Dubai Financial Services Authority

Cyber Risk Management Guidelines

December 2020

Table of Contents

INTRODUCTION

These Cyber Risk Management Guidelines (Guidelines) provide information on good practices to assist Firms in:

a) establishing a sound and robust cyber risk management framework; and

b) strengthening system security, reliability, resiliency, and recoverability.

The Guidelines are statements of industry best practices which Firms may adopt, taking into account the complexity of operations and the diversity, scale and scope of business activities in which the Firm engages. The Guidelines are principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. Although we do not prescribe a specific cyber risk framework, we do encourage Firms to implement a framework that is consistent with the eight principles outlined in the *G7 Fundamental Elements of Cybersecurity for the Financial Sector.*

Importantly, the Guidelines are focused on cyber risk[1] management practices and are not intended to address all information and communication technology (ICT) risks and controls. Notwithstanding, a strong ICT control environment is a fundamental and critical component of a Firm's overall cyber resilience. In practice, in the context of cyber risk management, Firms should maintain robust ICT and cyber control environments.

The DFSA will take into consideration in future risk assessments the best practice statements included in these Guidelines.

GOVERNANCE

Cyber risk management framework

1. Firms should implement a cyber risk management framework to provide a structure within which to identify, manage, and mitigate cyber risks effectively in an integrated and comprehensive manner. The cyber risk management framework should be tailored to the Firm's size, complexity, and risk appetite and should be aligned with the Firm's risk management framework.

2. The Firm's cyber risk management framework can be based on the existing industry standards prepared by experts and recognised professional institutions. The more commonly used frameworks/standards include:

    a) ISO/IEC 27000 set of standards;

    b) NIST Cybersecurity Framework;

    c) CIS Critical Security Controls for Effective Cyber Defence; and

    d) CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

[1] Cyber Risk in the context of the financial services sector refers to the operational risks that may result in loss of confidentiality, integrity and availability of data or information; and risk that can negatively impact the information technology (IT) infrastructure or business operations.

These publications may be viewed as benchmarks in developing firm-specific policies, procedures and controls. Firms may adopt a framework prepared by a parent/group entity or use other leading standards, guidelines or recommendations, reflecting current industry best practices in managing cyber risks.

3. Whenever a Firm chooses to adopt one of the above listed frameworks/standards, the Firm should carefully analyse its content and implement only the relevant components. Firms should tailor the guidelines to their needs rather than implement the entire set of practices described in the mentioned publications. Not all of the guidelines may be applicable. Furthermore, additional policies, procedures and controls may be required to address firm-specific risks.
4. The cyber risk management framework should clearly define roles and responsibilities, including accountability for decision making during business-as-usual operations as well as in emergencies and in crisis situations. Individuals assigned with specific roles and responsibilities may delegate tasks to others. However, they remain accountable and should ensure that delegated tasks have been correctly performed.
5. When developing or reviewing its own framework, a Firm should take into consideration the guidelines outlined in this document, as they describe key aspects of cyber risk management.

Cyber risk identification and assessment capabilities

6. Firms should identify cyber risks as a part of the Firm’s overall risk assessment. Firms should determine threats and vulnerabilities to their IT environment which comprises network, hardware, software, systems and interfaces, processes, people, and data.
7. In order to manage cyber risks, Firms should evaluate the inherent cyber risk and the effectiveness of relevant controls to arrive at the residual cyber risk. In addition, Firms should consider, as appropriate, any cyber risks the Firm presents to other counterparties (e.g. business partners, service providers and clients) and the risk such counterparties present to the Firm.
8. Once cyber risks are identified, Firms should perform an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations. Firms should then implement controls appropriate for the criticality and sensitivity of the information system assets and the level of the Firm’s risk appetite. Identified risks and controls should be monitored on an ongoing basis and updated if necessary.

