IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

aii 10 years
access to insurance initiative

Cyber Risk in the Insurance Sector

Report of the A2ii – IAIS Consultation Call

SEP
2019

The Consultation Calls are organised as a partnership between the Access to Insurance Initiative (A2ii) and the International Association of Insurance Supervisors (IAIS) to provide supervisors with a platform to exchange experiences and lessons learnt in expanding access to insurance.

Introduction

Cybersecurity threats are on the rise globally and there is a growing concern over the impact that cybersecurity incidents have on the financial sector as a whole, including the insurance sector. The IAIS Issues Paper on Cyber Risk to the Insurance Sector (IAIS, 2016)[1] stated, "Cyber risk presents a growing challenge for the insurance sector and one which, under the Insurance Core Principles, supervisors are obliged to address. Insurers collect, store, and manage substantial volumes of confidential personal and commercial information. Because of these reservoirs of data, insurers are prime targets for cybercriminals who seek information that can later be used for financial gain through extortion, identity theft, or other criminal activities. In addition, because insurers are significant contributors to the global financial sector, interruptions of insurer's systems due to cybersecurity incidents may have far-reaching implications."

The expert input on this consultation call was prepared and delivered by Marcelo Ramella (Deputy Director, Financial Stability Department at Bermuda Monetary Authority (BMA)) in the Spanish and second English call. Andrea Camargo (Director of Inspowering and Technical Expert of the A2ii) presented the expert inputs in first English call and the French call. Glory Kasasi (Principal Examiner, ICT – Pensions and Insurance Supervision Department, Reserve Bank of Malawi (RBM)), Jennifer McAdam (Senior Counsel, National Association of Insurance Commissioners (NAIC), US) and Marcelo Adrián Borre (Coordinador de Evaluación Normativa, Superintendencia de Seguros de la Nación(SSN), Argentina) joined them to share experiences from their jurisdictions.

1 Available at: https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

Definitions

Cyber attacks are attempts, successful or not, to obtain unauthorised access to information or information systems, in order to steal or alter information or block information systems. Cyber risk is the combination of the probability of a cyber attack occurring, with the damages that a cyber attack may have caused.[2] Cybersecurity, on the other hand, "refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience and recovery activities, and policies regarding the security of an insurer's operations."[3]

Cyber attacks may cause a broad range of damages, ranging from interruption of services and businesses, through to the destruction of data and property, data theft, etc. and up to, potentially, financial instability. Cyber attacks may generate considerable economic damage (the global cost of cyber attacks in 2018 were estimated at USD 800 billion).[4] The financial sector has received comparatively more cyber attacks than other economic sectors.

2 FSB (2018) Cyber Lexicon. Available at https://www.fsb.org/wp-content/uploads/P121118-1.pdf

3 IAIS (2018) Application Paper on Supervision of Insurer Cybersecurity. Available at: https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

4 McAfee (2018) Economic Impact of Cybercrime. Available at: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Cyber Attacks and the Financial Sector

The financial sector is particularly vulnerable to cyber attacks because, among other things, companies have in their possession valuable personal data of consumers as well as financial assets. The report on "The cost of malicious cyber activity to the US economy"[5] highlights cyber events and its distribution across various sectors of the US industry. Among other sectors like healthcare, education, the financial sector has seen the highest number of reported breaches in 2016 relative to its contribution to Gross Domestic Product (GDP) (pp.19–20, Council of Economic Advisers, 2018).

The IAIS Issues Paper on Cyber Risk to the Insurance Sector (2016)[6] states that, "the insurance sector faces cyber risk from both internal and external sources, including through third parties. Insurers collect, process, and store substantial volumes of data, including personally identifiable information. Insurers are connected to other financial institutions through multiple channels, including investment, capital raising, and debt issuance activities. Insurers execute mergers and acquisitions and other changes in corporate structure that may affect cybersecurity. Insurers outsource a variety of services, which may increase, or in some cases decrease, exposure to cyber risk." The Issues Paper highlighted some of the consequences that result from cybersecurity incidents in the insurance sector. These include:

- Loss of confidential data – Insurers are a high target for criminals because of personally identifiable information that they collect.
- Disruption of business – Cyber attacks can disrupt normal business operations and require significant recovery costs.
- Reputational damage – Policyholder trust might be compromised in the event of a cyber attack, where confidential information of policyholders is exposed. Cyber attacks pose a reputational risk that may affect the insurance sector as a whole.

