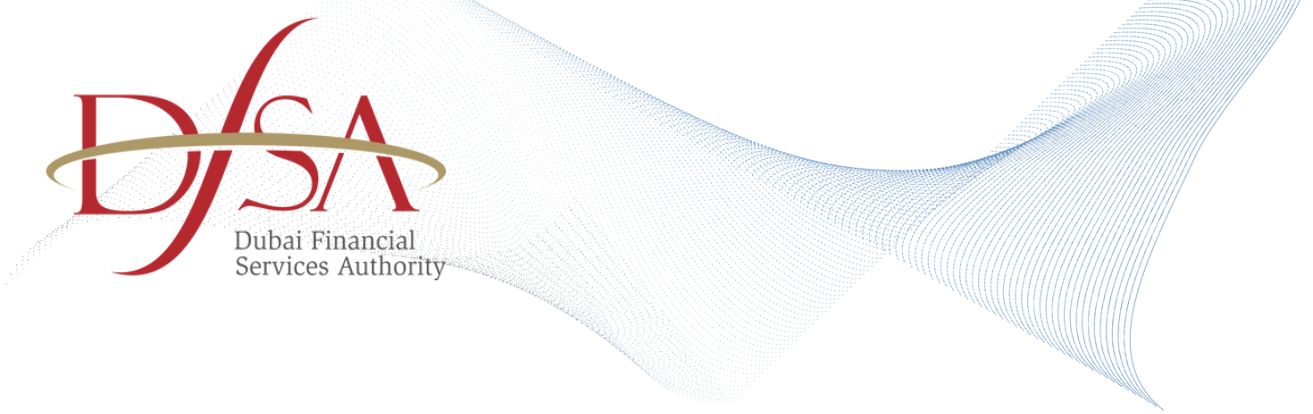
CYBER THEMATIC REVIEW | 2022



Contents

Foreword

It is my pleasure to present the 2nd edition of the Dubai Financial Services Authority's (DFSA) Cyber Thematic Review Report which summarises improvements Firms have made since our first review concluded in 2020. Our priorities for the past two years were to improve cybersecurity awareness in the Dubai International Financial Centre (DIFC), promote the sharing of cyber threat information, and support the continued development of cyber resilience within Firms in the DIFC. The results demonstrate that our efforts are paying off.

Strong digital infrastructure is essential to achieving greater operational and cyber resilience. Digital transformation has been a key priority for the financial services industry for a number of years. At the onset of the Covid-19 pandemic in early 2020, most Firms had to switch to remote working arrangements almost immediately, because of lockdown restrictions. Those who hadn't previously made investments in their IT infrastructures faced more challenges than those who were further along in their digital transformation. Technological innovation and digital transformation are, without a doubt, accelerating. Therefore, we must acknowledge many new risks. The more complex the digital infrastructure becomes, the more vulnerabilities are identified, requiring Firms to intensify their cybersecurity efforts and strengthen their cyber controls.

Cyber security remains one of the DFSA's top priorities. We expect Firms to invest in sufficient safeguards to protect against a cyber-attack. Moreover, we expect Firms to have appropriate responses when they experience an attack. This includes maintaining a robust Governing Body to oversee cyber-risk management; effective hygiene practices; and thorough response and recovery plans.

At the DFSA, over the past three years, we have been steadily increasing the intensity of our cyber risk supervision programme. We take a cooperative approach to addressing cyber threats by engaging with government agencies, financial institutions and cybersecurity experts. The most effective way to understand the challenges in addressing the cyber threats is to work together.

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

Justin Baldacchino
Managing Director - Supervision

Executive Summary

The purpose of this Report (Report) is to summarise key findings from the Cyber Thematic Review 2022 (Review) launched by the DFSA in January 2022. The Review was designed to assist in determining:

- the status of areas identified as needing improvement in the Cyber Thematic Review Report of 2020;
- the consistency of cyber risk management practices implemented by Authorised Firms, Authorised Market Institutions and Registered Auditors (collectively referred to as Firms) with the DFSA Cyber Risk Management Guidelines (Guidelines); and
- the current maturity level of cybersecurity frameworks implemented by Firms.