Board and senior management responsibilities and understanding of cyber risks

9. A Firm's Board[2] and senior management are responsible for establishing the cyber risk management framework and ensuring that it is followed and cyber risk is effectively managed. Even if the Firm's IT infrastructure and cybersecurity activities are outsourced to a specialised vendor, the Board and senior management continue to be responsible for cyber risk management oversight.

10. Boards and senior management should define the cyber risk appetite and tolerance for the Firm and should be regularly updated on current and emerging cyber risks and the efficacy of mitigation efforts. For example, senior management should be informed where a key performance indicator signals that a cyber risk control(s) may be underperforming or failing and where a key risk indicator signals an increase in the level of the Firm's cyber risk exposure.

11. Management information should be presented to the Board in a way that can be easily understood and analysed. Also, the Board should have a good understanding of cyber risks and should be regularly updated on current global cyber trends and be included in cybersecurity trainings, cyber awareness campaigns, and other information sharing and similar activities as established by the Firm.

Third-party cyber risk management

12. Firms should address cybersecurity requirements in agreements with third parties which involve accessing, processing, communicating or managing the Firm's data. Firms retain ultimate responsibility for the adequate management of cyber risks for all outsourced operations and data management; therefore, it is incumbent upon Firms to ensure adequate oversight of cyber risk controls is applied by third-party service providers.

13. Firms should address cyber incident notification requirements in agreements with third-party service providers and document collaboration procedures during cyber incident remediation. Firms should receive a timely notification in the event of a cyber incident that may impact the Firm's IT environment in order to assess its impact and launch cyber incident response procedures.

14. Firms should periodically verify that any third-party service providers continue to satisfy the Firm's cybersecurity requirements. This can be achieved, for example, through a review of a third-party control environment or independent audit reports. The frequency and scope of the review should be determined based on the criticality of systems and sensitivity of processed data.

15. Similar procedures should be considered for the subcontractors of third-party service providers where those contractors provide material services. Firms should be aware of

[2] References in the Guidelines to a Firm's Board should be read as including the Firm's board of directors, partners, committee of management, supervisory board or other governing body or person exercising equivalent powers and functions in relation to overseeing and directing the operation of the Firm, as appropriate.

what scope of services is outsourced to subcontractors and what actions were undertaken to mitigate cyber risks by both the third party and its subcontractors.

IT asset identification and classification

16. Firms should identify and classify IT assets based on their criticality and sensitivity in order to ensure that all IT assets receive an appropriate level of protection. Subsequently, Firms should define and apply appropriate controls to secure data according to their level of criticality and sensitivity.

17. Firms should maintain a current inventory of their IT assets in order to know all the assets that support their business functions and processes. Firms should have well-defined processes and clearly assigned responsibility for maintaining the IT asset inventory.

18. The Firm's IT asset inventory should be accurate, up-to-date and reviewed on a periodic basis. The review process should take into consideration the results of the Firm's most recent risk self-assessment and business continuity requirements. The review process should also include an assessment of the interconnections and dependencies between the Firm's IT assets and its business functions and processes.

Cyber training and awareness campaigns

19. Firms should establish a comprehensive cybersecurity training programme and a cyber awareness campaign to enhance the overall cybersecurity awareness level. A training programme should include information on cybersecurity policies and standards as well as individual responsibility in respect of cybersecurity and measures that should be taken to safeguard IT assets.

20. A cybersecurity training programme should be reviewed and updated to ensure that the contents of the programme remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks.

21. All employees (permanent and temporary) should receive training on at least an annual basis to develop and maintain appropriate awareness of, and competencies for detecting and addressing cyber risks. Employees should also be trained on how to report unusual cyber activity and cyber incidents. Such training should be conducted for all new employees within a reasonable period of them joining the Firm.

22. Firms should ensure that all new employees read and understand a Firm's information security policy and/or other relevant policies and procedures that describe information security and cybersecurity requirements.

23. Employees who have privileged access rights (e.g. IT administrators, IT support personnel) should be identified and should receive targeted information security training.

