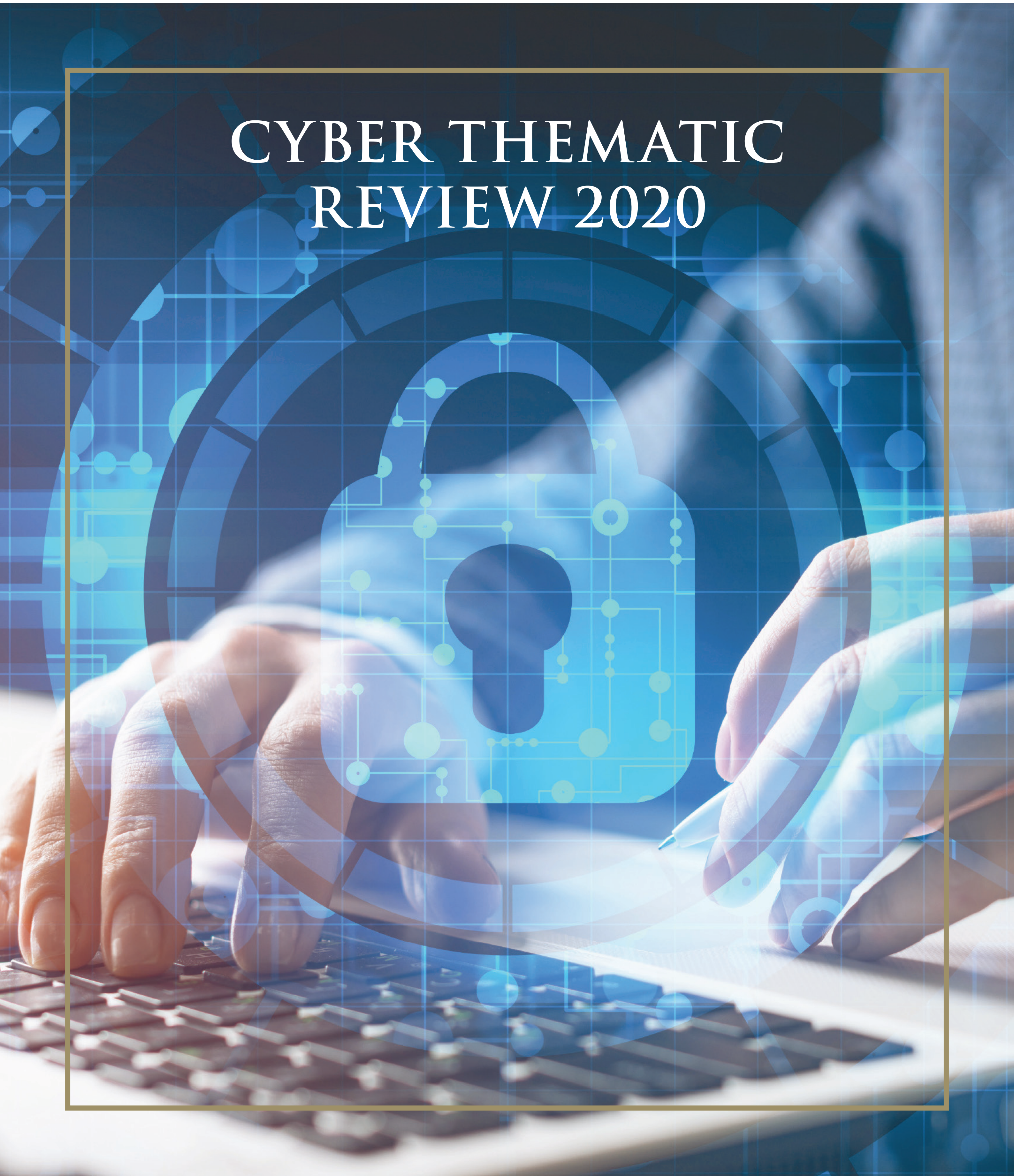
Dubai Financial
Services Authority

# CYBER THEMATIC REVIEW 2020



# TABLE OF CONTENTS

# Foreword

As we deliver the results of our thematic review on cyber risks, we are in an era of rapidly increasing cyberattacks around the world when cyber defences might be lowered and cyber vulnerabilities heightened due to the shift of focus to the health crisis. As cyberattacks targeting the financial services sector are becoming more frequent and sophisticated, it is crucial that financial institutions strengthen their vigilance and diligence around cyber risks and explore new approaches to build greater cyber resilience. Cyber risks have evolved and firms need to adapt their cyber security practices to those risks. As is commonly noted, a cyber breach is a matter of ***when*** it will happen, rather than ***if*** it will happen; therefore, it is important that firms not only focus on protection and prevention capabilities but also on strengthening their capabilities to respond to, and recover from, a cyber incident.

Cyber security should not be seen as the responsibility of the IT department alone. Managing this risk area requires a holistic view of vulnerabilities in an organisation, large or small. It also includes looking at risks associated with outsourced services providers. Cyber security is everyone's problem including the board of directors, senior management, and the business units. Cyber resilience should be embedded into the organisation's strategy with the objective of limiting the negative consequences of successful cyberattacks. This means changing the focus of activities from reactive to proactive actions. It involves planning your firm's response on an organisational level.

We strongly encourage firms to cooperate and share information about cyber threats. Cyber security is a shared responsibility, which we believe can best be addressed through public-private partnerships. We understand that our involvement with firms and other regulatory and professional associations is essential for building cyber security awareness among our stakeholders. We take, and will continue to take, a proactive approach to sharing knowledge, educating stakeholders and supporting companies in building their cyber resilience. Technological developments and technology risks will be a permanent element of our future business plans.

At the DFSA, we have been focusing our efforts on creating a community where firms may collaborate and share knowledge of emerging and observed cyber threats. If you have not already done so, I encourage you to register to access the DFSA Cyber Threat Intelligence Platform (TIP) via the DFSA ePortal.

