KPMG Taseer Hadi & Co.
Chartered Accountants

SECP Guidelines on Cybersecurity Framework for the Insurance Sector, 2020

Published on 16 March 2020

Effective from 1 July 2020

Introduction

In times of increasing reliance of the insurance sector on the technology, it has become vital to ensure that the insurer's information technology systems, and of its partners and intermediaries are fully secure from cyber risks.

Securities and Exchange Commission of Pakistan (SECP) issued Guidelines on Cybersecurity Framework for the **Insurance Sector**, 2020 ("Guidelines") for adoption of suitable cybersecurity measures.

Applicability

On **all insurers**, including **takaful operators** registered under the Insurance Ordinance 2000.

Alignment of Cybersecurity Framework with Risk Management Framework

Cyber risk should be a part of risk management policy. **The Chief Information Security Officer ("CISO") and the Risk Management Department** are to jointly develop cybersecurity strategy and framework to mitigate inherent cyber risk.

Developing cybersecurity framework

Insurers to consider existing core technical standards on cybersecurity such as:

- National Institute of Standards and Technology Cybersecurity Framework;
- Information Systems Audit and Control Association's COBIT ("Control Objectives for Information and Related Technologies"); or
- International Organization for Standardization (ISO) 27000 series, which consist of best practices to manage cyber risks.

Appointment of CISO

- Insure will **appoint its senior officer as CISO** who should have **adequate qualification and experience** and will be responsible to implement cybersecurity framework within the organization.
- The insurer within **3 months** of coming into effect of these Guidelines, to **assess whether a separate CISO is required** or not, taking into consideration the inherent risk exposure to the organization.
- **Head of Information Technology Department ("HITD") of Insurer preferably not be appointed as CISO**.
- If HITD and CISO are same person then reporting lines of both the roles are separate.
- CISO to **report to the Board at least once a year**.

Cyber risk assessment

- Implement **annual assessment programs** - to **help the Board and senior management** evaluate the adequacy and effectiveness of the cybersecurity framework.
- **Submit to the Commission - the cybersecurity framework assessment report ('Report")**, by **April 30** of **every year**. Report to be signed by CISO and the Chief Operations Officer/ Chief Executive Officer of the Company.

Data Security and Confidentiality

Cybersecurity framework should be able to **protect the policyholder data**.

Cyber risk insurance coverage

- Consider **cyber risk insurance** to cover cyber risks and mitigate losses from a variety of cyber incidents.
- Requirement for sound control environment still necessary despite purchasing cyber insurance.

Adequate cybersecurity systems

- Adequate **network security and system security** shall be in place to safeguard operating systems, software and databases against the cyber risks.
- **Encryption** at database level, storage level and during network transmission as per the classification and sensitivity of the data.

Cybersecurity Framework

Insurers will formulate a sound cybersecurity framework to anticipate, **detect, prevent and respond to cyber-attacks in line with international standards and best practices**.

➢ Cybersecurity Strategy and Framework

- Cybersecurity strategy should state how the insurer would **mitigate cyber risks** which should be in alignment with cybersecurity framework.
- The framework should promote operational security and **protection of policyholder data**.
- The framework should define its objectives and **requirements for people, processes, and technology** necessary for managing cyber risks and timely communication.
- **Roles and responsibilities of the insurer's Board** and its management should be clearly defined, and it is incumbent upon them to create a **culture** which recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity.
- The framework should clearly articulate a **plan for identification, assessment, measurement, monitoring, mitigation and management of cyber risks**. The insurers should consider how the insurer would **regularly review** and actively mitigate the cyber risks that it bears from and poses to its stakeholders.
- The **framework** should be **reviewed and updated** with sufficient frequency to ensure that they remain effective.

KPMG Taseer Hadi & Co.
Chartered Accountants

SECP Guidelines on Cybersecurity Framework for the Insurance Sector, 2020

Published on 16 March 2020

Effective from 1 July 2020

➢ Governance

- The responsibility for **strategy setting and effective management of cyber risk lies with the Board**. It should be regularly informed of the insurer's cyber risk profile to ensure its consistency with the insurer's risk tolerance as well as the insurer's overall business objectives.
- Insurers will define **roles and responsibilities** for officers **implementing, managing, and overseeing** effectiveness of cybersecurity framework and provide adequate resources, authority, and access to the Board.
- **Board and senior management** should cultivate **awareness** of and commitment to insurer's cybersecurity **at all staff levels**.
- Insurers will create **information security policies**, procedures and processes including oversight of **third-party service providers** and cyber risk management processes.

➢ Risk and Control Assessment

The insurers should:

- Identify and **classify functions** as well as their interconnectedness; proactive technology and processes; external dependency management; and situational awareness.
- Account for cyber risks in its risk management system, identifying and understanding its **business functions** and supporting processes. Such functions and processes should then be **classified by insurers in terms of criticality**, to guide the insurer's prioritization of its protection, detection, response, and recovery efforts.
- Maintain current **inventory of information assets** and system configurations, including interconnections with other internal and external systems.
- Maintain current **record** of both individual and system **access rights**.
- Conduct business **impact analysis** for cyber risks and regularly review and update this
- Ensure their **risk profiles** identify **key operational areas** exposed to cyber risk, arising from both internal and external sources.
- Identify cyber risks in its technologies and connection types; **delivery channels** for products and services; organizational characteristics and external threats.
- **Protect data** both when at-rest, in-transit and in-storage extending to backup systems and offline data stores as well.
- Manage cyber risks presented by third parties and verify that **third-party service providers have implemented appropriate measures to protect and secure the data** of insurer and its customers.
- Have appropriate situational awareness of the cyber risks that it faces and seek to identify cyber threats that could materially affect its ability to provide services or ability to meet its obligations, including protection of confidential data.

