ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

Governance Principles and Practices to Mitigate Cyber Threats and Crime

FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

ADGM Authorities Building, ADGM Square, Al Maryah Island, PO Box 111999, Abu Dhabi, UAE
مبنى سلطات سوق أبوظبي العالمي، مربعة سوق أبوظبي العالمي، جزيرة الماريه، ص ب 111999، أبوظبي، الإمارات العربية المتحدة

T +971 2 333 8888 adgm.com

Contents

Background and Purpose

As a regulator, we are consistently striving to deepen our understanding of the inherent and emerging risks that may impact our regulated community. In keeping with the pace of change, amidst aspects of increased technological complexity, a fundamental emphasis is placed on our responsibility to promote the adoption of policies and practices that aim to create stable and safe financial ecosystems that are responsive change. As a driver for innovation, productivity and growth, the FSRA acknowledges that the increased reliance on technology has exposed financial institutions to new digital vulnerabilities for financial crime purposes. Digital security incidents, in the form of cybercrime activities, could have far-reaching consequences for Firms. By way of example, the breach of customer information or trade secrets could lead to financial loss, reputational damage, and the associated legal costs that go hand-in-hand when remediating such incidents. Moreover, Firms who fall victim to cybercrime attacks are likely to suffer a loss in confidence by their shareholders, customers, employees and the market at large.

The creation of the cybersecurity governance principles and practices aims to provide guidelines to Firms with practical illustrations of how the principles should be interpreted to mitigate their cyber risks. The steady migration of criminal activities online through the global increase of data breaches exposing personal data leading to financial fraud and identity theft has been some of the driving factors shaping our approach. Amongst others, the rise of social engineering techniques through 'phishing' attacks, as well as the emergent threat posed by terrorist organisations extending their actions to digital environments to fund their activities, constitute further grounds for raising awareness in this area.

The FSRA are mindful that the inherent cybercrime vulnerabilities and adopted cybersecurity measures may vary by Firm due to different levels of sophistication and variance in reliance on technology. Firms are therefore required to tailor their risk management programmes by following a risk-based assessment methodology to identify the cyber risks their businesses are exposed to. This approach should equip Firms to devise a structured and thought through strategy to combat cybercrime through allocation of resources, establishing clear lines of responsibly, and the adoption of risk-based controls that are commensurate with their inherent cyber risks. These strategies will also need to outline how they intend to prepare for, respond and recover from cyber-attacks should they occur.

The provision of these guidelines are not intended to override existing regulation or legislation. Instead, it is intended to contribute to supporting a holistic response to illicit activity involving cyber-related criminality recognizing its correlation with fraud, money laundering and terrorist financing; and with the aim of balancing innovation and risk to create a safer and more resilient financial ecosystem.

Principle 1: Cybersecurity Governance and Risk Management Framework

A robust system of cybersecurity governance has clearly defined roles and responsibilities wherein cyber risk is managed through a risk management framework comprising a series of documented, agreed and understood policies, procedures and processes that define how the Firm's information assets are managed and protected. Achieving a consistent standard of sound practices for IT controls across a Firm requires commitment from the board and senior management. These policies should be formally approved by the board or a designated senior committee with oversight on cyber risk.

Good Practice

1. The board of directors and senior management of Firms should ensure that cyber risk is an element of their Firm's broader risk management framework and that exposures are recognised, assessed for impacts based on clearly defined metrics such as response time, cost and legal or compliance implications, and commensurate with a risk-based assessment.

2. Ensure that cybersecurity matters are placed on the board agenda on a defined periodic basis that is consistent with the Firm's strategy and risk tolerance. In so doing, the board should evaluate relevant industry frameworks and technology standards in developing a personalized approach to cybersecurity.

3. The role of the board, or an appropriate designated board committee with oversight on cyber risk, may include the responsibility to do the following:

    a) Engage management in establishing the Firm's vision, risk tolerance, and overall strategic direction

    b) Review the Firm's inherent risk profile in relation to its cybersecurity maturity, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results

    c) Review management's determination of whether the Firm's cybersecurity preparedness is aligned with its risk tolerance

    d) Review and approve plans to address any risk management or control deficiencies and to implement security control measures commensurate with the identified risk, complexity and size of the Firm's operations

    e) Review the results of management's ongoing monitoring of the Firm's exposure to and preparedness for cyber threats

    f) Develop a standalone information security policy to ensure that all users and networks within the organisation meets the minimum IT security and data protection requirements.

