BACKGROUND

The Federal Financial Institutions Examination Council (FFIEC) members are raising awareness of cybersecurity threats with financial institutions and critical third-party service providers. The focus has been concentrated on treating cyber threats as an enterprise-wide risk management issue in order to document the avoidance, mitigation and the ultimate understanding and acceptance of these cyber risks.

The National Institute of Standards and Technology (NIST) defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks.

REGULATORY EMPHASIS

In June 2013, the FFIEC announced the creation of the Cybersecurity and Critical Infrastructure Working Group to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups. In addition, the FFIEC began assessing and enhancing the state of the industry preparedness and identifying gaps in the regulators' examination procedures and training that can be closed to strengthen the oversight of cybersecurity readiness.

During the summer of 2014, Federal Financial Institutions Examination Council (FFIEC) members piloted a cybersecurity examination work program (Cybersecurity Assessment) at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks.

Currently, the following key areas have been identified for regulatory oversight:

- **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. 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. 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. 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. 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. 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.

In order to comply with these Cybersecurity guidelines, regulators recommend financial institutions assess the complexity of the institution's operating environment, including the types of communication connections and payments initiated, as well as how the institution manages its information technology products and services; and, to determine the institution's current practices and overall cybersecurity preparedness. In addition, regulators expect Boards and Executive Management to understand the institution's cybersecurity inherent risk; routinely discuss cybersecurity issues in meetings; monitor and maintain sufficient awareness of threats and vulnerabilities;

and, establish and maintain a dynamic control environment including the assurance that there is proper management for connections to third parties. Institutions are also tasked with ensuring cybersecurity incident scenarios and tests are part of any business continuity and disaster recovery planning.

NETBankAudit's Cybersecurity Assessment

In order to assist financial institutions in meeting the requirements and recommendations of the FFIEC guidance, NETBankAudit has developed a Cybersecurity Assessment that is compliant with FFIEC guidance. The Assessment is considered an addition to any IT Audit or Risk Assessment as the tests and reviews are specific to the cybersecurity threats utilizing a collaborative approach of testing the financial institution's controls specific to a simulated attack. The Assessment will provide an opinion of overall preparedness in place to protect the institution from cyber harm. Facilitation regarding threat and risk analysis is also incorporated into the process along with detailed and value-add recommendations for enhancement.

Our Cybersecurity Assessment complies with FFIEC guidance and considers the following key areas listed below (and discussed above) to ensure the institution's ability to identify and mitigate cybersecurity risks:

- Risk Management and Oversight
  - Governance Structure and Practices
  - Strategic Risk Management
  - Policy and Program
- Threat Intelligence and Collaboration
  - Personnel Knowledge and Training
  - Cyber Intelligence Integration
  - Information Flow and Assessment
- Cybersecurity Controls
  - Network Security Controls
  - Infrastructure Patching and Hardening
  - Logging and Monitoring
  - Vulnerability Assessment and Penetration Testing
- External Dependency Management
  - Risk Assessment and Documentation
  - External Support and Integration
  - Vendor Management and Oversight
- Cyber Incident Management and Resilience
  - Incident Response and Preparedness
  - Decision Making Structure and Resiliency
  - Cyber Response Experience and Training
  - Contingency Preparation and Insurance

The Assessment will include an External Penetration Test including social engineering tactics to gain access to the financial institution's network, similar to what an intruder would do to gain unauthorized access. Any successfully established connections from the social engineering or external penetration tests will be leveraged to complete internal penetration testing. The steps will include:

- Public Information Gathering
- Network Mapping
- Host Discovery
- Vulnerability Identification
- Privilege Escalation
- Anti-Virus and Intrusion Detection avoidance

- Attempt Vulnerability Exploits
- Observations/confirmation that the attack was recognized, and recommendations

THE DELIVERABLE

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.

To meet these requirements, NETBankAudit has developed the Cybersecurity Assessment. The Cybersecurity Assessment is performed in collaboration with management and in compliance with internal auditing standards. It includes a formal report with detailed testing and supporting documentation. The report and associated processes can be updated annually or as needed. All cybersecurity reviews and testing are tailored to each institution's specific threat and risk environment to ensure efficiency and effectiveness.

If your institution is interested in learning more about the Cybersecurity Assessment, please contact NETBankAudit at 800-243-0416, extension 507.