Taking from the report on "The cost of cybercrime"[7] examples were shared as to how the types and costs of cyber attacks may manifest in the insurance sector:

- Analysis done in 11 countries revealed that the insurance and banking sectors continue to have among the highest mean annual cost of cybercrime compared to other industries.[8] The mean annual costs of cyber attacks in the insurance sector was USD 12.93 million in 2017 and USD 15.76 million in 2018 (pp.12, Accenture, 2019).
- In terms of the types of attacks that the financial industry as a whole may experience, malware, web-based attacks, and denial-of-service attacks are the main contributing incidents to revenue loss (pp.17, Accenture, 2019).

5 Available at: https://info.publicintelligence.net/US-MaliciousCyberActivityCost.pdf

6 Available at: https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

7 Available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

8 Compared to insurance, the top 5 industries that continue to have the highest cost of cybercrime out of the 16 industries compared in the report include, banking, utilities, software, automotive and high tech industries (see pp.12, Accenture, 2019)

Regulation and Supervision of Cyber Risk

This section draws upon the IAIS Application Paper on Supervision of Insurer Cybersecurity (2018).[9] A number of international, national and industry organisations in the public and private sector have developed cybersecurity frameworks and guidance that are relevant to insurance supervision. One key source of guidance that insurance supervisors could refer to is the G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE).[10] The G7FE is a concise set of non-binding cybersecurity principles for public and private entities in the financial sector. It is intended to be useful both to firms and supervisors. The eight fundamental elements identified by the G7 are:

1. Cybersecurity Strategy and Framework
2. Governance
3. Risk and Control Assessment
4. Monitoring
5. Response
6. Recovery
7. Information sharing
8. Continuous learning

As per the Application Paper, the eight elements are discussed in the context of insurance and mapped to the relevant ICPs[11] . A brief summary of each element, related ICPs and examples provided on the call are as follows:

G7FE 1 – Cybersecurity Strategy and Framework

This calls for insurers to identify, manage and reduce their cyber risks in an integrated and exhaustive manner. This element of the G7FE is mapped to ICP 8.1, which calls for supervisors to require insurers to set up effective risk management system, and internal control systems that function within this framework. Examples of considerations include:

1. Is there a clear cyber security strategy and framework?
2. Does the cybersecurity strategy and framework determine the insurer's cybersecurity objectives and risk tolerance as well as how it can mitigate and manage its cyber risks?
3. Are cyber risks subject to review under the insurer's cyber security framework? When was the last review?

9 Available at: https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

10 Available at: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

11 All references to specific ICPs in this section are based on the November 2018 version, available at: https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe/file/87203/all-icps-adopted-in-november-2018

G7FE 2 – Governance

This element calls for financial institutions to define the roles and responsibilities of staff required in implementing, managing and supervising the implementation of cybersecurity strategy. Additionally, insurers must provide the necessary resources to implement the cybersecurity strategy and framework. This principle is consistent with ICP 7, which calls for supervisors to require insurers to establish and implement corporate governance frameworks that underpin stable and prudent administration and supervision of insurer activities, and that acknowledge and protect policyholder interests adequately. Examples of considerations include:

1. Does the board and senior management of the insurer participate in cyber security matters of the insurer? E.g. setting a strategy for the insurer, overseeing its cyber risk tolerance
2. Are there clear policies and procedures? Are they applied?
3. Are there sufficient resources to implement policies?
4. What is the cybersecurity budget?

