FFIEC Cybersecurity Assessment Tool

Overview for Chief Executive Officers and Boards of Directors

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council[1] (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[2]

Benefits to the Institution

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution's cybersecurity by doing the following:

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

CEO and Board of Directors

The role of the chief executive officer (CEO), with management's support, may include the responsibility to do the following:

- Develop a plan to conduct the Assessment.
- Lead employee efforts during the Assessment to facilitate timely responses from across the institution.
- Set the target state of cybersecurity preparedness that best aligns to the board of directors' (board) stated (or approved) risk appetite.
- Review, approve, and support plans to address risk management and control weaknesses.
- Analyze and present results for executive oversight, including key stakeholders and the board, or an appropriate board committee.

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

[2] A mapping is available in Appendix B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two resources.

- Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving areas of cybersecurity risk.
- Oversee changes to maintain or increase the desired cybersecurity preparedness.

The role of the board, or an appropriate board committee, may include the responsibility to do the following:

- Engage management in establishing the institution's vision, risk appetite, and overall strategic direction.
- Approve plans to use the Assessment.
- Review management's analysis of the Assessment results, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results.
- Review management's determination of whether the institution's cybersecurity preparedness is aligned with its risks.
- Review and approve plans to address any risk management or control weaknesses.
- Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

Assessment's Parts and Process

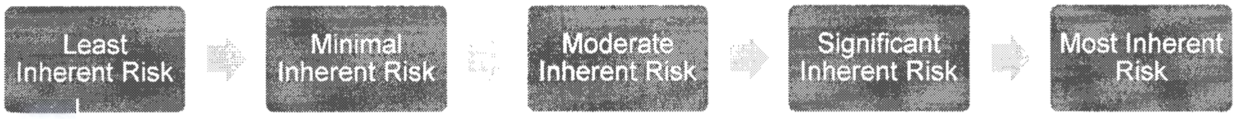
The Assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. Upon completion of both parts, management can evaluate whether the institution's inherent risk and preparedness are aligned.

Inherent Risk Profile

Cybersecurity inherent risk is the level of risk posed to the institution by the following:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Inherent risk incorporates the type, volume, and complexity of the institution's operations and threats directed at the institution. Inherent risk does not include mitigating controls. The Inherent Risk Profile includes descriptions of activities across risk categories with definitions for the least to most levels of inherent risk. The profile helps management determine exposure to risk that the institution's activities, services, and products individually and collectively pose to the institution.



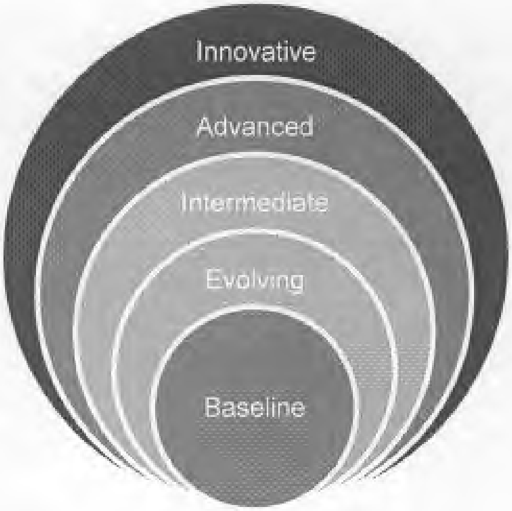
Least Inherent Risk → Minimal Inherent Risk → Moderate Inherent Risk → Significant Inherent Risk → Most Inherent Risk

When each of the activities, services, and products are assessed, management can review the results and determine the institution's overall inherent risk profile.