This document contains the findings of our thematic review of DFSA Authorised Firms' cyber risk management practices and our expectations. We encourage you to consider this information alongside your own practices and to approach us with any questions you might have.

I would like to extend thanks to all the firms that participated in this review. I believe you will find this report to be helpful and instructive, and I look forward to your cooperation on future thematic reviews.

Bryan Stirewalt
Chief Executive

# Executive Summary

The purpose of this report (Report) is to summarise key findings from the Cyber Thematic Review (Review) launched by the Dubai Financial Services Authority (DFSA) in July 2019. The objective of the Review was to identify the overall maturity level of cyber security programmes of Authorised Firms (Firms). More specifically, during the Review we assessed IT/cyber risk governance frameworks, IT/cyber hygiene practices, and resilience (incident preparedness) programmes. The Review was undertaken in two phases:

- Phase 1 consisted of a questionnaire seeking relatively high-level information on each Firm's cyber security practices and consisted mainly of multiple-choice questions. The questionnaire was sent to a total of 490 Firms. We were particularly pleased to have an 80% response rate with 392 Firms replying.

- Phase 2 consisted of desk-based reviews and onsite visits, including documentation reviews and staff interviews. This phase included 20 Firms representing a range of business models and financial services activities. Prior to our site visits, we requested each selected Firm to provide to us documentation regarding their cyber risk management practices.

We analysed findings and observations from the desk-based review and onsite visits along with further consideration of the questionnaire responses to prepare this Report. Please note that, in our Report, we have listed only key findings and observations that were common among the participants of the Review. Therefore, this Report does not include all identified issues and observations. Finally, not all of the findings and observations noted in this Report are relevant to all entities. Firms should use this Report as instructive information and not as a comprehensive guide to cyber risk management.

## Summary of findings

Our Review highlighted important areas for improvement within the cyber risk management practices of Firms operating in the Dubai International Financial Centre (DIFC). We grouped our findings into the three main categories of governance, hygiene and resilience and identified significant room for improvement in all three areas. In particular, we noted the following issues.

### *Governance*

1. A significant number of Firms have not implemented a cyber risk management framework. As a consequence, many Firms' cyber risk management activities tend not to be properly coordinated and are performed on an ad hoc basis.

