Summary

Prepared by NASCUS Legislative and Regulatory Affairs Department
November 7, 2014

FFIEC Cybersecurity Assessment General Observations

The Federal Financial Institutions Examination Council (FFIEC) has released its "observations" resulting from a cybersecurity exam work program (Cybersecurity Assessment) conducted at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. FIIEC stressed that the "observations" should not be construed as guidance.

Not surprisingly, FFIEC found the level of cybersecurity inherent risk varied significantly across financial institutions. An institution's cybersecurity inherent risk is the amount of risk posed by its operations. Management should understand how their operations affect their cybersecurity risk. For example, an institution's various connection types each represent a unique point of entry for potential attacks. These connection types might include:

- virtual private networks
- wireless networks
- local area networks
- employees' own devices

Because every connection represents a potential entry point for attacks, it is important for management to consider whether their financial institution needs of all of its connections. Management should also risk assess each connection and access point.

Cyber attackers develop techniques to target specific products and services, therefore each product or service may present unique risks to the institution. Understanding the threats presented b by each product or service helps management identify, assess, and mitigate the financial institution's specific risks. Likewise, the diverse array of technologies used by financial institutions adds to the possible vulnerabilities to be assessed.

Cybersecurity Preparedness

In reviewing financial institutions' current cybersecurity practices and overall preparedness, the Cybersecurity Assessment focused on five key areas.

1) Risk Management and Oversight

While many financial institutions discuss cybersecurity with boards, management, and staff when cyber-attacks are widely reported or when the financial institution experiences an attack, FFIEC notes that routinely discussing cybersecurity issues helps build a security culture. Other elements of a strong risk management and oversight culture include clearly defining roles, responsibilities and accountability to identify, assess, and manage cybersecurity risks across the financial institution.

2) Threat Intelligence and Collaboration

Threat intelligence is the acquisition and analysis of information to identify, track, and predict cyber-capabilities, intentions, and activities that offer courses of action to enhance decision making. It includes gathering, monitoring, analyzing, and sharing information from multiple sources on cyber threats and vulnerabilities. Management should maintain awareness of developing cybersecurity threats and vulnerabilities so they may evaluate risk and respond accordingly. FFIEC suggests management participate in information sharing forums as well as maintain and monitor event logs to enhance their ability to understand trends, react to threats, and improve internal reporting.

3) Cybersecurity Controls

Cybersecurity controls can be preventive, detective, or corrective. Preventive controls, those that impede unauthorized access to a financial institution's systems need to be reviewed and adjusted as the institution changes its information technology (IT) environment. FFIEC notes that institutions may wish to consider encrypting a variety of sensitive data in addition to customer/member information such as proprietary and technical information.

Detective controls such as anti-virus and anti-malware tools can help identify previously undetected attacks on the institution. FFIEC recommends that financial institutions also routinely scan IT networks for vulnerabilities and anomalous activity, and test systems for their potential exposure to cyber-attacks.

Corrective controls should be in place to remediate vulnerabilities identified by the institution. A review of reports of corrective controls by management, of both the institution's corrective controls and those of their third party service providers, provides a more complete view of their financial institutions' cybersecurity risk.

4) External Dependency Management

External dependency management includes the institution's oversight of their connectivity to third-party service providers, business partners, customers, or others. Institutions should evaluate a third party's cybersecurity controls before entering into a business relationship with that third party that includes some form of cyber connectedness.

5) Cyber Incident Management and Resilience

Cyber incident management involves incident detection, response, mitigation, escalation, reporting, and resilience. To mitigate against reputation risk, financial institutions should have procedures for managing the aftermath of a cyber-attack. Such procedures might include, as appropriate, notifying customers, regulators, and law enforcement when incidents affect personally identifiable customer information. Management should consider expanding existing business continuity and disaster recovery plans to incorporate cyber incident scenarios.

-End-

B/K