➢ Monitoring and Testing

The insurers should:

- Establish monitoring processes to rapidly **detect cyber incidents and periodically evaluate** the effectiveness of controls.
- **Protect network integrity** including control of information flow and network segregation if needed.
- Consider establishing a **Security Operations Centre** or developing similar capability to provide round the clock monitoring.
- Recognize **signs of a potential cyber** incident or detect that an actual breach has taken place.
- **Monitor** internal and external activities to detect vulnerabilities and address **misuse of access by third party service providers**, policyholders and potential insider threats through a strong cyber threat intelligence program.
- Manage identities and credentials for **physical, logical, and remote access to information assets**, based on principles of least privilege and separation of duties.
- Consider placing an effective intrusion **detection capability which may include data loss/leaks prevention and detection**, the recording and documentation of **audit logs**, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.
- Employ **monitoring and detection capabilities** to facilitate its incident response process and support information collection for the forensic investigation process.
- Test all elements of their cybersecurity framework to determine their overall effectiveness before being employed, and regularly thereafter. Proper procedures to be put in place to ensuring **Board and Senior Management are appropriately involved and informed of test results**.
- Consider using a combination of the available **testing methodologies** which may **include** the following elements:
  - **Vulnerability assessments** - to assess security vulnerabilities in the systems and processes.
  - **Scenario-based testing** - to address broad scope of scenarios, including simulation plausible cybersecurity incidents, and should be designed to challenge the assumptions of response and recovery practices.
  - **Penetration testing** - to identify vulnerabilities that may affect insurer's systems, networks, people or processes and to provide an in-depth evaluation of the security of insurers' systems.
  - **Red Team testing** - to challenge organizations and external dependencies and to test for possible vulnerabilities and effectiveness of mitigating controls.

KPMG Taseer Hadi & Co.
Chartered Accountants

SECP Guidelines on Cybersecurity Framework for the Insurance Sector, 2020

Published on 16 March 2020

Effective from 1 July 2020

- **Response testing** - to ensure effectiveness of insurer's response, resumption, and recovery plans and processes.
- **Integrated or Dynamic testing** - to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Testing should include scenarios that cover breaches affecting external dependencies.

➢ Response

The insurers should:

- Implement response and other controls for decision-making responsibilities, procedures, and processes for communicating with internal and external stakeholders.
- Provide **training** for employees and develop response plans.
- Upon detection of cybersecurity incident, **investigate and detect** the extent of damage and take immediate remedial actions.
- **Analyze critical functions**, transactions, and interdependencies to prioritize resumption and recovery actions while remediation efforts continue.
- Plan to access **external experts** on short notice.
- Develop and test response and recovery plans.
- Consider implementing system and process design and controls for critical functions and operations.
- Assist in or conduct **forensic investigations** of cyber incidents.

➢ Recovery

The insurers should:

- Have **validated plans** and procedures to recover from a cybersecurity incident.
- Test their systems and processes to enable timely recovery.
- Work with **third parties** to resume operations in a safe manner where insurer's system and process are interconnected with them.
- Make **formal plans** for **communicating** with policyholders, internal and external stakeholders likely to be affected due to cybersecurity incidents.

➢ Information Sharing

The insurers should:

- Timely **share** cybersecurity information with **all stakeholders** on **incidents.**
- Gather and analyze relevant cyber threat information.
- Ensure that cyber threat intelligence operations include the capability to gather and interpret information about cyber threats from **third-party service providers**.
- Make **cyber threat intelligence** available to appropriate staff to mitigate cyber risks.
- Plan for information-sharing through trusted channels.
- Exchange information with third-party service providers to understand each other's approach to securing systems.

➢ Continuous Learning

The insurers should:

- **Adopt** a **cybersecurity framework** based on continuous security amid changing threat environment.
- **Implement cyber risk management practices** to protect against future cyber events.
- **Capture data** from multiple internal and external sources.
- **Identify key lessons** from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities.
- **Actively monitor technological** developments and remain updated of new cyber risk management processes.

Contact us

Karachi Office
Sheikh Sultan Trust Building No. 2
Beaumont Road
Karachi – 75530
Telephone 92 (21) 3568 5847
Telefax 92 (21) 3568 5095
E-Mail karachi@kpmg.com

Lahore Office
351, Shadman–1
Main Jail Road
Lahore 54000
Phone +92 (42) 111 576 484
Fax +92 (42) 3742 9907
E-Mail lahore@kpmg.com

Islamabad Office
Sixth Floor, State Life Building
Blue Area
Islamabad
Telephone 92 (51) 282 3558
Telefax 92 (51) 282 2671
E-Mail islamabad@kpmg.com

www.kpmg.com.pk