4. The board of directors and senior management should adopt an appropriate 'tone at the top' and lead employee efforts to facilitate and foster a culture that promotes the sound management of cyber risk emphasizing the shared nature of responsibility on all employees in the Firm.

Principle 2: Cyber Risk Assessment

Firms should know what information assets they have and which are authorized to be on their network, including the locations of where their sensitive data is stored, as well as the inherent vulnerabilities and threats they are exposed to. Firms therefore need to take stock of their information assets and perform periodic cyber risk assessments as part of an ongoing and cyclical process.

Good Practice

1. Establish and maintain a cyber risk assessment program that evaluates its preparedness to withstand disruption brought about by a cyber-attack. Cyber risk assessments should be carried out on at least an annual basis with a scope that covers, amongst others: critical information assets, both internal and external vulnerabilities and threats, and the adequacy of its preventative controls.

2. Maintain an up to date inventory of its information assets. This will include identifying, defining and categorizing different assets. Asset inventory and identification of information assets are crucial components of a cyber risk assessment program because they indicate where a Firms critical information assets reside and inform the scope of a cyber risk assessment.

3. By way of example, Firms could consider the following approach when carrying out a cyber risk assessment program:

    a) Risk identification: identify all inherent and emerging threats to the Firm's information assets

    b) Risk assessment: assess the business impacts and likelihood for all of the risks in question

    c) Risk treatment: determine how the risks are addressed and remediated through the implementation of suitable control measures

    d) Risk monitoring: conduct ongoing monitoring of the effectiveness of the control measures and report back to concerned management on the state of preparedness

4. Based on a determination of exposure stemming from a review of the assessment results, Firms should prioritize on how they will manage their identified risks commencing with adequate control measures on their critical information assets (i.e. how the Firm will treat, tolerate, transfer or terminate the risk) and proportionate allocation of resources[1].

5. In order to monitor and maintain effective controls and drive continuous improvements over the identified risks, it is recommended that Firms establish a cyber risk register that tracks all cybersecurity related controls and processes. Firms should derive inputs from business, IT, risk management, internal audit and other associated functions to create and implement adequate control measures to enhance the Firms operational resilience profile. In general, Firms with processes and service offerings that are more inclined to cyber risks are expected to adopt a more stringent benchmark.

Principle 3: Management of Cyber Risks associated with Third Party Service Providers

Firms should evaluate all relevant cybersecurity risks that may stem from placing reliance on third party service providers who manage or store confidential customer and/or financial information. Firms should adopt a risk-based approach prior to and during the lifecycle of their engagements with third party service providers. This will aid the Firm in understanding the connectivity between and dependency on third party service providers.

Good Practice

1. Firms should carry out suitable due diligence prior to commencing any work with prospective third party service providers. This will include, but is not limited to:

    a) Consider adverse media and track record of the third party service provider

    b) Determine the security strategies and which privacy measures are undertaken to ensure data confidentiality, integrity and availability

    c) Establish and identify the use of any functions outsourced by the third party provider who will have access to critical data

    d) Discuss technology controls in place and the remediation of any identified control deficiencies

[1] Based on the outcome of the cyber risk assessment, Firms may consider purchasing cyber insurance as a way of transferring risk for high-impact security incidents which may prove costly to remediate. These measures may be of most relevance to Firms with an inherently high exposure to cyber risk, such as Firms that are heavily reliant on technology.

2. Institute contract provisions which require the service provider to adopt or align their IT security standards to that of the Firms. A Firm may consider performing an equivalence assessment to determine whether the service provider's security standards meet those of the Firm's.

3. Establish non-disclosure agreements where the parties agree not to disclose information obtained under the engagement to unauthorized individuals, (e.g. personally identifiable information or company trade secrets)

4. Establish breach notification responsibilities which require the service provider to inform the data owner (the Firm) of a security breach in a timely manner. Consideration should be attributed to defining the accountable party in these circumstances as well as any relevant associated costs.

5. Conduct ongoing due diligence and monitoring of existing third party service providers to determine compliance or deviation from the agreed terms of reference. Firms could incorporate contract provisions which grant them the right to audit specific procedures.

