service, whereas others considered a wider range of events.

Loss data collection was also used to identify cyber risks: some groups had been collecting data for a long period (more than 10 years), whereas others had collected data for only three or four years. Other identification processes included use of third-party assessments, gap and scenario analysis, inputs from the government and the industry and use of consultants and external experts for cyber defence reviews.

Cyber vulnerabilities

Cyber events (as defined by the FSB[3]) were reported to occur between 0 and 100 times during 2018 for approximately half of the participating insurance groups. For the rest of the sample, figures were in the regions of thousands and up to even billions. EIOPA pointed to the use of different cybersecurity tracking systems, some of which record a narrower definition of events than others, as the reason for the wide-ranging results. This highlights the need for uniform reporting or categorisation of cyber events across firms, in order to make data collection and analysis more effective.

The participating insurance groups reported that between 0% and 50% of cyber events became cyber incidents, with an average of 10% becoming incidents. Notably, the reported average time from occurrence to detection of the incident was under three days. EIOPA considered this a relatively short period of time.

Identifying cyber incidents can be a challenge for firms. Indeed, we have seen a number of cases where firms find out that they were attacked or breached many months, or even years, before they discover it. The unfortunate reality is that most insurers are underprepared for cyberattacks. Although they may have incident identification and response plans in place, these plans are typically not designed with cyber threats in mind nor are they continuously refreshed to reflect the rapid evolution of cyber threats. Therefore, when a real cyber incident occurs, it can often fall through the gaps.

The reported three-day timeframe from occurrence to detection is encouraging and better than what we might have expected in light of the associated challenge. It should be noted, however, that fast detection is a key component in terms of crisis management. Cyber incidents in particular can generate adverse outcomes and ripple through the business extremely rapidly, resulting in large and widespread damage. Therefore timely detection of cyber incidents remains a critical area of focus and improvement for firms.

[3] 'Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.' See https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

Types of cyber incidents

The most common types of cyber incidents noted by the participating insurance groups were:

- Phishing mails
- Malware infections (in particular, ransomware)
- Data exfiltrations
- Distributed denial of service (DDoS)

Malware infections were found to be the most costly incident, closely followed by phishing mails and DDoS. The most frequent problem experienced by the groups as a result of cyber incidents was business interruption, with costs for policyholders and third parties and data destruction and confidentiality breaches also reported as top impacts.

EIOPA, however, drew attention to the fact that cyber threats are constantly evolving and so, to ensure cyber resilience, firms should focus on addressing new, emerging threats beyond those mentioned in its report.

The extent of damages from phishing mails is not unexpected—human vulnerability is often the main vulnerability we encounter for our insurance clients. Firms are only as strong as their weakest links in terms of cyber resilience and so it is of vital importance that all staff across the business are both informed and engaged through continuous training and establishing the right culture, encompassing tone-from-the-top, clear policies and procedures and accountability. Dedicated information technology (IT) support and controls (for example, email filtering) can also go a long way to protecting the business.

As EIOPA says, problematically, cyber threats are dynamic and ever-changing. The sophistication of events reported in the news has dramatically increased in a short space of time, from unsophisticated attacks such as physical theft or payment card skimmers all the way to state-sponsored cyber espionage. With this in mind, rather than looking at what has happened in the past, we recommend that firms regularly consider new and novel ways in which their business objectives could be challenged by incidents involving technology. This should form part of a constant learning process to test and challenge the risk framework and management preparedness for an incident.

Managing cyber risks: Identification, analysis and measurement

Of the participating insurance groups in the EIOPA study, 80% included cyber risk in their Own Risk and Solvency Assessment (ORSA) and 63% explicitly included cyber risk in their Operational Risk Management (ORM) calculations.

In terms of the types of analysis of cyber incidents performed, 52% of the groups conducted stress tests, 23% worst case scenario analysis and 11% multiple scenario analysis. The remaining 14% used analysis such as heat maps, disaster recovery tests, penetration testing and crisis tests. Interestingly, 37% of the groups used only qualitative types of analysis.