HYGIENE

Anti-malware protection

24. Firms should deploy anti-malware software to servers and workstations. Firms should regularly update anti-malware definition files and schedule regular automatic anti-malware scanning on their servers and workstations.

25. Firms should use anti-malware software to scan any files received over networks (including email attachments and files downloaded from websites) and files kept on storage media before use. The anti-malware software should be used to detect and block malware, potentially malicious links in emails and malicious websites.

Network security

26. Firms should install network security devices (e.g. firewalls, intrusion detection and prevention systems) at critical junctures of their IT infrastructures to protect the network perimeters. Firms should backup and review rules on the network security devices on a regular basis to determine that such rules remain appropriate and relevant.

27. Firms should implement network surveillance and security monitoring procedures with the use of the network security devices to facilitate prompt detection of unauthorised or malicious activities.

Access controls

28. Firms should enforce strong password controls over users' access to systems and networks. Password controls should include a change of password upon first logon, minimum password length and history, password complexity, maximum validity period as well as a lockout threshold after a number of unsuccessful logon attempts.

29. Firms should implement multi-factor authentication (MFA) to all accounts in systems that can be accessed from the Internet. Moreover, MFA should be required for all administrative accounts if it is supported by the systems, regardless of whether they can be accessed from the Internet or through an internal network only. Where a system does not support MFA, the Firm should implement compensating controls.

User access management

30. Firms should only grant access rights and system privileges based on job responsibility. Firms should only allow individuals with proper authorisation to access sensitive information and use system resources solely to perform mandated business activities.

31. Firms should only grant user access to systems and networks according to the 'least privilege' principle and within the minimum period when the access is required. Firms should ensure that the appropriate person authorises and approves all requests to access IT resources.

32. Employees of vendors or service providers, who are given access to the Firm's systems, networks and other computer resources, should be subject to close supervision, monitoring and access restrictions similar to those expected of the Firm's own personnel.

33. Firms should limit access to administrative accounts to authorised IT employees, where possible. Privileged access rights should be allocated to users on an as-needed basis and assigned to a user ID different from those used for regular business activities. The regular business activities should not be performed from privileged user IDs.

34. Firms should immediately revoke user access to systems and networks if it is no longer required. The access rights of employees or third-party users should be removed upon termination of their employment, contract or agreement. Changes of the employment, contract or agreement should be reflected in removal of all access rights that were not approved for a new role or assignment.

35. Firms should perform regular reviews of user access to verify that privileges are granted appropriately and according to the 'least privilege' principle. The process should facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access.

Remote access and mobile devices

36. Remote access to the Firm's IT infrastructure should be properly secured, authorised and approved by an appropriate person. Firms should apply user access management procedures, access controls, including MFA and encryption techniques to secure communication between a remote user and the Firm's infrastructure.

37. Firms should ensure that mobile devices used to access the Firm's systems and data are properly secured. Security requirements, in particular access controls and encryption techniques, applied to the mobile devices should address threats raised by their usage outside the Firm's premises.

Change management

38. Firms should establish a change management process to ensure that changes and patches to production systems and hardware devices are assessed, tested, approved and implemented in a controlled manner. The change management process should explicitly consider cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created post-change.

39. Firms should establish separate physical or logical environments for systems development, testing and production.

40. Firms should adequately test the impending changes on the test environment and ensure that test results are accepted by appropriate business and/or IT personnel prior to the migration to the production environment.

41. All changes should be approved prior to the migration to the production environment by appropriate business and/or IT personnel with the authority to approve change requests.

42. Firms should enforce segregation of duties so that no single individual has the ability to develop, test and implement the change to the production environment.

43. Firms should implement an emergency change process to enable quick implementation of changes needed to resolve major incidents (e.g. system malfunctions affecting business continuity, critical security vulnerabilities). While the emergency change should be implemented in a controlled manner, the process requires swift actions and decisions; therefore, some aspects of the change management process (e.g. change documentation, thorough testing) can be completed after the emergency change is implemented on an exceptional basis.