6. Establish procedures to terminate the service provider's access to systems upon termination or conclusion of their contract term. These provisions should include the deletion by the third party of any and all sensitive information/data that it has had access to during the engagement.

Principle 4: Incident Response Planning

Firms should develop an incident response plan that outlines how the Firm will respond to an unplanned disruption to services brought about by a cybersecurity event. The response management framework should provide a set of instructions to assist the Firm in limiting disruption and potential damage with the aim of safeguarding its information assets and resuming critical business activities in a timely matter. In essence, the plan should detail how the Firm will prepare for, respond to and recover from a cybersecurity event.

Good Practice

1. While it is not always possible to plan for every conceivable incident, the Firm's incident response plan should have a plan for the most common types of cyber-attacks which the Firm may encounter, such as:

    a) Data breach (e.g. loss of personally identifiable information)
    b) Data corruption
    c) Denial of service attack
    d) Email compromise / take-over
    e) Insider attack
    f) Malware intrusion

g) Phishing

h) Ransomware

2. Develop IT security policies detailing the Firms approach to handling cybersecurity incidents. The policy should outline clearly defined roles and responsibilities for responding to and escalating cybersecurity incidents.

3. Develop containment and mitigation strategies to prevent the incident from inflicting further damage. An essential part of containment is decision making, (e.g. whether to shut down a system, disconnect it from a network or disable certain functions). These kinds of decisions can be made quickly and effectively if there are predetermined strategies and procedures in place for containing an incident.

4. Establish investigation and assessment processes. Firms must be able to conduct timely investigations on all security incidents to determine the extent of damage (i.e. data or monetary loss) and identify root causes. Effective investigation processes predetermine the kinds of information or data that is required in order to ascertain the facts and merits surrounding a specific offence. Firms who do not possess in-house investigation expertise should appoint a third party provider with incident response expertise to carry out an investigation when a cybersecurity incident occurs.

5. Develop recovery plans for systems and data (i.e. defining the 'recovery time' as a point in time when information systems need to resume before it negatively affects the operations). Recovery activities typically involve: restoring systems from clean back-ups or rebuilding systems from scratch, installing patches, replacing compromised files or devices with clean versions, changing passwords and taking measures to strengthen network perimeter security (e.g. increasing system logging and network monitoring).

6. Develop well-defined and tailored communication plans that set out how to notify relevant stakeholders in the event of an unplanned disruption to services, such as:

   a) Regulators: disclose timely and accurate details of the incident in question to your regulator

   b) Customers: apply discretion in notifying customers in accordance with the relevant pre-existing laws and regulations.

   c) Law enforcement: report and disclose information in relation to a suspected criminal offense

   d) Industry sharing bodies: consider disseminating appropriate information on threat intelligence with industry peers and/or information sharing bodies[2].

[2] Refer to Principle 8 on Collaboration and Information Sharing for guidance on collaborative practices.

7. Carry out scenario led discussions and/or rehearsals on the presumption that an incident has occurred. These procedures will aid Firms to decide on whether their strategies are fit for purpose or whether adjustments should be made – as opposed to relying on the cyclical review plan which could overlook the need to improve control measures in between prescheduled periodic review points.

Principle 5: Cybersecurity Awareness and Training

Firms should aim to create an appropriate level of cybersecurity awareness amongst their employees, enterprise-wide. Employees are the major sources of cybersecurity risk. These risks can often take the form of inadvertently clicking on a link in a phishing attempt. In such scenarios, even the best technical controls can be undermined. Cybersecurity awareness and training is thus an essential component to a robust cybersecurity risk management framework.

Good Practice

1. Awareness sessions should take place once annually and/or during an employee's on-boarding or change of roles, and as required on an ad hoc basis in response to specific cyber events. The content of the training should include education on the risks that users may encounter during their daily activities.

2. All users with access to the Firm's IT infrastructure (including third party service providers, executives and the board) must be informed and trained on their roles and responsibilities regarding cybersecurity.