G7FE 3 – Evaluation of Risks and Control

This calls for insurers to have identify functions, activities and services (including outsourced services) subject to cyber risks. Insurers must understand and assess the risks and implement the corresponding controls. This element is consistent with ICP 8, which calls for supervisors to require insurers to "have, as part of its overall corporate governance framework, effective systems of risk management and internal controls". ICP 19.12 calls for supervisors to require insurers and intermediaries to have policies and procedures in place for the protection and use of consumer information. Examples of considerations include:

1. What is the insurer's level of knowledge of their cyber risks? Is there a cyber risk registry? Is it used and updated?
2. Is cyber risk part of the general risk profile of the insurer?
3. Level of protection for consumer information

G7FE 4 – Monitoring

This calls for insurers to have monitoring systems that allows them to quickly detect cyber attacks and they must constantly assess the effectiveness of their controls in place for cyber risks, including cyber attack simulations. This is consistent with ICP 8.1 which calls for supervisors to require insurers to establish effective risk management systems, including early warning and risk response systems. This is also consistent with ICP 8.2, which calls for supervisors to require insurers to have monitoring systems to run regular effectiveness tests.
Examples of considerations include:

1. Are there permanent high-risk activity monitoring systems (e.g. access to confidential information)? Is monitoring done in real time?
2. What is being monitored (e.g. at-risk hardware and software)?
3. Is there evidence of simulations run by the insurer?
4. What use has been made of simulation outcomes?

G7FE 5 and 6 – Response and recovery

This calls for insurers to respond promptly to cyber attacks, taking into consideration the severity of the attack, curtailing its effects, issuing appropriate notifications to whom it may concern, and coordinating and implementing responses that allow them to return to normal operations. ICP 8.1.2 establishes the necessary elements that insurers must take into consideration in order to effectively respond to the materialisation of risks, and in proportion to the materialised risk. Examples of considerations include:

1. What policies and procedures are in place at insurer's end for enhancing awareness of cyber risks (e.g. staff capacity building programmes focused on cyber risks)?
2. Are there explicit plans with detailed descriptions of how to respond to attacks?
3. Are there explicit plans explaining in detail how to return to normal operations?
4. Are there cyber attack notification policies and procedures?
5. What investigations were implemented by the insurer after a cyber attack?

G7FE 7 – Information Sharing

This calls for insurers to provide information on threats, weaknesses, attacks and responses to attacks in order to improve responses to attacks, limit damages, heighten awareness and promote in-house learning. Insurers must provide this information internally and externally, including notifications to government authorities. ICP 8.1.2, particularly the contingency planning requirements, applies to this element. With respect to sharing technical information, ICP 16 (Enterprise Risk Management for Solvency Purposes) provides for the establishing of enterprise risk management requirements for solvency purposes, requiring insurers to address all relevant and material risks. ICP 3, ICP 25 and ICP 26 address the issue of supervisors exchanging information, together with cooperation among supervisors, including cooperation on international crisis management. Examples of considerations include:

1. Does the insurer belong to specialised groups exchanging cyber risk information
2. Does the insurer exchange information with its third-party service providers regarding the cybersecurity framework in order to promote mutual understanding of each other's approach to securing systems that are linked or interfaced.

G7FE 8 – Continuous learning

This element calls for insurers to keep their cyber risk management systems constantly under review, in order to ensure that they keep pace with new cyber risks, while also endowing them with adequate resources. ICP 16.10 calls for supervisors to require the risk management system of insurers to integrate a feedback loop based on appropriate information, management processes and objective assessment that allows them to take the necessary actions in a timely manner, in response to the insurer's risk profile changes. Examples of controls include:

1. Are there indications of the existence of feedback loops in insurer cyber risk management systems? If so, is there evidence that such loops are functioning effectively (e.g. are they being used)?
2. How often are risk management systems reviewed/updated? How exhaustive are these reviews?