2. A significant number of Firms perform only a limited cyber risk assessment. They tend to identify cyber risks only in relation to availability of IT systems, without sufficient attention to the sensitivity of processed data. Some Firms assess cyber risk as low without providing a rationale for the low rating.

3. In many instances, neither the board nor senior management oversight of cyber risk management was sufficient. This was especially prevalent where Firms outsourced their IT infrastructure and cyber security functions to an IT service provider. This was also evident in the fact that there was a lack of senior management review of cyber security audits, reviews and tests.

4. Only half of all Firms have a due diligence process to assess whether third-party service providers meet the Firm's cyber security requirements and even fewer Firms periodically test whether third-party service providers satisfy the Firm's cyber security requirements.

5. The vast majority of Firms declared that they do identify and classify their IT assets. However, we identified that Firms mostly focus on IT equipment only, and do not identify and classify information and IT systems or do that in an informal manner on an ad hoc basis.

6. A significant number of Firms have not established a comprehensive cyber security training programme or a cyber awareness campaign to enhance the overall cyber security awareness level. Moreover, the cyber training offered to employees by small and medium-sized Firms tends to be ad hoc rather than at regular intervals.

### *Hygiene*

7. A significant number of Firms have not performed Vulnerability Assessments or Penetration Tests of their Critical Information Systems in the past year. Firms using off-the-shelf systems do not recognise the necessity of performing such tests as they see it as a responsibility of the system vendors.

8. In cases where Critical Information Systems are accessible from the Internet, some Firms rely on basic user authentication using usernames and passwords. In addition, some Firms have not implemented strong password policies (e.g. minimum password length, required password complexity and account lockout threshold after a defined number of unsuccessful logon attempts).

9. A significant number of small and medium-sized Firms do not enforce encryption of workstation hard drives and portable devices to protect sensitive data.

### *Resilience*

10. Half of all Firms do not have continuous identification and response capabilities for managing cyber incidents in regard to all Critical Information Systems. Small and medium-sized Firms rely mainly on manual processes to monitor their infrastructure only during working hours or do not have monitoring capabilities at all.

11. The majority of Firms have implemented some form of a cyber incident response plan to respond to, and limit the consequences of, a cyber incident. However, in many cases, the cyber response procedures are addressed in general terms as components of the business continuity plan and are not tailored specifically to cyber threats.

12. Less than half of all Firms have implemented a crisis management communication plan that addresses external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement) and even fewer Firms have implemented an internal crisis communication plan (designed for relevant business units, senior management, board of directors, etc.).

13. More than half of Firms' cyber incident response plans do not include a formal requirement for periodically testing the Firm's response to a cyber incident. Moreover, where Firms do have a periodic testing requirement, we identified that a significant number of Firms have not tested any component of their cyber incident response plans in the past year.

14. Some small and medium-sized Firms use professional forums or groups to get information about particular cyber threats but tend not to share information about cyber incidents. Firms noted lack of sufficient detection capabilities and potential reputational harm as the main reasons for not sharing information about cyber incidents.

The Report describes these findings in further detail together with the DFSA's expectations and examples of best practices of cyber risk management. Firms are encouraged to consider this information, together with their own practices, and to implement improvements to their control environments and processes, where necessary.

"An effective cyber governance function begins with a defined cyber risk management framework."

# Key findings and our comments

## Governance

### 1. Cyber risk management framework

We noted that a significant number of Firms have not implemented a cyber risk management framework or, in the case of small and medium-sized Firms, at least a description of their approach to mitigate cyber risks. This issue is more common among the latter group of Firms where, as a consequence, Firms' cyber risk management activities tend not to be properly coordinated and are performed on an ad hoc basis. We note that the lack of a defined written approach to cyber risk management may negatively impact the overall effectiveness of IT and cyber controls as well as the Firm's cyber security processes. The lack of a defined approach does not allow for effective monitoring of cyber risks and, consequently, for an adequate response to those risks.

