BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

Insurer cybersecurity – Executive Summary

Cyber risk presents the insurance sector with a growing challenge and one that supervisors need to address. To provide guidance to insurance supervisors seeking to develop or enhance their regulatory regimes and supervisory practices applicable to insurance sector cybersecurity, the International Association of Insurance Supervisors (IAIS) published the *Application Paper on Supervision of Insurer Cybersecurity* in November 2018. This paper follows up the *Issues Paper on Cyber Risk to the Insurance Sector*, published in August 2016.

The Application Paper draws from different cyber security frameworks and guidance developed by international, national and industry organisations, both public and private sector. In particular, it builds on the following guidance: the G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE), the Committee on Payments and Market Infrastructures-Technical Committee of the International Organization of Securities Commissions (CPMI-IOSCO) Guidance on Cyber Resilience for Financial Market Infrastructures, and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (G7FEA).

Supervision of insurer cybersecurity practices

The Application Paper uses as the G7FE as a starting point. It identifies the following fundamental elements of cybersecurity for the financial sector: (1) Cybersecurity Strategy and Framework; (2) Governance; (3) Risk and Control Assessment; (4) Monitoring; (5) Response; (6) Recovery; (7) Information Sharing; and (8) Continuous Learning.

It then analyses how each fundamental element conforms with the Insurance Core Principles (ICPs) and provides a series of recommendations based on the CPMI-IOSCO guidance but presented in an insurance context. The paper then provides examples of current practice in different countries.

Finally, the paper describes the assessment of desirable outcomes for each element, which are based on the G7FEA's five desirable outcomes that a mature entity is likely to exhibit and that less mature entities can aim for. These desirable outcomes are: outcome 1 (O1) – the fundamental elements are in place; O2 – cybersecurity influences organisational decision-making; O3 – there is an understanding that disruption will occur; O4 – an adaptive cybersecurity approach is adopted; and O5 – there is a culture that drives secure behaviour.

The table summarises the main conclusions of the paper and presents some selected examples of recommendations.

Fundamental elements	Mapping to ICPs	Selected examples of recommendations	Out-comes
Cybersecurity strategy and framework	8 (Risk Management and Control)	• Cybersecurity strategy should clearly articulate principles regarding how the insurer intends to address cyber risks. • Cybersecurity framework should clearly define its cybersecurity objectives and horizon, as well as the requirements for people, processes and technology necessary for managing cyber risks.	O1, O2
Governance	7 (Corporate Governance) and 8	• The board should be regularly apprised of the insurer's cyber risk profile. • Senior management should closely manage the insurer's implementation of its cybersecurity framework.	O1, O2

		• The insurer should designate a senior executive to be responsible and accountable for the cybersecurity framework within the organisation.	
Risk and control assessment	8 and 19 (Conduct of Business)	The insurer should: • adequately account for cyber risks in its overall risk management system • describe the overall cyber risk to which the enterprise is exposed • protect data in transit and in storage commensurate with the criticality and classification of the information held • identify the cyber risks that it incurs from and poses to third parties and coordinate with its relevant stakeholders • have appropriate situational awareness of the cyber risks that it faces	O1, O3
Monitoring	8	The insurer should: • employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process • test its cybersecurity framework and communicate the results within its organisation, using a combination of the available methodologies and practices (that is, vulnerability assessment, scenario-based, penetration or red team testing)	O1, O4
Response	8	The insurer should: • have the capability to assist in or conduct forensic investigations of cyber incidents • develop and test response, resumption and recovery plans • have a policy and procedure to meet the disclosure obligations set forth in the laws and regulations of all relevant jurisdictions	O1, O3, O4
Recovery	8	The insurer should: • have in place plans and procedures to recover from a cybersecurity incident • design and test its systems and processes to enable timely recovery of accurate data following a breach • have formal plans for communicating with policyholders and internal and external stakeholders	O1, O3, O4
Information sharing	8, 3 (Information Exchange) and 25 (Supervisory Cooperation and Coordination)	The insurer should: • plan for information sharing through trusted channels, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants • consider engaging with the Financial Services Information Sharing and Analysis Center (FS-ISAC), an acknowledged global resource to the financial sector for cyber and physical threat intelligence analysis and sharing	O1, O5
Continuous learning	8	The insurers should: • implement cyber risk management practices that go beyond reactive controls and include proactive protection against future cyber events • actively monitor technological developments and keep abreast of new cyber risk management processes	O1, O5

Assessing insurers' cybersecurity practices

Jurisdictions may develop supervisory requirements or expectations based on the above recommendations, examples and desirable outcomes. To assess insurers' progress and compliance with the expected cybersecurity outcomes, supervisors need to plan and design effective programmes for conducting cybersecurity assessments.

The Application Paper offers the following "assessment components", based on G7FEA, for insurance supervisors to consider in their assessment programmes:

1. Establish clear assessment objectives and communicate those objectives to insurers
2. Set and communicate methodology and expectations
3. Maintain a diverse toolkit and process for tool selection
4. Report clear findings and concrete remedial expectations
5. Ensure that assessments are both reliable and fair

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.