CASE STUDY: MALAWI

The Malawi case study was presented by Glory Kasasi from the Reserve Bank of Malawi (RBM)

RBM is the sole regulator of the financial sector in Malawi, including insurance. RBM largely applies a risk-based approach to supervision. An IT landscape survey was conducted among insurers 5 years ago, which showed significant use of information and communications technology (ICT) amongst the insurers including use of management information systems, mobile services and online customer portals. At the national level, cyber regulation comprises of a Cybersecurity Act of 2016 and a National Cyber Security Strategy of 2018. Recognition of cybersecurity at the national level has positively reinforced the work of RBM in addressing cybersecurity issues.

In 2011, RBM issued a risk management directive for insurers. The directive calls for insurers to have effective governance measures, strategies, frameworks, policies and procedures in place for risk management. In addition, RBM has more prescriptive risk management guidelines that provide specific guidelines to financial institutions (banks and pension administrators), specifically to strengthen their IT governance, establish sound and robust technology risk management and to strengthen system security, reliability, resilience and recoverability.

In terms of ICT supervisory tools, RBM uses pre-examination requests, questionnaires containing questions on expected controls used for onsite supervision as well as a questionnaire for IT and risk officers which is under pilot. The weaknesses and challenges that RBM has observed in its market include the following:

- Lack of understanding by some of the insurers on cyber risk
- Currently no overview of the cyber threat landscape for the insurance sector
- Cyber response structure within the RBM is missing
- Absence of formal guidance as to how incidents in regulated institutions should be communicated to other potentially affected divisions within RBM or other relevant authorities in Malawi

Looking ahead on current and future developments, the International Monetary Fund (IMF) bilateral Technical Assistance (TA) mission on Information and Cyber Security Risk Supervision to develop a supervision framework for cyber risk is currently underway. RBM is also updating its IT risk management guidelines for banks to incorporate cyber risk issues. In 2020, Cyber Security Risk Management guidelines will be issued to banks and, subsequently, be adapted to be applicable to all relevant supervised financial institutions. The RBM also plans on formalising a cyber crisis management plan, conducting crisis exercises as well as establishing a cyber incident reporting mechanism for supervised institutions.

For questions or more information on the relevant activities of the RBM, please contact gkasasi@rbm.mw

CASE STUDY: US

The US case study was presented by Jennifer McAdam from the National Association of Insurance Commissioners (NAIC)

The NAIC begun drafting the Data Security Model Law in 2016 and it was adopted by members of the NAIC in October 2017. The NAIC Insurance Data Security Model Law (#668) was developed in response to major data breaches involving large insurers. A massive data breach in one of the largest health insurers, Anthem, was uncovered in 2015, was addressed through multi-state examinations prior to the adoption of the Insurance Data Security Model Law. To address the Anthem data breach, insurance commissioners across the United States collaborated with one another and law enforcement authorities to conduct multi-state examinations to evaluate the Anthem cyber attack and secure consumer data. The examinations oversaw corrective actions that aimed to repair the Anthem systems and prevent future cyber attacks. The collaboration driven multi-state exams formed a starting point for discussions on what kind of model legislation can be used by regulators in dealing with a similar breach in future.

The NAIC model law is consistent with the NYDFS (New York Department of Financial Services), a cybersecurity regulation for financial services companies. The NAIC Data Security Model Law applies to insurers, agents and entities licensed or required to be licensed by the department of insurance. This includes establishing standards for: data security, investigating a "cybersecurity event"; and notifying the state insurance commissioner of any "cybersecurity events". The NYDFS law is more rules-based than the NAIC data security model law which is more principles-based. In addition, the NAIC Data Security Model Law provides additional requirements regarding data security and gives regulators more power to enforce the recommendations that they make to insurers including notifications to the commissioner in case of a cyber event or data breach.