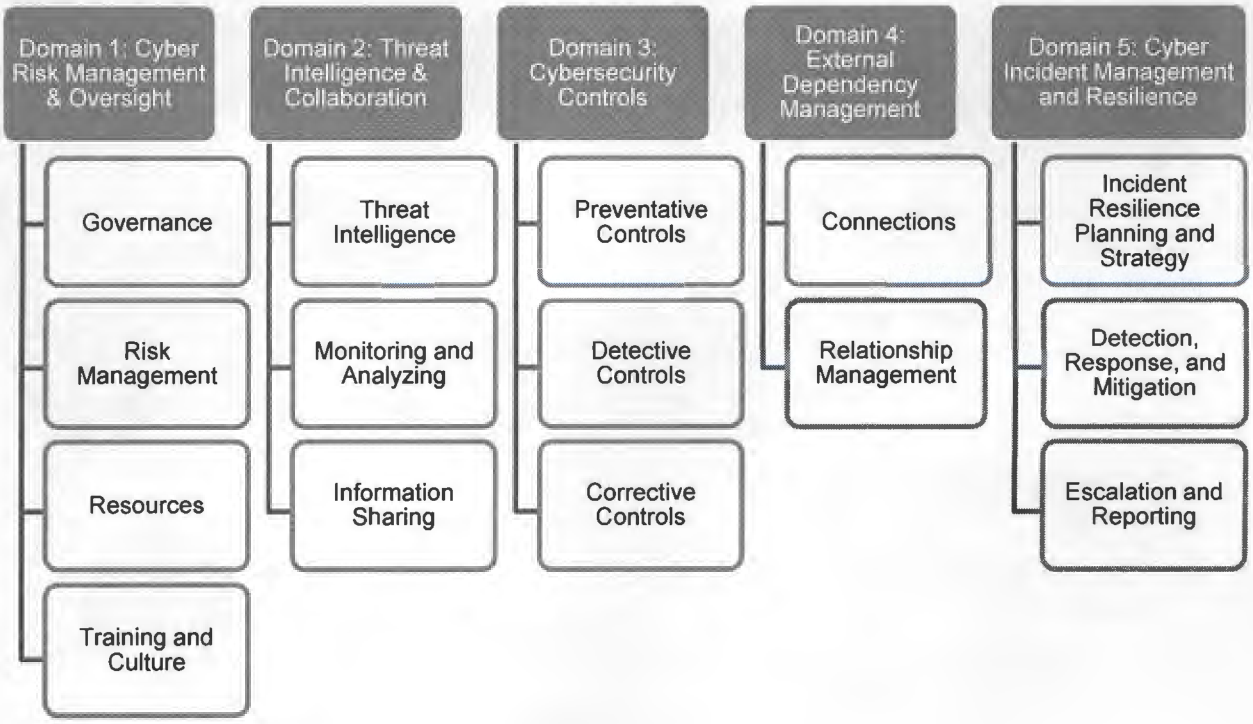
Cybersecurity Maturity

The Assessment's second part is Cybersecurity Maturity, designed to help management measure the institution's level of risk and corresponding controls. The levels range from baseline to innovative. Cybersecurity Maturity includes statements to determine whether an institution's behaviors, practices, and processes can support cybersecurity preparedness within the following five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience



The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level. Management determines which declarative statements best fit the current practices of the institution. ***All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.*** While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level. The figure below provides the five domains and assessment factors.


Domain 1: Cyber Risk Management & Oversight
Governance
Risk Management
Resources
Training and Culture
Domain 2: Threat Intelligence & Collaboration
Threat Intelligence
Monitoring and Analyzing
Information Sharing
Domain 3: Cybersecurity Controls
Preventative Controls
Detective Controls
Corrective Controls
Domain 4: External Dependency Management
Connections
Relationship Management
Domain 5: Cyber Incident Management and Resilience
Incident Resilience Planning and Strategy
Detection, Response, and Mitigation
Escalation and Reporting

