KPMG
cutting through complexity

The SFC – Senior Management's Responsibilities to Mitigate Cyber Security Risks

December 2014

Why is this important?

The Securities and Futures Commission (SFC) released two circulars on 26 and 27 November 2014 aimed at licensed corporations (LCs), focusing on information security management and the mitigation of cyber security risks. The two circulars represent the SFC's third and fourth reminders in the past 12 months on the importance of cyber security. In the new circulars, the SFC highlights senior management's responsibilities under General Principle 9 of the Code of Conduct and Part IV of the Internal Control Guidelines, which clearly state the SFC's expectations regarding senior management's oversight of the integrity, security, availability and reliability of electronic data.

Furthermore, all LCs are required to conduct a self-assessment with a view to preventing, detecting, mitigating and managing the risk of potential loss of their own and investors' information or assets due to cyber attacks, and implementing commensurate controls to address the issues identified. With the SFC's growing scrutiny of cyber security, LCs should consider whether their organisation has adequate controls in place to mitigate the emerging cyber threats.

KEY FOCUS AREAS

1. *Implement policies and procedures to manage cyber security threats*
2. *Identify cyber security risks and vulnerabilities in IT systems*
3. *Enhance controls and technology solutions*
4. *Review cyber security controls of third-party service providers*
5. *Ensure continuity of critical activities and systems*

Leading practices to consider

1

Implement policies and procedures to manage cyber security threats

Many organisations have established information security policies covering traditional IT security controls such as logical and physical access to systems, program changes, program developments, system jobs and incident management. While such policies provide a basic foundation for information security, LCs should consider extending policies and procedures to address today's cyber threats including cyber incident response, log aggregation, threat intelligence and data loss prevention.

2

Identify cyber security risks and assess vulnerabilities in IT systems

LCs should implement effective IT governance and establish an independent IT risk management function to identify and manage cyber security risks in the organisation. The IT risk management function should perform regular risk assessments against the latest regulatory requirements and market leading practices to identify key IT and cyber security risks. Additionally, LCs should regularly appoint qualified parties (internal or external) to conduct comprehensive security penetration testing to simulate real-life cyber attacks to identify vulnerabilities and assess the organisation's security posture.

3

Enhance controls and technology solutions

Based on the findings identified from the risk assessments performed by the IT risk management function, LCs should consider whether additional solutions and tools are required to address any control gaps. Along with the increased regulatory focus on the proper handling of customer data, we have observed an increasing trend among organisations to adopt data leakage prevention solutions. Other common technologies to defend against cyber threats include network intrusion detection systems, log aggregation and analysis systems, anti-distributed denial of service systems, and password management tools.

4

Review cyber security controls of third-party service providers

Many organisations lack visibility over the security of their third-party service providers. For outsourcing arrangements involving the use of technologies, LCs should require that third-party service providers assess cyber security risks pertaining to the services provided and comply with the relevant information security policies and procedures defined by the LCs. LCs should also implement effective controls to monitor and validate the service providers' level of compliance. Such requirements should be specified clearly in the agreements, and regular assessments / audits should be conducted by the LCs to ensure that the service providers comply with the relevant information security requirements.

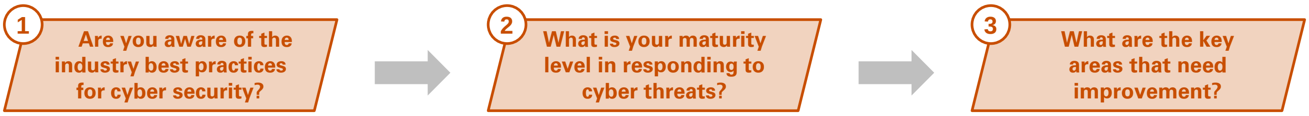
5

Ensure continuity of critical activities and systems

In today's commercial environment, even an hour of down time can lead to significant financial and reputation loss. To protect against system disruptions, LCs should work with the business lines to determine the system availability requirements for each business critical system. Once such availability requirements are defined, a disaster recovery plan should be formulated to ensure the prompt recovery of critical systems in the event of unplanned system disruption or failure. LCs should also continuously monitor the performance of the critical systems and conduct regular disaster recovery drills to ensure that business critical systems can resume in accordance with the defined system availability requirements.

How KPMG can help

KPMG's Cyber Maturity Assessment (CMA) programme can assist you in assessing the maturity level of your organisation to help identify, prevent and manage cyber security risks.



1 Are you aware of the industry best practices for cyber security?

2 What is your maturity level in responding to cyber threats?

3 What are the key areas that need improvement?

Contact us

For more information regarding the regulatory requirements for cyber security, please contact one of our Information Protection and Business Resilience team leaders.

Henry Shek
Partner, Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Kelvin Leung
Senior Manager, Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com

Alvin Li
Senior Manager, Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Sidney Kwong
Manager, Advisory
KPMG China
T: +852 2847 5177
E: sidney.kwong@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.