We suspect that the high percentage of qualitative analyses reflects the fact that cyber risk is very hard to quantify. There are many connected elements and complexities to account for but not much historical data available on cyber events. Further, as cyber threats are rapidly evolving, the data which is available is usually inappropriate for application to the future. However, without quantification, firms will not be able to define risk appetite, justify cybersecurity spend or meet increasing regulatory expectations.

The quantitative analysis that was performed by the groups typically estimated cyber incident costs such as:

- Crisis management costs
- Legal expenses
- Total operational and financial losses
- Remediation and disaster recovery costs

Additionally, the impact on reputation was considered by some groups and allowance was made for cyber insurance cover where appropriate.

68% of insurers

have insurance for cyber risks.

Whilst the report showed that a large percentage (68%) of firms have insurance for their own cyber risks, it should be noted that use of cyber insurance is not without difficulties. There is often ambiguity over what cyber insurance policies cover, particularly given that the cyber insurance industry is still developing. Moreover, traditional insurance policies have usually been designed without taking into consideration cyber exposures. So-called non-affirmative (also known as 'silent') cyber risks occur when cyber exposures are neither explicitly included nor excluded from a policy.

The reported balance sheet impacts of cyber incidents ranged from €0.2 million to €430 million (0.002% and 10% of the own funds of the groups that provided these estimates). EIOPA explained that the variance of these impacts was in part due to the groups considering cyber incidents of different types and levels of severity.

A small number of groups stated that the balance sheet impact of cyber incidents might not be material. Furthermore, the groups found Solvency Capital Requirement (SCR) impacts difficult to provide, with some simply stating that they calculated operational risk capital based on the Solvency II Standard Formula.

In our experience, where insurers do quantify cyber risk, it is often based on traditional approaches used for other operational risks, such as formulaic assessments resulting in red/amber/green, discrete scenario analysis or simple frequency-severity and catastrophe models. Such approaches are calibrated using historical data and expert judgement. However, as mentioned above, there is not much relevant data on cyber events and, although judgement can be used to adjust models for future appropriateness, this is usually subjective and lacks transparency. Furthermore, traditional approaches fail to properly allow for the nonlinear relationships between cyber risk drivers and the complex relationships among different cyber risk pathways. This makes it difficult for firms to aggregate risks to find an accurate measurement of capital needs.

With this in mind, the inconsistency in reported balance sheet impacts is not surprising—to the extent that insurers continue to use traditional approaches, estimates will be suboptimal at best. To help tackle this issue, Milliman proposes a forward-looking causal approach, which provides an interconnected map of firms' risks and controls and uses this to predict the circumstances that could lead to loss. Importantly, the calibration focuses on the underlying mechanisms of the business, which are easier to understand and quantify than directly estimating the endpoint loss from a particular cyber incident.

Conclusion and next steps

EIOPA concluded that the results of its survey show a general engagement of insurers to work towards ensuring cyber resilience, although it pointed to the need for further action to be taken.

To this aim, EIOPA plans to develop guidelines to define supervisors' expectations on cybersecurity. It also mentioned that the streamlining of cyber incident reporting frameworks could be helpful, though EIOPA made no commitment to initiate such an exercise.

How Milliman can help

Milliman consultants have considerable experience helping firms to develop their cyber risk management frameworks. We are well-placed to benchmark firms' approaches against the rest of the industry, and provide insight and advice that is tailored to your individual circumstances and needs.

We have helped numerous clients introduce robust processes for identifying and assessing cyber risks, ranging from building up a narrative through to the use of new analytical techniques and artificial intelligence (AI).

Our unique cyber risk modelling solution leverages our Complexity-based Risk Analysis (CRisALIS™) platform, allowing firms to quantify and aggregate their cyber risk in a manner that incorporates a dynamic understanding of how the risk behaves. This includes the risks they are exposed to through third parties such as partners, vendors and clients. It can also be used by (re)insurers to enhance their underwriting and pricing for cyber risk, shedding light on the risk and control drivers of each potential loss and giving firms an actionable view of their exposures.

If you have any questions or comments on this paper, cyber risk, or any other aspect of your risk management framework, please contact any of the consultants below or your usual Milliman consultant.

Milliman

CONTACT
Claire Booth
claire.booth@milliman.com

Emma Hutchinson
emma.hutchinson@milliman.com