MILLIMAN BRIEFING NOTE

EIOPA's 2018 Stress Tests: Cyber risk Questionnaire

June 2018

OVERVIEW

On 14 May 2018 the European Insurance and Occupational Pensions Authority (**EIOPA**) launched its fourth stress testing exercise for the European Union (**EU**) insurance sector[1]. The aim of this exercise is to assess the EU insurance market's vulnerability to specific adverse scenarios.

As part of this stress test exercise, EIOPA have included for the first time a 'cyber questionnaire' to ask firms for information on:

- Their perceived exposure to cyber risk (both internal and underwritten); and
- How they manage cyber risk.

As cyber risk increasingly becomes an area of interest and concern for insurers, this questionnaire is included in EIOPA's 2018 stress test exercise to allow EIOPA to identify trends, risks and current approaches to managing cyber risk across the EU insurance sector. The risk of cyber-attack entered the top ten risks in the World Economic Forum's 2012 Global Risk Report, and has been prominent in this list ever since. Moreover, in The Global Risks Report 2018[2] cyber-attacks have risen to third in the top risks by likelihood and sixth in the top risks by impact.

Cyber risk is currently high on many firms' risk registers, and is becoming an increasingly important issue in terms of strategic priorities.

A target group of 42 of the EU's largest insurance and reinsurance groups have been asked to participate in the exercise with the aim of achieving a high level of market coverage of firms as well as a mix of life and non-life business lines. For firms outside of this target group the questionnaire offers a useful reference point when thinking about their own cyber risk management. Some firms may choose to complete the cyber questionnaire as an internal exercise to assess the extent to which their risk management framework currently encompasses the elements referred to in the questions.

Cyber Questionnaire: "a level playing field"

The first section of the cyber risk questionnaire covers the definition of cyber risk, as defined at group level. Participating firms are asked to state the main differences between their internal definitions of cyber risk against the benchmark definition provided by the International Association of Insurance Supervisors (**IAIS**), in a 2016 paper entitled "Issues Paper on Cyber Risk to the Insurance Sector."[3]

The IAIS definition of cyber risk is as follows:

"Cyber risk can be defined as any type of risk emanating 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 − being related to individuals, companies, or governments."

The IAIS definition is broad, with many existing operational risks potentially falling under the scope of this definition. While cyber risk is often associated with new risks that have emerged in a digital age, many risks considered 'cyber risks' are traditional operational risks that have become classified as cyber risks as a result of the increasing integration of technology within firms' systems and processes. Cyber risk is difficult to define and definitions will vary depending on the organisation. Despite this variation, for many firms the risk of a breach of sensitive data is an area of particular concern given the potential reputational consequences and the significant regulatory fines that can be incurred, particularly since the introduction of the General Data Protection Regulation.

Alternative definitions are also mentioned by EIOPA within the stress test technical specifications[4]; these include definitions from the Bank for International Settlements (**BIS**) & the International Organization of Securities Commissions (**OICV-IOSCO**), the Organisation for Economic Co-operation and Development (**OECD**) and the Prudential Regulation Authority

[1] https://eiopa.europa.eu/Pages/Financial-stability-and-crisis-prevention/Stress-test-2018.aspx

[2] The Global Risks Report 2018, 13th Edition. World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[3] http://www.iaisweb.org/page/consultations/closed-consultations/2016/issues-paper-on-cyber-risks-to-the-insurance-sector//file/60062/issues-paper-on-cyber-risk-to-the-insurance-sector-public-consultation

[4] https://eiopa.europa.eu/Publications/Surveys/EIOPA-BOS-18-189_Technical%20Specifications_v20180528_28_05.pdf

(**PRA**). The PRA definition[5] interestingly distinguishes between malicious ('deliberate' attacks) and non-malicious cyber loss events (accidental errors and losses of data).

The aim of this section of the questionnaire is to establish whether there is a "level playing field" among insurers by understanding how cyber risk is defined within the industry. As insurers seek to further leverage the benefits of technology for their businesses the scope of what is considered a 'cyber risk' is expected to widen further still.

Cyber Questionnaire: cyber risk as an element of your own risk profile

In the second section of the cyber risk questionnaire EIOPA asks firms for information on how they manage cyber risks, and assesses the impact of past cyber-attacks on firms by gathering information on the frequency of cyber-attacks experienced by the firms and the level of associated economic loss resulting from those attacks.

Initial questions cover the existing risk management framework for cyber risk, with questions including the following:

- Is cyber risk explicitly part of your operational risk management (**ORM**) policy?
- In your group/company, the risk analysis for cyberattacks is based on: Expert judgement/External data/Both/Other?
- Are you dealing with cyber risk through specific and regular loss collection?
- Are you modelling potential impacts qualitatively or quantitatively, or both?
- Do you include cyber risk in your ORSA scenarios?

These questions seek information on how firms analyse and assess their exposure to cyber risk. Modelling cyber risk robustly can be a challenge for firms due to the evolving nature of the risks and the limited availability of historical cyber risk data. Many firms take a frequency severity approach to modelling their cyber risk, however approaches do vary across the industry. Some firms have focussed on modelling the particular types of cyber risk that they perceive to be most material to their organisation. For other firms capital is not always considered an effective mitigant against cyber loss events and so the focus has been on implementing an effective control environment as well as quantifying a cyber loss event.

The questionnaire also asks for specific details on past cyber-attacks, including:

- The number of identified incidents;
- The number of successful attacks;
- The annual losses caused by attacks; and
- The average time between the attack and identification by the company, in days.