The Review assessed cyber risk governance frameworks, cyber hygiene practices, and resilience programmes and compared results with the outcomes of the 2020 review.

The Review was conducted via an online questionnaire seeking information on each Firm's cyber security practices and consisted primarily of multiple-choice questions. The questionnaire was sent to a total of 512 Firms. We were particularly pleased to have a 92% response rate, an increase of 12% compared to the 2020 review.

This Report does not include all identified issues and observations. It describes only key findings and observations to summarise the overall status of improvements in the cyber risk management practices of Firms. Not all of the findings and observations noted in this Report are relevant to all Firms. Therefore, Firms should read this Report taking into consideration the nature, scale, and complexity of their business and in conjunction with the Cyber Thematic Review Report 2020. Firms should use this Report as instructive information and not as a comprehensive guide to cyber risk management.

The Review identified a material improvement in overall cyber maturity in that Firms have made improvements in most of the control areas assessed in the 2020 review. In particular, the review identified significant improvements in third-party cyber risk management and user authentication controls, including strong password requirements and Multi-factor Authentication. However, despite measurable improvement, all 14 key findings from the Cyber Thematic Review Report 2020 continue to require Firms' attention.

Unfortunately, the Review identified that Firms did not improve their practices in three areas: incident response testing programme; Vulnerability Assessments and Penetration Testing; and IT asset identification and classification.

The Review also identified that the overall implementation of the Guidelines is improving.

- On average, Firms implemented 80-90% of the governance practices described in the Guidelines. Notwithstanding, and despite the significant improvements made by Firms compared to the 2020 review, the implementation of the third-party risk management section of the guidelines showed a lower implementation rate of 70%.
- Firms declared that, on average, they have implemented 90% of the practices described in the Hygiene section in the Guidelines. However, there was significantly less adoption of guidance elements related to encryption and cybersecurity testing.
- Resilience is the area with the lowest implementation rates. Firms declared that, on average, they had implemented only 60-75% of the resilience practices identified in the Guidelines. The low rates reflect the fact that in many instances Cyber Incident Response Plans prepared by Firms do not include important elements of an effective cyber response. Moreover, a significant number of Firms have not tested their Cyber Incident Response Plans in the past year.

The status of findings of the Cyber Thematic Review of 2020

The 2020 Cyber Thematic Review highlighted important areas for improvement within the cyber risk management practices of Firms operating in the DIFC. This Review assessed Firms' response to the 2020 review and whether Firms have made necessary improvements. The findings were grouped into four tiers to present the level of improvements Firms had made in comparison with the 2020 review results:

- significantly improved (more than 20% of Firms improved their practices);
- improved (12 – 20% of Firms improved their practices);
- little improved (4 – 12% of Firms improved their practices); and
- no change (less than 4% of Firms improved their practices).

The table below shows the level of improvement to control areas that Firms have made since the 2020 review. The higher the area is placed on the list the higher the level of improvement that was noted. The number to the left of each "Area for improvement" corresponds to the numbered paragraphs that follow the table.

Category	Area for improvement	Status
Governance	4. Third-party cyber risk management	**Significantly improved**
Hygiene	8. Multi-factor Authentication for external access (e.g. VPN, webmail)	
Hygiene	9. Encryption of data stored on hard drives and portable devices	**Improved**
Resilience	11. Cyber incident response planning and preparation	
Governance	3. Board and senior management responsibilities and understanding of cyber risks	
Governance	6. Cyber training and awareness campaigns	
Resilience	10. Continuous monitoring, detection and response capabilities	
Resilience	12. Crisis communication plans (internal/external)	
Governance	2. Cyber risk identification and assessment capabilities	
Resilience	14. Information sharing	**Little improved**
Governance	1. Cyber risk management framework	
Resilience	13. Incident response testing programme	**No change**
Hygiene	7. Vulnerability Assessments and Penetration Testing	
Governance	5. IT asset identification and classification	

The Review identified that Firms have made significant improvements in regard to third-party cyber risk management and user authentication controls, including password requirements and Multi-factor Authentication for external access (e.g. VPN, webmail). In the following sections, the Report describes the status of improvements Firms have made relative to each key finding outlined in the Cyber Thematic Review Report 2020. The following sections contain only summaries of the findings without detailed descriptions of issues and our expectations. For detailed descriptions please refer to the Cyber Thematic Review Report 2020.

