iComply

Cyber Risk Management Guidelines

The Dubai Financial Services Authority (DFSA) issued the Cyber Risk Management Guidelines to all authorised firms operating in the Dubai International Financial Centre (DIFC) on the 22nd of December 2020. The key objective is to ensure that Firms have in place an appropriate framework for the identification and management of cyber risks that include IT systems & controls and governance arrangement for effective management and preparedness.

Introduction

The Guidelines are statements of industry best practices which a Firm may adopt, taking into account the complexity of operations and the diversity, scale and scope of business activities in which it engages. The Guidelines are principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. This should be read in conjunction with the *G7 Fundamental Elements of Cybersecurity for the Financial Sector*. The link to this document is attached below:

https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en

All firms should review their internal processes and conduct a gap-analysis to identify and enhance their processes, systems and controls. The guidelines are categorised under 3 topics namely Governance (framework), Hygiene (protection) and Resilience (detection).

A summary of the guidelines is as follows:

Governance

A Firm's Board and senior management are responsible for establishing the cyber risk management framework and ensuring that it is followed and cyber risk is effectively managed.

The guidelines expects all Authorised Firms to:

- implement a cyber risk management framework to provide a structure within which to identify, manage, and mitigate cyber risks effectively in an integrated and comprehensive manner
- customize the framework to the Firm's size, complexity, and risk appetite and align with the overall risk management framework
- implement framework based on the existing industry standards and recognised professional institutions

- clearly define roles and responsibilities, including accountability for decision making and delegation of authority
- determine threats and vulnerabilities to their IT environment which comprises network, hardware, software, systems and interfaces, processes, people, and data
- implement controls appropriate for the criticality and sensitivity of the information system assets and the level of the Firm's risk appetite
- identified risks and controls should be monitored on an ongoing basis and updated
- present management information to the Board in a way that can be easily understood and analysed
- address cybersecurity requirements in agreements with third parties which involve accessing, processing, communicating or managing the Firm's data
- identify and classify IT assets based on their criticality and sensitivity in order to ensure that all IT assets receive an appropriate level of protection
- establish a comprehensive cybersecurity training programme and a cyber awareness campaign to enhance the overall cybersecurity awareness level
- ensure that all new employees read and understand the information security policy

Hygiene

Appropriate IT infrastructure should be in place to assist Firms to have a robust cyber security incident prevention. In ensuring the same Firms should:

- deploy anti-malware software to servers and workstations and update them regularly
- use anti-malware software to scan any files received over networks
- install network security devices like firewalls, intrusion detection and prevention systems
- implement network surveillance and security monitoring procedures
- enforce strong password controls over users' access to systems and networks
- implement multi-factor authentication (MFA) to all accounts in systems that can be accessed from the Internet
- grant access rights and system privileges based on job responsibility, and closely supervise access given to third parties
- limit access to administrative accounts to authorised IT employees
- immediately revoke user access to systems and networks if it is no longer required
- apply enhanced security controls to secure communication between a remote user and the Firm's infrastructure
- ensure that mobile devices used to access the Firm's systems and data are properly secured
- establish a change management process to ensure that changes and patches to production systems and hardware devices are assessed, tested, approved and implemented in a controlled manner
- establish patch management procedures including the identification, categorisation and prioritisation of security patches
- implement backup procedures for critical systems and data

- implement encryption techniques to protect sensitive information stored on workstation hard drives and portable storage media
- limit access to datacentres and server rooms to authorised personnel only
- periodically test IT infrastructure and systems, including vulnerability assessments, scenario-based testing, penetration tests and/or red team exercises, depending on the results of the Firm's cyber risk assessment

Resilience

Early detection provides useful lead time to mount appropriate counter measures against a potential breach, and allows proactive containment of actual breaches. In realizing the same Firms should:

- apply ongoing monitoring of their IT infrastructure to detect the occurrence of anomalies and events indicating a potential cyber incident
- regularly review system logs recording user activities, warnings, errors and security events to identify suspicious activities
- implement a robust cyber incident response plan
- ensure that cyber incident response and recovery processes are closely integrated with crisis management, business continuity and disaster recovery planning
- provide the regulator with consistent and timely information regarding material cyber incidents
- participate in threat intelligence sharing communities, whether through intelligence sharing platforms, professional forums, or other information sharing communities, to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats to improve their cyber response and remain up-to-date in their defences

Reference

https://www.dfsa.ae/your-resources/publications-reports/seo-letters

https://365343652932-web-server-storage.s3.eu-west-2.amazonaws.com/files/1216/0863/2796/20201222_Dear_SEO_Letter_Cyber_Risk_Management_Guidelines.pdf

Contact us for more information

iComply Risk Management Limited
Wework Hub71, Al Khatem Tower,
ADGM Square, Al Maryah Island,
Abu Dhabi, United Arab Emirates
Phone: +9714 4326801
Mobile: +97150 5350068