Firms may have different definitions with regards to what constitutes a 'successful' attack, and what comes into the scope of 'losses'. Therefore there is a risk that there is significant inconsistency in the data that is collected from different firms. Moreover, it could be that even in the case of the largest firms, there will be limited experience of cyber incidents and successful attacks.

EIOPA defines a cyber-attack in the context of this questionnaire as only relating to the "deliberate exploitation of computer systems, technology-dependent enterprises and networks". This type of attack will often result in outcomes such as stolen hardware, identity theft, extortion, malware, phishing or system infiltration.

EIOPA also states that any economic losses reported should only include 'immediate' emerging costs and not 'slow burn' costs[6]. 'Immediate' costs are largely unavoidable costs that arise directly after the loss event and include remediation costs, public relations expenses and costs due to the interruption of business.

Costs that are not considered 'immediate' costs (so-called 'slow burn' impacts) typically include long-term business impacts such as regulatory fines, third party litigation expenses, changes in share price, loss of competitive advantage and customer churn from reputational damage. These costs are not to be included in the reported figures in the cyber questionnaire.

EIOPAs omission of 'slow burn' costs might reflect the greater difficultly in quantifying some of these costs compared to 'immediate' costs. For example it might be difficult to exactly assess the extent to which a loss of new business is a result of reputational damage from a specific cyber event, and how long that effect might last. 'Immediate' costs, on the other hand, should be more easily quantifiable as they relate to expenditure carried out to address that cyber event in the short term.

[5] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf?la=en&hash=6F09201D54FFE5D90F3F68C0BF19C368E251AD93

[6] The classification of costs as "immediate" and "slow burn" come from the report Lloyd's (2017) "Closing the gap – insuring your business against evolving cyber threats". Available at: https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap

Respondents are then asked to rank the type of attacks they have experienced firstly in terms of frequency, and secondly in terms of cost. This information will help EIOPA identify the types of attacks that insurers are most vulnerable to, and the ones that are most severe in terms of immediate monetary losses. For each of the attacks listed, respondents are asked to state:

- The type of attack - a choice of either website defacement, website manipulation for distribution of malware, ransomware infection, data theft or 'other'.
- The effect of the above type of attack – a choice of either business interruption, material costs for policyholder information, material costs for third parties or damage to reputation.

In some cases a cyber-attack could result in several, or all, of the above 'effects' and so the wide ranging nature of cyber-attacks may be lost in EIOPA's results. The questionnaire does, however, offer a 'free-form' answer box, in which participants can provide further information on the cyber-attack.

Cyber Questionnaire: cyber risk as a part of underwriting risk

The final section of the questionnaire collects information on firms that underwrite cyber risk. This section of the questionnaire is therefore not relevant for firms that do not participate in this market such as life insurers and retail non-life insurers. This section of the questionnaire collects quantitative information on the number of cyber insurance contracts written, gross premiums written, technical provisions, claims received (both number of claims and monetary amount), combined ratio and the sum of the cyber risk coverage which is reinsured.

The market for cyber risk insurance is rapidly growing; a study by Aon[7] estimates the global cyber market to be worth $2.3bn in premiums, with growth rates in the market amounting to approximately 30% per annum for the years 2011-2015. Despite this, our experience shows that in fact many insurers are failing to take out insurance to cover their cyber risks, based on a perception that tightly worded policy terms will result in a failure to pay out. This is an interesting dilemma for the industry, as insurance has the potential to be a key control for those facing major cyber risks.

EIOPA's questionnaire covers both angles from which a company could be exposed to cyber risk: both through its own internal business exposure as covered in part B of the questionnaire as well as through the underwriting of cyber risk policies as covered in part C of the questionnaire.

Summary

This is the first time EIOPA have asked firms to disclose information about cyber risk as part of their industry stress test. The inclusion of the cyber risk questionnaire in EIOPA's fourth stress test highlights the growing significance of cyber risk for insurers. The results of the 2018 Stress test will be disclosed in an insurance stress test report, due to be published by EIOPA in late January 2019. It is expected that EIOPA will report the results of the cyber questionnaire on an aggregate level in this report. If this is the case, the cyber questionnaire goes some way to improving data availability on the frequency and severity of cyber-attacks and in the first instance, succeeds in opening a conversation on how cyber risk should be defined.

The questionnaire notably doesn't ask firms for details of the mitigation actions and controls they have in place to respond to a successful cyber-attack. It also doesn't cover the types of cyber risk metrics firms are monitoring on a regular basis. Therefore there are additional areas for firms to consider internally when managing cyber risk which are not within the scope of the cyber questionnaire. Despite the omissions in the questionnaire, the findings of this survey should provide useful insight into the EU insurance industry's experience of cyber risk.

How Milliman can help

Our consultants have experience in advising our clients on cyber risk issues and modelling. We undertake a range of work for clients to enable them to develop their cyber risk framework.

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

[7] "Global Cyber Market Overview, uncovering the hidden opportunities", Aon, 2017. Available at: http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

Milliman maintains a strong and growing presence in Europe with 250 professional consultants serving clients from offices in Amsterdam, Brussels, Bucharest, Dublin, Dusseldorf, London, Madrid, Milan, Munich, Paris, Stockholm, Warsaw, and Zurich.

CONTACT

United Kingdom

Jonathan Lim

jonathan.lim@milliman.com

Claire Booth

claire.booth@milliman.com