Governance

1. Cyber risk management framework

The 2020 review noted that a significant number of Firms had not implemented a cyber risk management framework. As a consequence, many Firms' cyber risk management activities tended not to be properly coordinated and were performed on an ad hoc basis.

This Review identified a slight improvement in this area as 8% more Firms have now 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. Similar improvement was noted regarding the implementation of a formal information security policy and a description of roles and responsibilities for individuals and bodies involved in cyber risk management during business-as-usual operations, including accountability for decision making.

2. Cyber risk identification and assessment capabilities

In 2020, most Firms declared that they identified and assessed cyber risks. However, the 2020 review found that a significant number of Firms performed only a limited cyber risk assessment that considered only the availability of IT systems, without sufficient attention to the sensitivity of processed data.

The current Review results show that the number of Firms formally identifying and assessing the risk has risen to 89% (an increase of 13%). Moreover, the involvement of senior management in the periodic assessment of cyber risks and mitigating controls has also increased to 82% (an increase of 15%). The results also show that Firms pay more attention to the sensitivity of data and not only availability. However, this aspect cannot be easily quantified without detailed analysis of numerous cyber risk assessments prepared by Firms. We will continue to assess this practice during our cyber risk assessments.

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

The 2020 review identified that 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 evident in the fact that there was a lack of senior management review of cyber security audits, reviews and tests.

In the current Review, Firms declared improvements in all aspects of the Governing Body and senior management oversight. More than 82% of Governing Bodies (an increase of 15%) receive information on cyber risks and relevant mitigating controls on a periodic basis, mostly quarterly. A similar improvement was noted regarding the other areas of the Governing Body oversight responsibilities. 18% more Governing Bodies receive management reports on identified Cyber Incidents. Also, the Review identified significant improvements in the Governing Body and senior management oversight of third-party risk management practices.

4. Third-party cyber risk management

The 2020 review identified that only half of all Firms had a due diligence process to assess whether third-party service providers (TPSPs) meet the Firm's cyber security requirements and even fewer Firms periodically tested whether the TPSPs continued to satisfy the Firm's cyber security requirements.

This year, almost 74% of Firms declared that they follow a due diligence process to ensure that TPSPs meet cybersecurity requirements as defined by the Firm, before the TPSP can access the Firm's data or information systems. This represents a 23% increase compared to the 2020 review. It remains a concern that 26% of Firms still don't have a sufficient TPSP due diligence process.

The review also identified a significant improvement in the number of Firms that periodically verify that TPSPs continue to satisfy the Firm's cybersecurity requirements. In particular, 65% of Firms have implemented this practice compared to 31% (an increase of 34%) in the 2020 review. We will continue to monitor this area and periodically assess the implementation of the third-party risk management practices. We expect all Firms to implement TPSP due diligence and review processes.

5. IT asset identification and classification

The previous review showed that many Firms identified and classified their IT assets. However, Firms mostly focused on IT equipment only and did not identify and classify information and IT systems or did that in an informal manner on an ad hoc basis.

The current Review specifically asked Firms whether they classified IT assets (hardware and software) based on their criticality as well as sensitivity. More than 85% of Firms (similar to the previous review) answered positively. However, this aspect requires additional verification through the detailed analysis of numerous IT asset lists prepared by Firms. We will continue verifying this practice during our cyber risk assessments.

6. Cyber training and awareness campaigns

The 2020 review identified a significant number of Firms which did not establish 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 Firms tended to be ad hoc rather than at regular intervals.