Patch management

44. Firms should establish patch management procedures including the identification, categorisation and prioritisation of security patches. Firms should implement security patches to systems, hardware devices and workstations in a timely manner.

45. Firms should implement security patches according to the change management process, as a standard change or an emergency change, depending on how urgently a vulnerability needs to be addressed.

Backup management

46. Firms should implement backup procedures for critical systems and data. All critical system images and data should be backed up regularly and backup copies should be retained for a required period of time, as determined by the Firm.

47. Firms should carry out periodic testing and validation of the recovery capability of the backup copies and assess if backup media (e.g. tapes, disks, including USB disks) are adequate and sufficiently effective to support the Firm's recovery process.

48. Firms should encrypt all backup copies containing sensitive information before they are transported offsite for storage. The backup media should be given an appropriate level of physical and environmental protection.

Encryption

49. Firms should implement encryption techniques to protect sensitive information stored on workstation hard drives and portable storage media. The use of encryption techniques should be commensurate with the level of criticality and sensitivity of data. In particular, this is relevant to workstation hard drives, external drives such as USB pen drives, external hard disks, mobile phones, tablets and similar electronic equipment used to store or process critical and sensitive data.

50. For the purpose of exchanging sensitive information between a Firm and external parties, the Firm should implement measures to preserve data confidentiality. For this purpose, the Firm should at all times take appropriate measures, including sending information through encrypted channels or encrypting the exchanged sensitive information using strong encryption with adequate key length.

Physical security

51. Firms should limit access to datacentres and server rooms to authorised personnel only. Firms should only grant access to the datacentres and the server rooms on an as-needed basis. Physical access to the datacentres and the server rooms should be revoked immediately once it is no longer required.

52. For vendors, system administrators or engineers, who may require temporary access to the datacentres and the server rooms to perform maintenance or repair work, Firms should ensure that there is proper notification of and approval for such personnel for visits and activities. Firms should ensure that visitors are accompanied at all times by an authorised employee while in the datacentres or the server rooms.

53. Firms should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the datacentres and the server rooms. Firms should establish physical security measures to prevent unauthorised access to systems and computer equipment.

Cybersecurity testing

54. Firms should use a variety of methods to periodically test IT infrastructure and systems, including vulnerability assessments, scenario-based testing, penetration tests and/or red team exercises, depending on the results of the Firm’s cyber risk assessment.

55. Cybersecurity testing of internet-facing systems should be conducted regularly and whenever systems are updated or deployed.

56. Where the maintenance of the systems has been outsourced to a third-party service provider, it is the Firm’s responsibility to ensure that the vendor’s systems are tested periodically. Firms may perform tests themselves or consider reliance on testing performed by third party service providers. Also, Firms may take into consideration, and rely on, test results delivered by independent auditors.

57. Firms should establish a process to prioritise and remedy adverse testing outcomes. Subsequently, Firms should conduct follow up tests to assess whether identified gaps have been fully addressed. Further testing should be done on an ongoing basis to identify and eliminate new vulnerabilities.

RESILIENCE

Continuous monitoring and detection capabilities

58. Firms should apply ongoing monitoring of their IT infrastructure to detect the occurrence of anomalies and events indicating a potential cyber incident. Early detection provides Firms with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches.
59. Firms should regularly review system logs recording user activities, warnings, errors and security events to identify suspicious activities and system errors indicating a potential cyber incident.
60. Firms should develop a process for reporting potential cybersecurity incidents and define a point of contact to which the events should be reported. All employees and contractors should be made aware of their responsibility to report potential cybersecurity incidents as quickly as possible.

