FFIEC CYBERSECURITY ASSESSMENT GENERAL OBSERVATIONS

During the summer of 2014, Federal Financial Institutions Examination Council (FFIEC) members[1] piloted a cybersecurity examination work program (Cybersecurity Assessment) at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. This document presents general observations from the Cybersecurity Assessment about the range of inherent risks and the varied risk management practices among financial institutions and suggests questions for chief executive officers and boards of directors to consider when assessing their financial institutions' cybersecurity and preparedness. This document should not be construed as guidance. Related guidance appears at the end of the document.

CYBERSECURITY INHERENT RISK

The Cybersecurity Assessment found that the level of cybersecurity inherent risk varies significantly across financial institutions. It is important for management to understand the financial institution's inherent risk to cybersecurity threats and vulnerabilities when assessing cybersecurity preparedness. Cybersecurity inherent risk is the amount of risk posed by a financial institution's activities and connections, notwithstanding risk-mitigating controls in place. A financial institution's cybersecurity inherent risk incorporates the type, volume, and complexity of operational considerations, such as connection types, products and services offered, and technologies used.

Questions to Consider

- What types of connections does my financial institution have?
- How are we managing these connections in light of the rapidly evolving threat and vulnerability landscape?
- Do we need all of our connections? Would reducing the types and frequency of connections improve our risk management?
- How do we evaluate evolving cyber threats and vulnerabilities in our risk assessment process for the technologies we use and the products and services we offer?
- How do our connections, products and services offered, and technologies used collectively affect our financial institution's overall inherent cybersecurity risk?

Connection Types

Financial institutions have numerous access points and use a variety of connection types, including

- virtual private networks
- wireless networks
- telnet, File Transfer Protocol
- local area network that directly connects to other networks or to Internet service providers
- bring your own device (BYOD)

Because each connection represents a potential entry point for attacks, it is important for management to consider whether the financial institution needs to maintain the types and frequency of all of its connections and which connections may be more vulnerable. For example, a financial institution's employees who use their own devices (i.e., BYOD) to connect to their organization's network may inadvertently expose their financial institution to malware.

Products and Services

Because cyber attackers develop techniques to target specific products and services, each product and service may introduce specialized cybersecurity risks. For example, stolen customer or employee credentials can be used by cyber criminals to commit wire transfer or automated

[1] The FFIEC members are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Administration, and the State Liaison Committee.

clearing house (ACH) fraud at a financial institution offering ACH origination. Understanding the threats and techniques attackers use for each product and service helps management to identify, assess, and mitigate the financial institution's specific risks.

Technologies Used

Financial institutions use a vast array of technologies to support their customers and employees, including core systems, automated teller machines (ATM), Internet and mobile applications, and cloud computing.

Each type of technology introduces complexity and potential vulnerabilities. For example, financial institutions offering ATMs may be vulnerable to ATM cash-out scams and financial institutions offering Web-facing services may be vulnerable to distributed denial-of-service (DDoS) attacks.

CYBERSECURITY PREPAREDNESS

In addition to cybersecurity inherent risk, the Cybersecurity Assessment reviewed financial institutions' current practices and overall preparedness, focusing on the following:

- Risk management and oversight
- Threat intelligence and collaboration
- Cybersecurity controls
- External dependency management
- Cyber incident management and resilience

Risk Management and Oversight

Risk management and oversight involves governance, allocation of resources, and training and awareness of employees.

Many boards discuss cybersecurity with management when cyber attacks are widely reported or when the financial institution experiences an attack. Financial institutions generally leverage existing information security policies and practices to address cybersecurity risks. Routinely discussing cybersecurity issues in board and senior management meetings will help the financial institution set the tone from the top and build a security culture. Strong governance includes clearly defined roles and responsibilities that assign accountability to identify, assess, and manage cybersecurity risks across the financial institution.

Questions to Consider

- What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities to our financial institution?
- How is accountability determined for managing cyber risks across our financial institution? Does this include management's accountability for business decisions that may introduce new cyber risks?
- What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

While most financial institutions understand the need to train employees on cybersecurity risk management, the outcome and benefits improve when training and awareness programs are kept current and are provided on a routine basis. Employees can be a financial institution's first line of defense for many types of attacks, particularly social engineering attacks through phishing e-mails, which attempt to acquire sensitive information by masquerading as a trustworthy entity.

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. Threat intelligence and collaboration includes gathering, monitoring, analyzing, and sharing information from multiple sources on cyber threats and vulnerabilities.

Questions to Consider

- What is the process to gather and analyze threat and vulnerability information from multiple sources?
- How do we leverage this information to improve risk management practices?
- What reports are provided to our board on cyber events and trends?
- Who is accountable for maintaining relationships with law enforcement?