The 2022 Review identified that more than 80% of Firms organised at least one cybersecurity training for their employees in the past year (an increase of 14%) and more than two-thirds of Firms did the same for their Governing Bodies. During the discussion with Firms, we noted that many Firms regularly organise cyber trainings and in some instances the participation in the cyber trainings is reflected in the annual employee performance assessment.

Hygiene

7. Vulnerability Assessments and Penetration Testing

The previous review identified that a significant number of Firms did not perform Vulnerability Assessments or Penetration Tests of their critical information systems.

Unfortunately, the Review has not identified any improvement in this area. We would like to remind Firms that they should use a variety of methods to test critical IT infrastructure and information systems, including Vulnerability Assessments, scenario-based testing, Penetration Tests and/or red team exercises. Regular

Vulnerability Assessments and Penetration Tests enable Firms to identify known cyber security vulnerabilities that may affect the Firm's systems, infrastructure and processes. We will continue verifying this practice during our cyber risk assessments.

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

The 2020 review identified that in cases where information systems were accessible from the Internet, some Firms relied on basic user authentication using usernames and passwords. In addition, some Firms had 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).

Currently, most Firms have Multi-factor Authentication enabled for systems that can be accessed from the Internet. The Review identified a significant improvement of 22% comparing to the previous review. Moreover, almost all Firms implemented strong password policies to their IT systems (an increase of 18%).

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

In 2020, a number of small and medium-sized Firms did not enforce encryption of workstation hard drives and portable devices to protect sensitive data. This review identified a material improvement. However, there are still many Firms that should implement these controls to their IT environments and we will be closely monitoring Firms' progress in this area.

Resilience

10. Continuous monitoring, detection and response capabilities

The previous review showed that half of all Firms did not have continuous identification and response capabilities for managing Cyber Incidents related to information systems. Small and medium-sized Firms relied mainly on manual processes to monitor their infrastructure only during working hours or did not have monitoring capabilities at all.

Based on the questionnaire responses, an overall improvement of 17% in this area was noted. Currently, 75% of Firms declared that they have implemented procedures for detecting, monitoring, analysing and responding to Cyber Incidents. However, the quality of improvements must be verified during the cyber risk assessments as this process and technical controls applied are complex and require detailed examination.

11. Cyber incident response planning and preparation

The previous review identified that many Firms 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 were addressed in general terms as components of the business continuity plan and were not tailored specifically to cyber threats.

The Review identified an improvement in this area. More Firms (an increase of 16%) supplemented their plans with a description of procedures for responding specifically to Cyber Incidents as well as definitions of incident management roles and responsibilities. Moreover, 13% more Firms implemented procedures for post-incident review.

12. Crisis communication plans (internal/external)

In 2020, half of all Firms declared that they implemented a crisis management communication plan that addresses external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement) and even fewer Firms implemented an internal crisis communication plan (designed for relevant business units, senior management, Governing Body, etc.).

A 13% improvement in this area was noticed during the Review as more than 65% of Firms stated they have the internal and external communication plans prepared and ready to use in case of a material Cyber Incident. Still, there is a room for improvement as more than one third of Firms have not implemented communication plans. We would like to remind Firms that 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.

13. Incident response testing programme

The previous review showed that more than half of Firms' Cyber Incident Response Plans did not include a formal requirement for periodically testing the Firm's response to a Cyber Incident. Moreover, the Review identified that a similar percent of Firms had not tested any component of their Cyber Incident Response Plans in the past year.

Unfortunately, The Review has not identified improvements in this area. The percentage of Firms that have not tested their Cyber Incident Response Plan in the past year remained steady around 50%. Some Firms added a formal requirement for periodically testing the Firm's response to a Cyber Incident to their plans. The number of Firms that haven't tested their Cyber Incident Response Plans is very concerning and we will closely monitor improvements in this area and will be verifying the status of testing during our cyber risk assessment.

