limitless consulting

The 2024 Cyber Thematic Review conducted by the Dubai Financial Services Authority (DFSA) assesses the cyber risk management maturity of firms within the Dubai International Financial Centre (DIFC). This initiative evaluates governance, hygiene, and resilience in light of the evolving cybersecurity threat landscape, aiming to enhance the overall cybersecurity framework across the DIFC.

Cyber Thematic Review 2024 – Key Highlights

<70% Compliance with third-party risk management remains below this %.

80 - 90% No. of firms that have implemented governance practices are between 80 to 90%.

90%> No. of firms who have declared that they identify and classify their IT assets.

<80% Despite improvements, implementation of resilience requirements remains below 80%.

35% There is a concern that 35%of firms do not conduct incident response testing on a regular basis.

Key Themes and Findings:

1. Governance Challenges

Governance remains a critical area where firms, especially Small and Medium Enterprises (SMEs), face significant obstacles:

- **Cyber Governance Frameworks:**

  SMEs often lack structured and consistent governance frameworks. This absence results in ad-hoc approaches to cybersecurity management, undermining the effectiveness of IT and cyber controls. Moreover, senior management and governing bodies frequently lack adequate oversight of cyber risk programs, with limited engagement in reviewing findings from cybersecurity audits or assessments.

- **Cyber Risk Assessment:**

  Significant number of firms perform a limited cyber risk assessment focused only on the availability of IT systems, without sufficient attention to the sensitivity of processed data.

- **Third-Party Cyber Risk Management:**

  Many firms fail to conduct adequate due diligence on third-party providers or include cybersecurity clauses in contractual agreements. Periodic reviews to ensure continued compliance are also lacking.

Key Themes and Findings (Continued):

2. Cyber Hygiene Gaps

Cyber hygiene practices, while improving, continue to demonstrate critical gaps:

- **Encryption:**

  Implementation of encryption techniques for securing data at rest and in transit remains inconsistent. This creates vulnerabilities, particularly for sensitive data stored on removable media or unprotected devices.

- **Vulnerability Assessment & Penetration Testing :**

  Firms primarily rely on basic automated scans for vulnerability assessments, neglecting comprehensive methods such as penetration testing, red teaming, or scenario-based assessments. This leaves critical IT infrastructure inadequately tested against sophisticated threats.

3. Resilience Shortcomings

Despite progress, resilience efforts show significant areas for enhancement:

- **Incident Response Plans (IRPs):**

  The plans were stated in general terms and not tailored specifically to cyber threats. The majority of small or medium-sized Firms have not developed response plans/playbooks for different common cyber-attack scenarios. Moreover, there were a number of instances where Firms had not reviewed and updated their plans on a regular basis.

Key Themes and Findings (Continued):

3. Resilience Shortcomings

- **Threat Intelligence Sharing:**

Only 66% of firms are active participants in Cyber Threat Intelligence Platforms (TIP), limiting the collective capability to preempt and respond to threats. Moreover, delays in notifying the DFSA about material incidents often extend beyond the required 72-hour timeframe.

- **Reliance on External Providers:**

SMEs disproportionately depend on external service providers without adequate oversight. This lack of internal control over outsourced activities increases exposure to cyber risks.

- **Cybersecurity Training:**

Training for staff and management is inconsistent across firms, particularly for SMEs. Many fail to update training content to address emerging risks or use interactive methods like phishing simulations. This results in a workforce that is insufficiently prepared to identify and respond to cyber threats.

limitless consulting

Recommendations:

1. Enhancing Frameworks

- Firms must adopt comprehensive cyber risk management frameworks aligned with DFSA rules.
- Senior management must actively oversee cyber risk activities.

2. Strengthening Hygiene

- Broader implementation of encryption and cybersecurity testing is essential.
- IT asset registers should be updated regularly to reflect current systems and mitigate risks.

3. Improving Resilience

- Develop and regularly test robust incident response plans ensuring inclusion of tailored crisis communication protocols.
- Increase engagement in cyber threat intelligence platforms for information sharing.

4. Fostering Awareness

- Annual training programs and phishing simulation campaigns should be standard.
- Cybersecurity strategies should be informed by emerging trends.