In some cases, Firms claim that the lack of the cyber risk management framework is a product of the Firm assessing itself as having low cyber risk. While we accept that a low cyber risk rating may be accurate, in limited and very specific cases, most Firms that adopted a low rating failed to demonstrate sufficient analysis to justify the low rating. Moreover, the level of cyber risk may impact the complexity of the framework but it does not dictate whether the Firm should develop a framework at all.

An effective cyber governance function begins with a defined cyber risk management framework. The purpose of the framework is to provide a structure within which to identify, manage, and mitigate cyber risks effectively in an integrated and comprehensive manner. Moreover, the 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. An effective cyber risk management framework is a framework that is tailored to the Firm's size, complexity and risk appetite. The framework can be based on the existing industry standards prepared by experts and recognised professional institutions. The more commonly used frameworks/standards include:

- CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures;
- ISO/IEC 27000 set of standards;
- NIST Cybersecurity Framework; and
- CIS Critical Security Controls for Effective Cyber Defence.

Where a Firm chooses to adopt one of the above frameworks/standards, the Firm should carefully analyse the framework/standard and implement only the relevant processes and controls. Firms should tailor the framework/standard to their needs rather than implement the entire set of practices described in the mentioned publications.

Finally, when developing or reviewing the framework, Firms should take into consideration the findings, observations, and expectations outlined in the remainder of this report, as they represent key aspects of cyber risk management.

### 2. Cyber risk identification and assessment capabilities

The majority of Firms declared that they identify and assess cyber risks. However, we found that a significant number of Firms perform only a limited cyber risk assessment that considers only the availability of IT systems, without sufficient attention to the sensitivity of processed data. For example, the risk that a cyberattack may result in the unavailability of IT systems is widely identified, but the risk that a cyberattack may result in a data breach is not widely considered. Some Firms declared that they assessed their cyber risk rating as low; however, they were not able to present a reasonable rationale for such a statement.

In some cases, we found that Firms confuse incident management and problem management with cyber risk management. Incident and problem management are critical components of cyber risk management. However, cyber risk management is a holistic process that seeks to identify the risk of incidents and problems, prevent or mitigate their likelihood of occurrence, and prepare the Firm to respond to threats and incidents.

We expect firms to 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, IT systems and interfaces, processes, people and data.

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.

Once 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 (see point *5. IT asset identification and classification*) and the level of the Firm's risk appetite. Identified risks and controls should be monitored on an ongoing basis and updated if necessary.

## 3. Board and senior management responsibilities and understanding of cyber risks

In many instances, we identified that the board and/or senior management do not maintain sufficient oversight of cyber risk management processes. Neither the board nor senior management are informed of current cyber issues or emerging risks and are not given enough information to assess the appropriateness of mitigating actions. In addition, the results of cyber security audits, reviews and tests are not reviewed by senior management on a regular basis.

In some cases, where Firms outsource their IT infrastructure and cyber security functions to an IT service provider, board and senior management have limited or no oversight of cyber risk issues. Firms attributed this to a lack of board understanding of cyber risks and trust in the expertise of service providers.

The board and senior management are ultimately responsible for setting 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 cyber security activities are outsourced to a specialised vendor, the board and senior management continue to be responsible for cyber risk management oversight. The board and senior management 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.

Management information should be presented to the board in a way that can be easily understood and analysed. Also, board members should have a good understanding of cyber risks and be updated on the current global cyber trends on a regular basis (see point *6. Cyber training and awareness campaigns*).

## 4. Third-party cyber risk management

More than two-thirds of respondents, which had identified their Critical Information Systems, declared that at least one of their Critical Information Systems is managed by a third-party service provider. We found that in many cases Firms do not assess whether service providers process their data with controls that satisfy the Firm's cyber security requirements.

Only half of all Firms have a due diligence process to assess whether third-party service providers meet their cyber security requirements and even fewer Firms periodically test whether third-party service providers satisfy the Firm's cyber security requirements. These findings show that Firms are not assessing sufficiently whether their data is processed in a secure manner.