The most significant component of the model law is Section 4, which outlines the requirements of the licensee's Information Security Program:

- Licensee should designate someone to be in charge of the Information Security Program.
- Licensees are required to perform a risk assessment to identify potential threats to the security of their data and the systems in which the data is stored.
- Licensees are required to assess these potential threats on an ongoing basis and to assess the Program annually.
- Licensees are required to mitigate identified risks commensurate with their size and complexity, among other risk factors under the risk management provision.

The NAIC model law is scalable to the size, complexity, and scope of the licensee's activities and licensees can therefore determine which security measures they must take based on its risk assessment. However, there are some requirements which the licensee should meet under the model law:

- Board oversight: The executive management must report to the Board annually, in writing, regarding the overall status and compliance with this law.
- Third-party service providers: The licensee is also required to exercise due diligence when selecting third-party service providers, making sure that those providers also implement appropriate administrative, technical, and physical measures to protect and secure the information systems.
- Other obligations include:
  - The licensee must monitor, evaluate, and adjust its Information Security Program to be consistent with the changes in technology, as well as its own changing business arrangements.
  - The licensee is required to establish a written incident response plan to respond to a cybersecurity event, which should be evaluated and revised if an event does occur.
  - Insurers need to submit a written statement annually, certifying the insurer complies with the requirements set forth in Section 4 of the model law.

In addition, regulators perform on-site examinations to assess the overall financial condition of insurers and this includes an assessment of their IT and cyber risk frameworks. The NAIC Financial Condition Examiners Handbook (Examiners Handbook) provides guidance that state regulators use as part of the financial examination process, and includes a review of whether and how the insurer is addressing its cyber risk. The Examiners Handbook was recently updated to incorporate the National Institute of Standards and Technology (NIST) cybersecurity framework and its five functions: Identify, Protect, Detect, Respond, and Recover.

As of August 2019, the NAIC data security model law has been implemented and adopted in eight states so far. Although the law has not been adopted across all the states in the US, insurance commissioners still have the power to conduct examinations of companies and make recommendations to update their cybersecurity practices.

For questions or more information on the relevant activities of the NAIC, please contact JMcAdam@naic.org

CASE STUDY: ARGENTINA

The Argentina case study was presented by Marcelo Borré from the Superintendencia de Seguros de la Nación (SSN), Argentina

The SSN recently launched an Insurance and InsurTech Innovation Board (or Innovation Hub). The hub brings together different actors in the technology sector and insurance industry to engage in dialogue, in order to promote innovation in the insurance industry. The Innovation Hub is a public-private collaboration space that seeks to create an environment for dialogue regarding the use of technology for the insurance sector. The hub aims to:

- establish a communication channel that will raise awareness of new business models and technologies related to insurance,
- identify regulatory challenges related to risks and opportunities of InsurTechs,
- contribute to the competitiveness of the insurance sector, and
- promote efficiency and competition in the insurance industry.

The SSN is preparing internal guidelines for the operation of the Innovation Hub, which can be modified according to the changes that occur in the InsurTech space. In this regard, the SSN will establish the necessary measures to protect the interests of policyholders, with the adoption of new technologies and ensure the proper functioning of the insurance market.

The SSN recognises that the implementation of the Innovation Hub is of key significance, as it will boost the growth of innovative solutions and technologies for the benefit of the insurance sector and policyholders. Likewise, the Innovation Hub will contribute to compliance with the ICPs, analysing new market behaviours resulting from the issuance of SSN Resolution No. 219/2018 that has allowed issuing of insurance in a digital form.

The Innovation Hub also has a component related to cyber risk, made up of members from insurers, service providers (e.g. BigTechs, software companies), SSN staff, Ministerio de Modernización and cyber risk experts and consultants. Their objectives is to develop good risk management practices and measures to prevent cybercrimes.