14. Information sharing

The 2020 review identified that some small and medium-sized Firms used professional forums or groups to get information about particular cyber threats but tended not to share information about Cyber Incidents. Since then, the number of Firms subscribing to the threat intelligence platforms has slightly risen and currently 59% of Firms use this tool to exchange information about cyber threats (an increase of 10%). Moreover, since January 2019 more than 200 Firms have registered to the DFSA Cyber Threat Intelligence Platform (TIP), which shares an average of 170 threats each week.

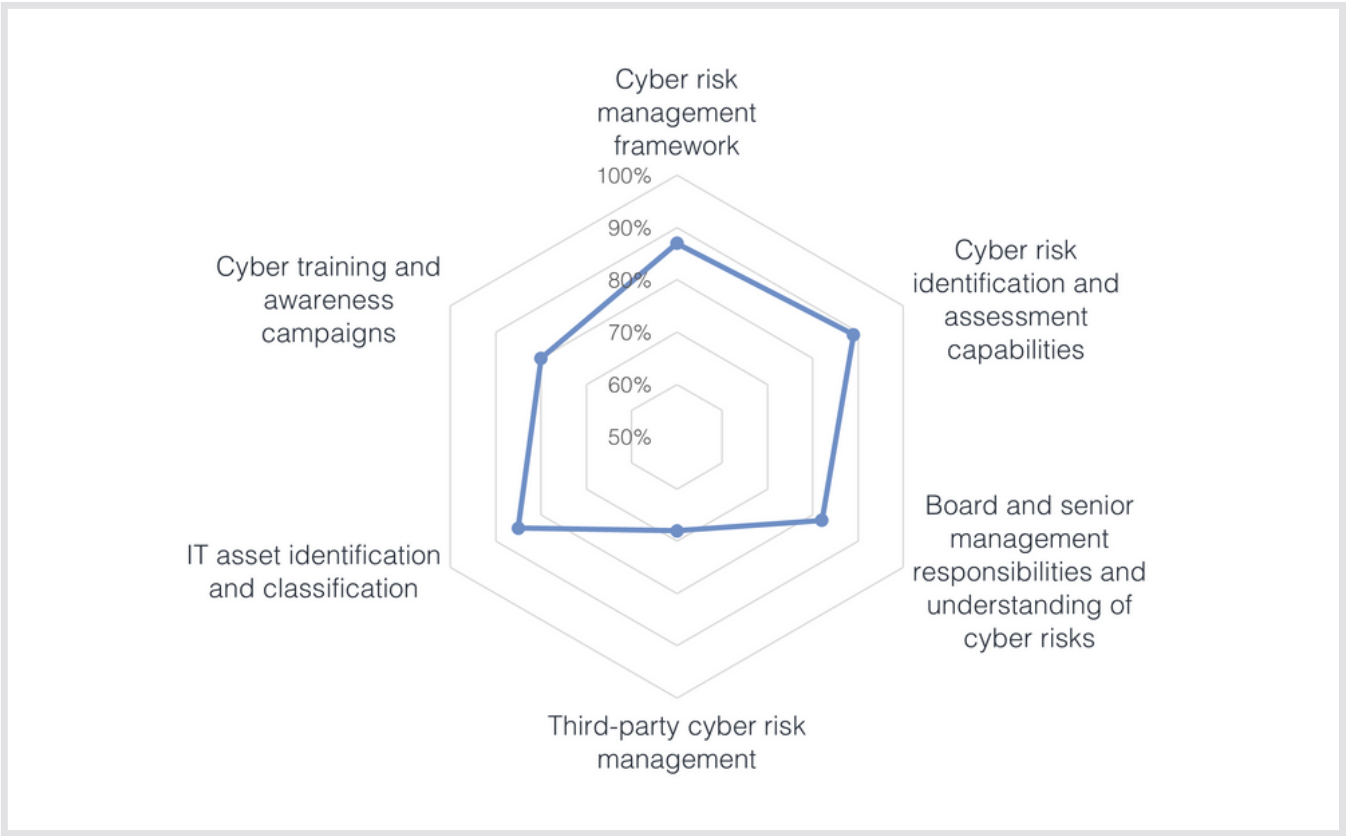
Implementation status of the DFSA Cyber Risk Management Guidelines

The questionnaire was specifically designed to assist in determining the overall consistency of Firms' cyber risk management practices with the DFSA Cyber Risk Management Guidelines issued in December 2020. 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.