Cyberattacks can affect systems or data hosted by third parties or be initiated through third parties' IT infrastructure, employees or their service providers. Therefore, third party vendors have an important role in safeguarding data confidentiality, integrity and availability. Firms should address the cyber security requirements in agreements with third parties involving accessing, processing, communicating or managing the Firm's data. Firms retain ultimate responsibility for cyber risks for all outsourced operations and data; therefore, it is incumbent upon Firms to ensure adequate oversight of cyber controls is applied by third-party service providers.

In addition, Firms should periodically verify that third party service providers continue to satisfy the Firm's cyber security requirements. This can be achieved 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.

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

Finally, in addition to understanding whether a third-party service provider continues to satisfy the Firm's cyber security requirements, the Firm should consider more holistically the factors that may impact the service quality. For example, the current environment has seen instances of service providers experiencing financial distress. Such distress could result in a reallocation or reduction of resources (e.g. staff reductions, cuts in IT spending, delays in system upgrades) that may negatively impact the service quality including the provider's cyber security posture. Therefore, it is important that a Firm maintain view of the drivers of potential future impacts to the strength of their third-party service provider's cyber security. These drivers of risk should be factored into the Firm's suite of key risk indicators.

## 5. IT asset identification and classification

Over 90% of Firms declared they identify and classify their IT assets. However, Firms mostly focus on IT equipment only and do not identify and classify information and IT systems, or do that in an informal manner on an ad hoc basis. Moreover, Firms which have implemented an IT asset classification process usually focus on criticality of assets for business continuity purposes and do not take into consideration asset sensitivity.

Additionally, we found that a number of Firms do not consistently and regularly review and update their IT asset classification and are often unable to present an asset inventory reflecting the current state of their IT environment.

We expect that all Firms should identify and classify IT assets based on their sensitivity and criticality in order to ensure that all classified assets receive an appropriate level of protection. Firms should maintain a current inventory of their IT assets in order to know all the assets that support their business functions and processes. Subsequently, Firms should define and apply appropriate controls to secure data according to their level of criticality and sensitivity.

Firms should have well-defined processes and clearly assigned responsibility for maintaining the IT asset inventory. IT asset inventories should be reviewed and updated on a periodic basis. The review process should take into consideration the results of the Firm's most recent risk 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.

### 6. Cyber training and awareness campaigns

More than two-thirds of Firms declared that they provide cyber training for employees. However, we found that the vast majority of cyber training offered to employees by small and medium-sized Firms tends to be ad hoc rather than at regular intervals. In such cases, staff may not be properly trained and prepared for cyber risks that they might face during their work.

The majority of large Firms have developed comprehensive training programs and ensured that each employee attends a cyber security training session at least on an annual basis. Additionally, large firms launch cyber awareness campaigns in many different forms (e.g. mock phishing campaigns and periodic cyber security newsletters).

All Firms should establish a comprehensive cyber security training programme or a cyber awareness campaign to enhance the overall cyber security awareness level. The training programme should include information on cyber security policies and standards as well as individual responsibility in respect of cyber security and measures that should be taken to safeguard information system assets. Firms should ensure that all staff (permanent or temporary) receive training at least on an annual basis to develop and maintain appropriate awareness of, and competencies for detecting and addressing, cyber risks. They should also be trained on how to report any unusual activity and cyber incidents. Such training should be conducted for all new and current employees. All new employees should read and understand a Firm's Information Security Policy and/or other relevant policies and procedures that describe information security and cyber security requirements.

Moreover, we would like to stress that employees who have privileged access to the Critical Information Systems (e.g. IT administrators, IT support personnel) should be identified and should receive targeted information security training.

## Hygiene

### 7. Vulnerability Assessments and Penetration Testing

A significant number of Firms have not performed Vulnerability Assessments or Penetration Tests of their Critical Information Systems in the past year. A common response from Firms is that such decisions are driven by the fact that the majority of a Firm's IT infrastructure is outsourced to third-party service providers and the Firm places reliance on the service provider's controls and procedures. Also, Firms using off-the-shelf systems do not recognise the necessity of performing such tests as they see it as the responsibility of system vendors.