3. Firms may choose to assess their points of exposure and customize their training to particular groups commensurate with their exposure to cyber risks. The range of training topics could include, but is not limited to:

    a) The emerging landscape of cyber threats and its implications
    b) The Firms IT security policy and procedures
    c) Spotting cyber risks
    d) Social engineering schemes (including phishing and schemes using social media)
    e) Escalation policies
    f) Handling confidential information
    g) Individual responsibility to safeguard the Firm against cyber threats
    h) Password protection
    i) Physical and mobile security

4. Firms may also consider devising a separate training module that is tailored and targeted at specific groups in the Firm with heightened exposure such as, IT staff and general management. The content of this training module could focus on:

a) Application lifecycles
b) Application security
c) Emerging technology issues
d) Privilege management
e) Software vulnerabilities

5. In addition, Firms may consider 'random testing' to measure the effectiveness of their cyber awareness program, and to take appropriate measures based on the responses from the targeted employees. In this scenario a test email containing 'malware' is sent to a group of employees to test their response. Hereafter, employees may need to undergo further training if they did not manage the situation in an acceptable manner.

Principle 6: Protective Controls

In addition to the safeguards that arise from employee awareness initiatives, Firms are expected to demonstrate that they have adopted suitable protective controls that are commensurate with their identified risk, complexity and size of the Firm's operations. Where appropriate, and consistent with the Firms risk tolerance, the scope of a Firms protective controls may include a combination of measures exceeding the most commonly used security controls.

Good Practice

1. Firms should evaluate relevant industry frameworks and technology standards in developing a personalized approach[3]. Firms do not necessary need to re-invent their security configuration standards because they could opt to adopt and comply with existing security configuration standards of reputable international standard-setting bodies as a benchmark.

2. Implement technical controls that are appropriate to address relevant components and protocols in the Firm's network architecture. Technical controls are primarily implemented and executed by computer systems through mechanisms contained in the hardware, software, or Firmware components of the system. They offer automated protection against the misuse and/or unauthorized access to sensitive information and facilitate the detection of security violations.

3. Adopt robust Identity and Access Management (IDAM) practices. IDAM refers to the creation of policies, procedures and systems that support an individual user (or system) to a set of permissions within the Firms system. These policies outline which users have

[3] Although not a mandatory requirement, the formal adoption of technology standards provide a baseline requirement for the critical infrastructure organizations need to possess to manage cyber risks and protect their critical information assets from cyber-attacks.

access to specific systems, data or functionality, and the circumstances under which access is granted, reviewed and revoked. Firms should consider the following effective IDAM practices, which are not limited to:

a) User privileges

i. Users with administrative or privileged access should use a designated device dedicated for carrying out approved privileged tasks and activities.
ii. Issue privileged users with a standard user account which has different password policies to reduce the exposure of various associated attack methods.
iii. Require privileged users to adopt two-factor authentication (physical or logical) to increase the difficulty for an attacker to gain unauthorized access.
iv. Restrict privileged access to the information and functions required to complete specific agreed upon duties.

b) Password practices

i. Where appropriate, consider using password managers or vaults to generate and securely store multiple passwords, particularly for master passwords, without relying on passwords recorded on documents. Where appropriate, include password managers as part of the scope in vulnerability assessments and periodic patching cycles.
ii. Implement 'password blacklisting' practices to prevent the use of common passwords that are easily cracked. Firms could decide to extract a list of common passwords on their networks as examples to inform their staff members during training and awareness initiatives.
iii. Consider the use of biometric authentication such as fingerprint or facial recognition for some systems[4].

c) Audit logs

i. Adopt tamper proof data logging practices which are protected from any modification.
ii. Capture adequate information to establish what events occurred and who (or what) caused them (e.g. type of event, when the event occurred, associated user ID, program or command used to initiate the event). This will assist in intrusion detection and remediation of a cyber incident.
iii. Review the logs of privileged users following a known or reported system software problem, an unexplained system or user problem, or a known violation of existing requirements by a user.

[4] These technologies reduce the password burden on staff members although they are not full-proof as they could be prone to impersonation or spoofing attacks. It is therefore suggested that ongoing proportionate assurance measures are incorporated as part of the periodic review cycle in order to maintain effectiveness.

d) Data back-up

i. Regularly back-up data in a different location with different access controls.
ii. Encrypt data back-up before placing it in the cloud and avoid disclosing the decryption credentials to the cloud provider.
iii. Consider 'kill switch' technology which remotely disables access to information in an emergency situation.