Many financial institutions rely on media reports and third-party service providers to gather information on cyber events and vulnerabilities. Financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities so they may evaluate risk and respond accordingly. Participating in information sharing forums (e.g., Financial Services Information Sharing and Analysis Center) is an important element of a financial institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents.

Likewise, many financial institutions share cyber threat information when prompted by law enforcement or regulators. Identifying points of contact for local or federal law enforcement improves a financial institution's ability to respond efficiently to threats before they manifest and to incidents once they occur.

Most financial institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information with other sources of information broadens the financial institution's ability to understand trends, react to threats, and improve reports to management and the board.

Cybersecurity Controls

Cybersecurity controls can be preventive, detective, or corrective.

Questions to Consider

- What is the process for determining and implementing preventive, detective, and corrective controls on our financial institution's network?
- Does the process call for a review and update of controls when our financial institution changes its IT environment?
- What is our financial institution's process for classifying data and determining appropriate controls based on risk?
- What is our process for ensuring that risks identified through our detective controls are remediated?

Most financial institutions implement preventive controls to impede unauthorized access to their systems. Preventive controls need to be reviewed and adjusted when financial institutions change their information technology (IT) environment, such as permitting unpatched devices to connect to their networks. Additionally, many financial institutions encrypt customer information in transit. As a preventive control, financial institutions may also consider classifying and encrypting different types of sensitive data, including proprietary and important technical information.

Most financial institutions have tools in place, such as anti-virus and anti-malware tools, to detect previously identified attacks. In addition to these tools, financial institutions should routinely scan IT networks for vulnerabilities and anomalous activity, test systems for their potential exposure to cyber attacks, and remediate issues when identified.

Most financial institutions have a process for implementing corrective controls to address previously identified vulnerabilities by installing patches on their primary IT system. Given the interconnectedness financial institutions' IT systems and the existence of widespread vulnerabilities, management can have a more complete view of their financial institutions' risk

by reviewing reports on the corrective controls in place across their critical systems and those of their third parties.

External Dependency Management

External dependency management includes the connectivity to third-party service providers, business partners, customers, or others and the financial institutions' expectations and practices to oversee these relationships.

Questions to Consider

- How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?
- What are our third parties' responsibilities during a cyber attack? How are these outlined in incident response plans?

Many financial institutions have processes to manage third-party relationships and document their connections. Before executing a contract, it is important for management to consider the risks of each connection and evaluate the third party's cybersecurity controls. In addition, financial institutions should understand the third parties' responsibility for managing cybersecurity risk and incident response plans.

Cyber Incident Management and Resilience

Cyber incident management involves incident detection, response, mitigation, escalation, reporting, and resilience.

Questions to Consider

- In the event of a cyber attack, how will our financial institution respond internally and with customers, third parties, regulators, and law enforcement?
- How are cyber incident scenarios incorporated in our financial institution's business continuity and disaster recovery plans? Have these plans been tested?

Financial institutions should have procedures for notifying customers, regulators, and law enforcement when incidents affect personally identifiable customer information. Documenting the procedures used for incident detection and response and providing detailed metrics on cyber incidents will inform management and the board and supports the timely escalation and decision making in the event of cyber attacks.

Many financial institutions have business continuity and disaster recovery plans and are able to call on third parties to provide mitigation services when incidents occur. Expanding these to incorporate cyber incident scenarios will improve financial institutions' response capabilities. Additionally, testing plans across business functions and with third parties will help financial institutions identify and manage gaps before cyber attacks occur.

SUMMARY

Today's financial institutions are critically dependent on IT to conduct business operations. This dependence, coupled with increasing sector interconnectedness and rapidly evolving cyber threats, reinforces the need for engagement by the board of directors and senior management, including understanding the institution's cybersecurity inherent risk; routinely discussing cybersecurity issues in meetings; monitoring and maintaining sufficient awareness of threats and vulnerabilities; establishing and maintaining a dynamic control environment; managing connections to third parties; and developing and testing business continuity and disaster recovery plans that incorporate cyber incident scenarios. As a result of the Cybersecurity Assessment, FFIEC members are reviewing and updating current guidance to align with changing cybersecurity risk.

ADDITIONAL RESOURCES

For information on the Cybersecurity Assessment and other cyber-related issues, visit the FFIEC Web site's Cybersecurity Awareness page at www.ffiec.gov/cybersecurity.htm. In addition, FFIEC guidance includes

- *FFIEC Information Technology Examination Handbook*, "Information Security" http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
- *FFIEC Information Technology Examination Handbook*, "Business Continuity Planning" http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx
- *FFIEC Information Technology Examination Handbook*, "Outsourcing Technology Services" http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
- *FFIEC Information Technology Examination Handbook*, "Management" http://ithandbook.ffiec.gov/it-booklets/management.aspx
- *FFIEC Information Technology Examination Handbook*, "Operations" http://ithandbook.ffiec.gov/it-booklets/operations.aspx