Cyber incident response planning and preparation

61. Firms should implement a robust cyber incident response plan that, at a minimum, contains the following:
    a) procedures for detecting, monitoring, analysing and responding to cyber incidents;
    b) definitions of incident management roles and responsibilities;
    c) an internal communication plan that includes communication protocols for key internal stakeholders (e.g. relevant business units, senior management, the Board);
    d) an external communication plan that includes communication protocols for key external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement);
    e) a recovery plan and/or references to a disaster recovery plan;
    f) procedures for post-incident review; and
    g) cyber incident response plan periodic testing requirements.
62. The cyber incident response plan should be approved by senior management and the Board. As cyber risks evolve, the plan should be modified, adjusted and tested on a regular basis. The response plan should be updated based on current cyber threat intelligence as well as lessons learned from previous events, and adjusted to account for new processes and services.
63. Firms should plan in advance for communications with internal and external stakeholders and should prepare pre-approved communication templates relating to identified scenarios that can be easily adjusted (if required) and promptly released in case of a cyber incident. The communication plans may be developed to address a range of possible scenarios, taking into consideration experiences from previous incidents.

64. Procedures described in the plan should be periodically tested to determine their overall effectiveness, identify potential gaps that should be addressed and identify parts that require updates. Tests may be conducted in different forms (e.g. a table-top exercise, simulations) and the appropriate scope of testing should be determined each time a test is planned. While Firms may decide to test only selected procedures at one time, they should ensure that all aspects of the cyber incident response plan are tested on a regular basis. Testing requirements should be specified in the cyber incident response plan.

Cyber incident response and recovery

65. Upon detection of a potential cyberattack, Firms should perform an analysis to determine the nature and extent of the attack. While the analysis is ongoing, Firms should also take immediate actions to contain the attack to prevent further damage, and launch recovery processes to restore operations based on their cyber incident response plan.

66. Firms should resume operations responsibly, while allowing for continued remediation, by:

    a) eliminating remaining harmful effects of a cyber incident;

    b) restoring systems and data to normal state;

    c) identifying and mitigating all vulnerabilities that were exploited;

    d) remediating vulnerabilities to prevent similar cyber incidents; and

    e) communicating appropriately internally and externally.

67. Firms should ensure that cyber incident response and recovery processes are closely integrated with crisis management, business continuity and disaster recovery planning, and also coordinated with relevant internal and external stakeholders.

68. After the closure of a cyber incident, Firms should analyse whether established procedures were followed and whether the actions taken were effective. Firms should identify key lessons from the cyber event in order to improve future cyber incident response and recovery processes.

Cyber incident notification

69. Firms should provide the DFSA with consistent and timely information regarding material cyber incidents. Firms are strongly encouraged to submit the initial notification to the DFSA via the DFSA ePortal as promptly as possible, and within 72 hours of detection of the incident. A cyber incident is considered a material cyber incident if it causes any of the following losses:

    a) impact to client data and/or client assets;

    b) leakage of sensitive information;

    c) disruption to critical business function(s) and/or critical information system(s);

    d) significant operational impact to internal users that is material to clients or business operations;

    e) material financial loss;

f) where it is believed the root cause of the incident, and/or the incident itself, may impact external stakeholders such that there is concern of systemic risk to the Dubai International Financial Centre (DIFC), Dubai and/or the United Arab Emirates; or

g) negative reputational impact is imminent (e.g. public/media disclosure).

70. Firms should have procedures in place to determine whether a cyber incident should be reported to other regulatory bodies and external stakeholders (e.g. regulators/authorities, law enforcement, clients, DIFC Commissioner of Data Protection, vendors, media, other stakeholders).

Information sharing

71. Firms are strongly encouraged to participate in threat intelligence sharing communities, whether through intelligence sharing platforms, professional forums, or other information sharing communities, to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats to improve their cyber response and remain up-to-date in their defences. The DFSA launched the DFSA Threat Intelligence Platform (TIP) to enable Firms to cooperate and share information about cyber threats. Firms are encouraged to register with the DFSA TIP via the DFSA ePortal.

72. Firms should identify opportunities for improvements to their cyber incident response and recovery processes from various sources: cyber publications; reports on the cyber incidents; information sharing and discussions between peers; trend and threat analysis; regulatory and supervisory initiatives; and cyber risk management best practices.