The questionnaire responses were analysed and observations were grouped into the three main categories of governance, hygiene and resilience.

Governance

The chart below shows the levels of overall consistency of Firms' governance practices with the Cyber Risk Management Guidelines.

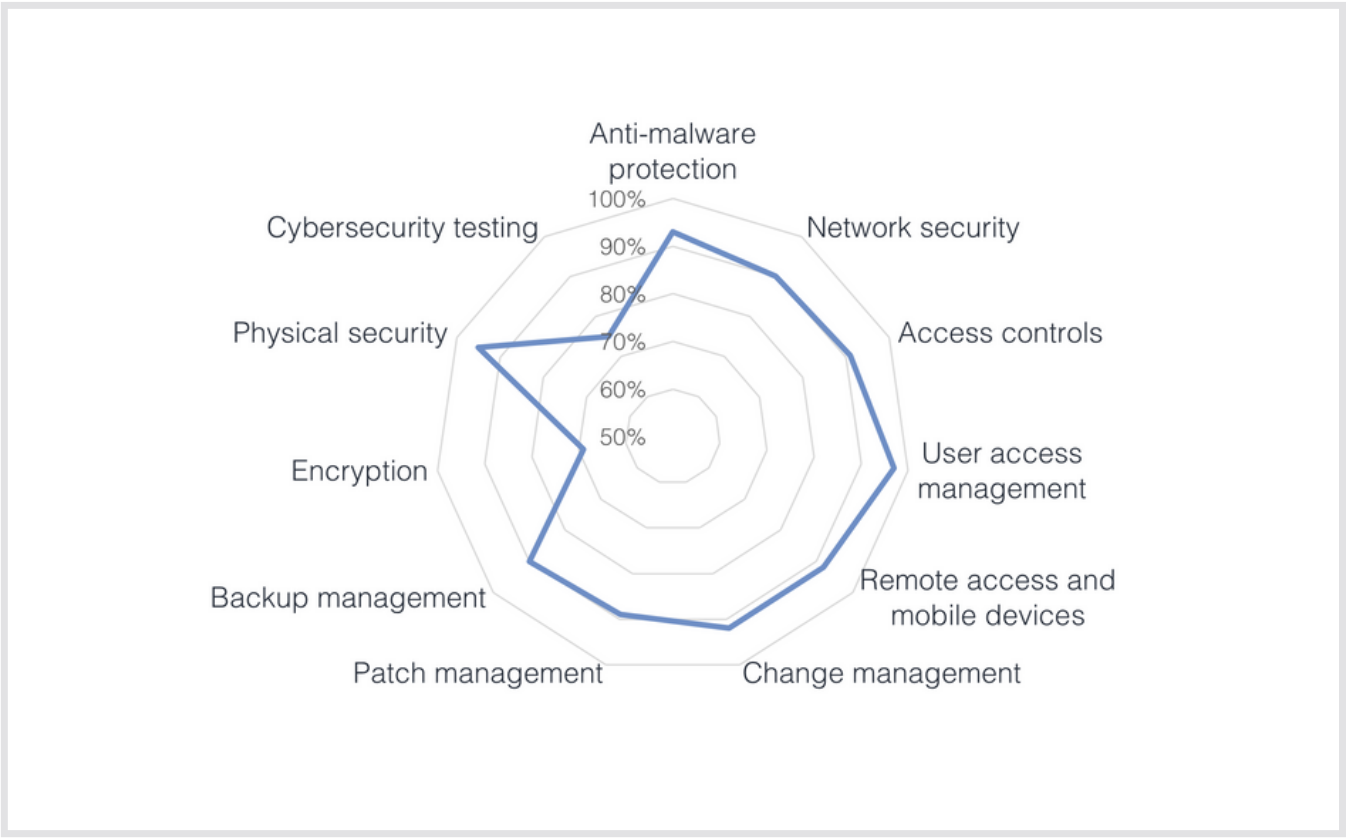


Overall implementation of the IT/cyber governance elements of the Guidelines is improving. Firms implemented approximately 80-90% of the governance practices described in the Guidelines, with the exception of third-party risk management processes, where the implementation rate is lower than 70%. Despite a significant increase in number of Firms applying third-party risk management practices, in comparison to the 2020 review, there is significant room for improvement in this area.