For questions or more information on the relevant activities of the SSN, please contact mborre@ssn.gob.ar or mesadeinnovacion@ssn.gob.ar

Questions and Discussion

How do you maintain the balance between managing cyber risk and allowing financial innovation? Both cyber risks and innovation-associated risks are to be considered as distinct as much as related to each other. Insurers have to assess and determine their risk tolerance for cyber threats and their risk appetite for innovation and be clear in their risk statements on how much risk they are prepared to take on, and how are they intend to manage these risks. Supervisors are usually interested on how robust the insurers' risk assessment and management is, the transparency and governance of the process of deciding how much risk an insurer can take on and how to manage it. Ultimately, supervisors should be keen on looking into how much all these commitments are delivered in practice.

How are ICT examinations/examiners structured within authorities? Are there different specialists for different ICT areas? At the RBM, there are three different departments responsible for different areas of supervision. Each department has ICT experts who are responsible for conducting ICT examinations in their area. At the Gibraltar Financial Services Commission (GFSC), the Chief Information Officer (CIO) introduced ICT controls supervision, which is inclusive of cyber, data security, systems controls and governance, business continuity and disaster recovery across all industries. The GFSC has been doing this for over four years. This model has worked for the authority and has formed part of their onsite and supervisory processes, and is also an integral part of their authorisations process.

Are there any past cases of cyber attacks in the insurance sector and how existing frameworks have helped to combat them? In Malawi, the RBM has not been made aware of any specific cyber attacks whether within the insurance or banking industry. However, it is key to have a response mechanism to deal with such attacks. In the US, prior to the adoption of the Insurance Data Security Model Law, the Anthem data breach of 2015 was addressed through collaboration-driven multi-state examinations. State regulators collaborated with the Anthem companies, the Federal Bureau of Investigation, and cybersecurity firms to evaluate the attacks and issue corrective actions.

With respect to interconnected or cross-border cyber threats, how can supervisors set security requirements for cloud supervision[12] to deal with data from different sectors and countries at the same time? Digital technology services, such as cloud technology, are often outsourced. As most of these digital developments are not yet regulated in many countries, supervisors cannot currently rely on cross-border mechanisms. However, it is important for insurers to be aware of existing risks and have proper risk management response frameworks in place.

12 For more information on cloud computing, see the Financial Stability Institute (FSI) paper "Regulating and supervising the clouds: emerging prudential approaches for insurance companies" available at: https:// www.bis.org/fsi/publ/insights13.pdf. The paper was presented on the A2ii-IAIS Consultation Call on 28th November 2019. A report of the call is forthcoming.

How many notifications have been made to NAIC regarding cyber attacks and what are the main issues that delay the adoption of the model law across the different states? Insurers are not required to make notifications to the NAIC, but rather notify the commissioners directly. Currently, data has not been gathered to account for how many notifications have been made regarding cyber attacks. The main challenge in ensuring a uniform adoption of the Data Security Model Law across all US states has been opposition from industry players. However, the law is gradually being adopted across all states.

How can supervisors achieve effective cyber risk supervision in cases where there are no ICT experts within the supervisory authority? There are various possibilities that supervisors can pursue in this regard. The supervisor may rely on external experts where needed, including when the supervisor does not have in-house experts and/or does not have the critical mass or budget to secure in-house expertise. Importantly, the supervisor should be able to assess the soundness of the firm's own management of cyber risk, independent from the "technical knowledge" of cyber risk. An analogy is the supervision of internal actuarial models that insurers use, that supervisors may not be technically able to fully understand. For example, in Canada, the Office of the Superintendent of Financial Institutions (OSFI) is working on a guidance note for the supervision of internal models used to determine regulatory capital requirements (see link http://www.osfi-bsif.gc.ca/Eng/Docs/e25-dft.pdf). The underlying logic also applies to cyber risk.

Implementation Partner:

IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Supported by:

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Ministry of Foreign Affairs of the Netherlands

Hosted by:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Access to Insurance Initiative
Hosted by GIZ Sector Project
Financial Systems Approaches to Insurance
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362
Fax: +49 61 96 79-80 1362
E-mail: secretariat@a2ii.org
Internet: www.a2ii.org

a2ii_org

Promoting access to responsible, inclusive insurance for all.