e) Encryption

i. Adopt the proportionate use of encryption mechanisms to store and transmit sensitive data based on a risk-based approach that considers impact and exposure.
ii. Regarding stored data, consider encrypting sensitive data stored on:

    a. Portable media devices such as USB drives and backup drives (as well as restricting access to USB ports to reduce the risks of data leakage or unauthorised software)
    b. The Firms private systems
    c. A cloud service

iii. Regarding data in-transit, consider encrypting sensitive data transmitted over untrusted networks including the internet as well as any network where the Firm does not operate on or control physical and logical access to the communication and transmission lines.

f) Product design and change management

i. Include the cybersecurity team during product design and change management processes. This should be done to embed cyber resilience at the earliest stage of design, development and system acquisition. In so doing, the Firm will be able to leverage off of the cybersecurity team on best practice throughout the system development lifecycle and into the change management processes.

g) Bring Your Own Device (BOYD) security controls

i. Firms who permit their staff members to use their own personal devices to carry out work related responsibilities should adopt appropriate policies and procedures to address the confidentiality and integrity of the Firm's data (i.e. how it should be handled) and incorporate measures to address specific cyber threats.

Principle 7: Detection Systems and Processes

All Firms should create and implement robust detection systems with the aim of identifying vulnerabilities and threats and ensuring the necessary countermeasures are adopted before they can be exploited. In so doing, Firms should define and differentiate between 'normal' and/or 'expected' activity, as well as 'abnormal' and 'suspicious' activities. The detection and identification processes should be used to improve the Firm's response capabilities and inform the Firm's countermeasures to cyberattacks by enhancing the facility's protection as required.

Good Practice

1. Firms should carry out periodic penetration testing at least annually and/or after any significant infrastructure or application upgrade or modification. When determining the scope of penetration tests, a Firm may commence with, but is not limited to, the Firms:

    a) Network including all live devices such firewalls, servers and routers
    b) Wireless devices
    c) Web-based applications
    d) Mobile applications
    e) Commercial-Off-The-Shelf (COTS) software
    f) In-house developed applications

2. Firms must carry out ongoing security monitoring of their systems to detect attempted attacks on their systems. To enable a more timely detection of suspicious activities, Firms may use Security Information and Event Management (SIEM) technologies or processes[5]. These tools and processes detect suspicious user activities such as unauthorized access to applications or files, as well as abnormal movement of information across the network referenced against a baseline of 'normal' and/or 'expected' activity.

3. Firms can choose to heighten the monitoring of the activity of users with privileged access. To this effect, Firms could identify specific logs to collect and analyse based on agreed scenarios and generate alerts that are relevant. Examples of alerts that could be developed include, which are not limited to:

    a) attempted logins from unexpected geographical regions or locations
    b) account lockouts
    c) failed or disabled Multi-Factor Authentication (MFA)
    d) multiple login attempts from a single host or IP address
    e) password attacks on accounts

[5] This approach will aid Firms to collect information from disparate devices or sources into a single location with the expressed intension of performing advanced analysis from a more holistic view of the Firm's IT security exposures.

f) unexpected time of day login attempts

4. Firms could also implement Data Loss Prevention (DLP) tools or processes. DLP tools prevent users from uploading sensitive information into email, cloud storage services, and unauthorized transfer capabilities. DLP processes include filtering and monitoring all outbound email messages to ensure that data is not transmitted outside of the Firm's network in error or through wilful intent.

5. Firms may adopt data analytics tools and processes to monitor events on their network and systems. Threats detected by the Firm, in addition to information collected through collaboration and information-sharing channels, can be analysed and used to enhance the Firm's capability of predicting and/or detecting malicious cyber activities in real time.

Principle 8: Collaboration and Cyber Threat Intelligence

Information sharing is an effective way for Firms to improve their understanding of the potential threats and motives by attackers or organised crime syndicates. In so doing, Firms can take proactive steps to reduce their vulnerability to cybersecurity threats. Firms should therefore consider participating in confidential information sharing arrangements with other financial institutions, security and law enforcement agencies. To this effect, Firms may consider participating in an industry forum with established information and intelligence sharing practices which Firms can build into their incident response plans. The collective impact of combining data and insights from these forums helps Firms and their industry peers to address cybersecurity threats more effectively.

Good Practice

1. Periodically review the Firm's information sharing partners.

2. Assign responsibility for gathering cybersecurity intelligence and analysis at organizational and individual levels.

3. Establish processes and channels to distribute threat intelligence to appropriate groups in the organisation, such as risk management and front-line IT security staff members.