The findings and expectations described in the Governance section of the previous Cyber Thematic Review Report remain valid. The governance practices described in the Guidelines should be acknowledged and implemented by all Firms. Proper IT governance practices are crucial to establish an effective cyber risk management framework.

Hygiene

The chart below illustrates the levels of overall consistency of Firms' hygiene practices with the DFSA Cyber Risk Management Guidelines.



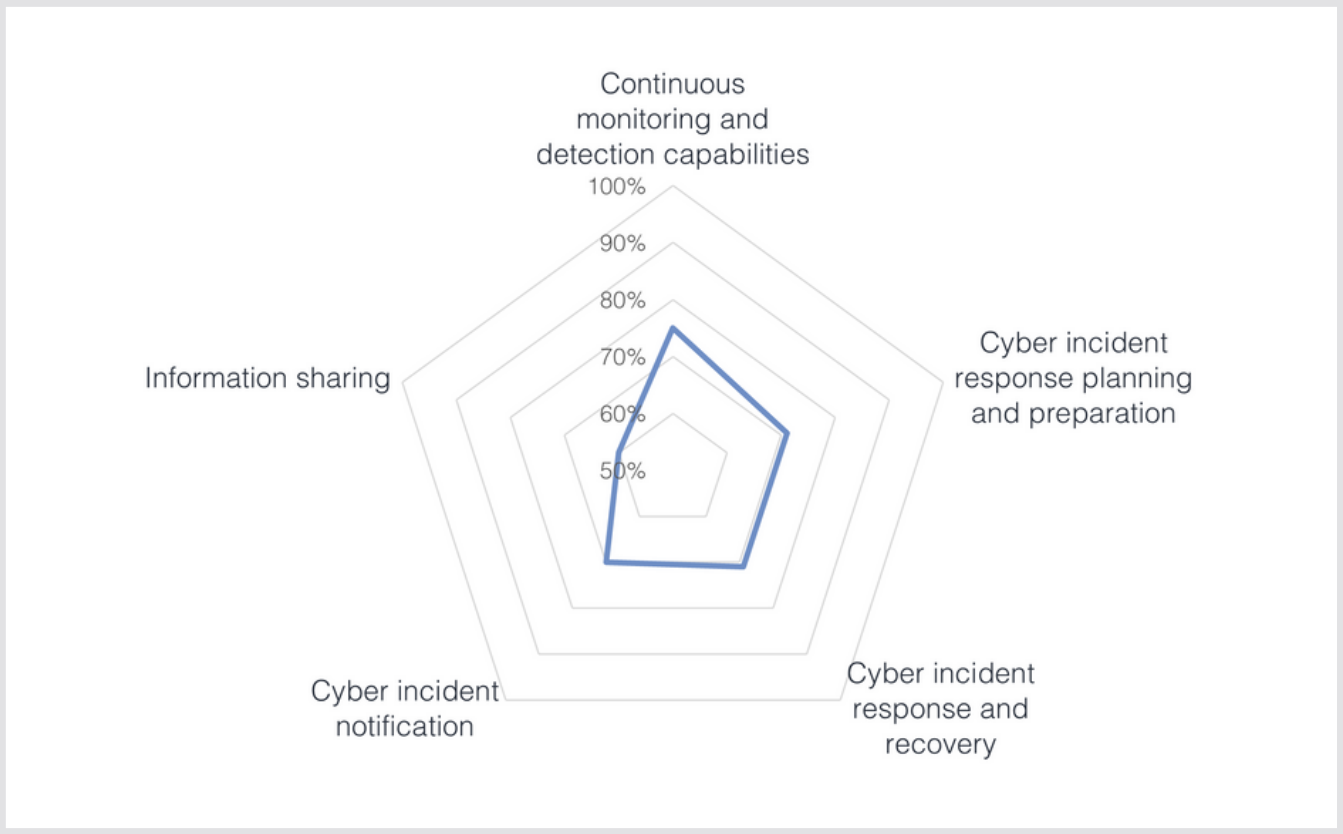
In the current Review, Firms declared that, on average, they have implemented 90% of practices described in the Hygiene section of the Guidelines. However, encryption and cybersecurity testing were identified as two exceptions. Regarding encryption, on average, Firms have implemented 69% of practices described in the Guidelines and an overall improvement of 18% was noted. However, the number of Firms that have not enforced expected controls related to encryption of hard drives and portable devices is still significant.