Firms should use a variety of methods to test critical IT infrastructure and Critical Information 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. Regular Vulnerability Assessments of Critical Information Systems allow a Firm to identify known cyber security vulnerabilities. Moreover, Penetration Tests allow a Firm to identify vulnerabilities that may affect the Firm's systems, infrastructure and processes. Testing of the internet-facing Critical Information Systems should be conducted regularly and whenever systems are updated or deployed. Additionally, Firms may carry out red team exercises to simulate a real-world cyberattack to test their cyber preparedness.

"Firms should use a variety of methods to test critical IT infrastructure and Critical Information 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."

Where the maintenance of the Critical Information Systems has been outsourced to a third-party service provider, it is the Firm's responsibility to ensure that the vendor's IT 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.

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.

### 8. Multi-factor Authentication for external access (e.g. VPN, webmail)

We found that some Firms that have their Critical Information Systems accessible from the Internet still rely solely on basic user authentication using usernames and passwords. Firms using such authentication mechanisms without any additional access controls may be exposed to significant risk of unauthorised access to their Critical Information Systems.

In addition, some Firms have not implemented strong password policies (e.g. minimum password length, required password complexity and account lockout threshold after a defined number of unsuccessful logon attempts). The lack of a strong password policy in combination with single-factor authentication creates a critical cyber security risk.

Many IT systems and IT service providers support Multi-factor Authentication (MFA) and allow users to enable it to better protect their accounts. There are different methods of MFA and the most common methods used by Firms are: one-time passwords (OTP) delivered via mobile applications, email or SMS, and code generated by an authenticator (e.g. hardware security token or mobile application). The use of two or more of these factors to verify a user's identity is one of the basic methods to reduce the risk of unauthorised access from the use of stolen credentials or identity theft. With the use of MFA, the victim's password will no longer be enough to give cybercriminals access to the Firm's systems.

Firms should implement MFA to all accounts in the Critical Information Systems that can be accessed from the Internet. Moreover, MFA should be required for all Administrative Accounts if it is supported by the Critical Information System, regardless of whether they can be accessed from the Internet or through an internal network only. Users having access to the Administrative Accounts are often victims of targeted attacks as their credentials are especially desired by cybercriminals.

### 9. Encryption of data stored on hard drives and portable devices

The vast majority of large Firms use encryption techniques to protect sensitive data stored on workstation hard drives and portable devices. Additionally, some Firms do not allow using portable devices at all and have implemented technical controls to ensure that data cannot be copied to external drives. However, a significant number of small and medium-sized Firms do not enforce encryption of workstation hard drives and portable devices.

Firms should implement encryption techniques to protect sensitive information stored on workstation hard drives and portable devices. The use of encryption techniques should be commensurate with the level of criticality and sensitivity of data and should be applied to all devices. 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.

## Resilience

### 10. Continuous monitoring, detection and response capabilities

Half of all Firms do not have continuous identification and response capabilities for managing cyber incidents in regard to all Critical Information Systems. Small and medium-sized Firms constitute a large part of this group. Unfortunately, a significant number of small and medium-sized Firms have not established any continuous monitoring capabilities to monitor anomalous activities and events that can be indicators of a potential cyber breach. Other small and medium-sized Firms mainly rely on manual processes to monitor their infrastructure during working hours. A majority of large Firms, on the other hand, have implemented continuous monitoring of their Critical Information Systems (in real time or near real time) to detect potential cyberattacks and immediately support their cyber response.

All 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. A Firm's monitoring and detection capabilities enable the Firm to determine the nature and extent of a cyberattack to facilitate its cyber incident response process, based on the characteristics of the attack.

### 11. Cyber incident response planning and preparation

The majority of Firms have implemented some form of a cyber incident response plan to respond to, and limit the consequences of, a cyber incident. However, in many instances the plans were not comprehensive and did not include important elements of an effective cyber response (refer to the below list of expected elements). Moreover, in some cases the plans have not been updated on a regular basis. We also identified that cyber response procedures are typically addressed in general terms as a part of business continuity plans and are not tailored specifically to cyber threats.

Cyber resilience is a broad topic which includes protecting the Firm's reputation and ensuring commercial viability. Therefore, the cyber incident response plans should be more aligned to crisis management and not just business continuity.