The low implementation rate related to cybersecurity testing is driven by the fact that many Firms still do not perform regular Vulnerability Assessments and Penetration Tests. This is especially concerning in the context of internet-facing systems which should be tested regularly and whenever systems are updated or deployed.

On the other hand, almost all Firms implemented expected controls in three other areas: user access management; physical security; and anti-malware protection which helps in keeping at least a basic level of defence against cybersecurity threats.

Resilience

The chart below shows the levels of overall consistency of Firms' resilience practices with the DFSA Cyber Risk Management Guidelines.



Resilience is the area with the lowest implementation rate. The low rate reflects the fact that in many cases Cyber Incident Response Plans prepared by Firms do not include important elements of an effective cyber response. Moreover, a significant number of Firms have not tested their Cyber Incident Response Plans in the past year.

The weakest result is related to information sharing. Only 59% of Firms subscribed to a cyber threat intelligence platform. 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.

Enhancing the cyber resilience of Firms operating in or from the DIFC is one of our top priorities and we will be focusing on this area during the cyber risk assessments.

Next steps

We continue to give focus to how effectively Firms mitigate cyber risk. Our priorities in cyber risk supervision remain unchanged. We work to improve cybersecurity awareness in the DIFC, promote the sharing of cyber threat information, and support continued development of cyber resilience within Firms in the DIFC.

In 2021, we began conducting firm-specific cyber risk focused risk assessments. The purpose of the assessments is to assess whether Firms have improved their cyber risk systems and controls following the 2020 cyber thematic review; and whether Firms have begun to implement the Guidelines we issued in December 2020.

We will continue conducting the cyber risk assessments and verifying the implementation status of the Guidelines. During our cyber risk assessments, we will take into consideration the results of the current Review, and assess Firms' practices with particular attention to the following areas:

- Cyber risk identification and assessment capabilities,
- Third-party cyber risk management,
- IT asset identification and classification,
- Encryption techniques,
- Vulnerability Assessments and Penetration Testing,
- Continuous monitoring, detection and response capabilities,
- Incident response testing programme.

Moreover, we plan to perform cyber thematic reviews in two-year cycles to check the maturity level of cybersecurity frameworks implemented by Firms.

We will also continue hosting events aimed at raising cyber awareness. Our approach includes outreach sessions, forums and roundtable discussions dedicated to cyber security topics. Moreover, we plan to engage relevant institutions in cyber simulations that help them to test their response to cyber incidents and assess their cyber resilience. We will be informing Firms about upcoming events and other initiatives through SEO letters and announcements on our website.

Glossary

Cyber Incident – An event that:

- jeopardises the cybersecurity of an information system or the information the system processes, stores or transmits; or
- violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

Cyber Incident Response Plan – The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a Cyber Incident.

Governing Body – 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.

Multi-factor Authentication – The use of two or more of the following factors to verify a user's identity:

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

Penetration Testing – 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 – 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.


DFSA
Dubai Financial
Services Authority