The cyber incident response plan is a predetermined set of instructions and procedures to respond to and recover from a cyber incident. The cyber incident response plans, as well as data backup and contingency plans, jointly play an important role in strengthening a Firm's cyber resilience.

A robust cyber incident response plan should contain the following at a minimum:

- procedures for detecting, monitoring, analysing and responding to cyber incidents;
- definition of incident management roles and responsibilities;
- an internal communication plan that includes communication protocols for key internal stakeholders (e.g. relevant business units, senior management, board of directors);
- an external communication plan that includes communication protocols for key external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement);
- a recovery plan and/or references to a disaster recovery plan;
- procedures of post-incident review; and
- Cyber Incident Response Plan periodic testing requirements.

"Cyber resilience is a broad topic which includes protecting the Firm's reputation and ensuring commercial viability. Therefore, the cyber incident response plan should be more aligned to crisis management and not just business continuity."

Once the plan is prepared, it 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.

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.

### 12. Crisis communication plans (internal/external)

The Review identified that 48% of Firms' cyber incident response plans do not contain a crisis communication plan that addresses external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement) and 43% of Firms have not implemented an internal crisis communication plan (e.g. relevant business units, senior management, board of directors).

Effective communication with internal and external stakeholders during a crisis is essential to minimise the negative impact on a Firm's reputation and potential spread of misinformation. 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.

The crisis communication plans are important and should be prepared in advance. During a cyber incident, Firms may not have enough time to prepare and launch appropriate communication to all interested parties. The communication plans prepared in advance help shorten time required to communicate effectively with stakeholders during the crisis.

### 13. Incident response testing programme

More than half of all Firms' cyber incident response plans do not include a formal requirement for periodic testing of the Firm's response to a cyber incident. Moreover, a significant number of Firms have not tested any component of their cyber incident response plans in the past year.

Similar to other response plans (e.g. a business continuity plan), testing requirements should be an integral part of the cyber incident response plan. Testing is an essential component of any cyber resilience framework. Establishing and testing the cyber incident response plan for critical processes and information systems, before an incident occurs, can contribute to a faster and more effective recovery. 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.

### 14. Information sharing

We noted that most large Firms use cyber threat intelligence platforms to share or access information about current cyber threats. Some small and medium-sized Firms use professional forums or groups to get information about particular cyber threats but tend not to share information about cyber incidents at all.

Firms noted a lack of sufficient detection capabilities and potential reputational harm as the main reasons for not sharing information about cyber incidents.

We would like to emphasise that cyber security is a shared responsibility, involving both the private sector and the public sector, and there are a number of benefits to sharing cyber threat intelligence, whether through intelligence sharing platforms, forums, or other information sharing communities. Firms that participate in threat intelligence sharing communities can improve their cyber response and remain up-to-date in their defences by learning about emerging attack methods. Moreover, sharing information with other entities helps to determine how attackers may exploit industry-specific vulnerabilities. Given its importance, Firms should consider information sharing as an important and significant factor in strengthening their cyber resilience. Finally, Firms are encouraged to register to access the DFSA TIP via the DFSA ePortal. TIP is available to all DFSA Authorised Firms.

# Glossary

**Administrative Account** – In regard to an information system, any user account that has full privileges and unrestricted access to the information system.

**Critical Information System** – An Information System, the failure of which will cause significant disruption to the operations of the DIFC Entity or materially impact the relevant DIFC Entity's service to its clients. A Critical Information System includes but is not limited to a system which:

a) processes transactions that are time critical; or
b) provides essential services to clients.

**Multi-factor authentication (MFA)** is an authentication method in which an individual is granted access only after successfully presenting two or more pieces of information (factors) to an authentication mechanism.

The use of two or more of the following factors to verify an individual's identity:

a) knowledge factor, "something an individual knows";
b) possession factor, "something an individual has";
c) biometric factor, "something that is a biological and behavioural characteristic of an individual".

**Penetration Testing** is a test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

**Vulnerability Assessment** is a systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

Dubai Financial
Services Authority

For General Enquiries
T +971 (0) 4 362 1500   W www.dfsa.ae