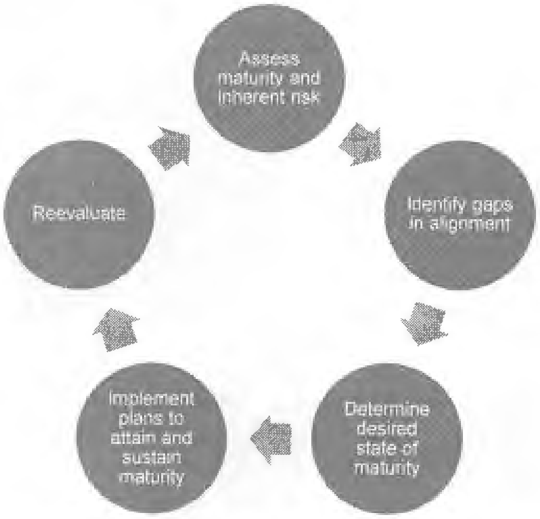
Management can review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. The following table depicts the relationship between an institution's Inherent Risk Profile and its domain Maturity Levels, as there is no single expected level for an institution. In general, as inherent risk rises, an institution's maturity levels should increase. An institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating the institution's inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections).

Risk/Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				▨	▨
	Advanced			▨	▨	▨
	Intermediate		▨	▨	▨	
	Evolving	▨	▨	▨		
	Baseline	▨	▨			

Management can then decide what actions are needed either to affect the inherent risk profile or to achieve a desired state of maturity. On an ongoing basis, management may use the Assessment to identify changes to the institution's inherent risk profile when new threats arise or when considering changes to the business strategy, such as expanding operations, offering new products and services, or entering into new third-party relationships that support critical activities. Consequently, management can determine whether additional risk management practices or controls are needed to maintain or augment the institution's cybersecurity maturity.

Supporting Implementation

An essential part of implementing the Assessment is to validate the institution's process and findings and the effectiveness and sufficiency of the plans to address any identified weaknesses. The next section provides some questions to assist management and the board when using the Assessment.


Assess maturity and inherent risk
Identify gaps in alignment
Determine desired state of maturity
Implement plans to attain and sustain maturity
Reevaluate

Cybersecurity Management & Oversight

- What are the potential cyber threats to the institution?
- Is the institution a direct target of attacks?
- Is the institution's cybersecurity preparedness receiving the appropriate level of time and attention from management and the board or an appropriate board committee?

- Do the institution's policies and procedures demonstrate management's commitment to sustaining appropriate cybersecurity maturity levels?
- What is the ongoing process for gathering, monitoring, analyzing, and reporting risks?
- Who is accountable for assessing and managing the risks posed by changes to the business strategy or technology?
- Are the accountable individuals empowered with the authority to carry out these responsibilities?
- Do the inherent risk profile and cybersecurity maturity levels meet management's business and risk management expectations? If there is misalignment, what are the proposed plans to bring them into alignment?
- How can management and the board, or an appropriate board committee, make this process part of the institution's enterprise-wide governance framework?

Inherent Risk Profile

- What is the process for gathering and validating the information for the inherent risk profile and cybersecurity maturity?
- How can management and the board, or an appropriate board committee, support improvements to the institution's process for conducting the Assessment?
- What do the results of the Assessment mean to the institution as it looks at its overall risk profile?
- What are the institution's areas of highest inherent risk?
- Is management updating the institution's inherent risk profile to reflect changes in activities, services, and products?

Cybersecurity Maturity

- How effective are the institution's risk management activities and controls identified in the Assessment?
- Are there more efficient or effective means for attaining or improving the institution's risk management and controls?
- What third parties does the institution rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- How does management validate the type and volume of attacks?
- Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?

Summary

FFIEC has developed the Assessment to assist management and the board, or an appropriate board committee, in assessing their institution's cybersecurity preparedness and risk. For more information and additional questions to consider, refer to the *FFIEC Cybersecurity Assessment General Observations* on the FFIEC's Web site.

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446
• http://www.ffiec.gov

Joint Statement

Cyber Insurance and Its Potential Role in Risk Management Programs

The Federal Financial Institutions Examination Council (FFIEC) members[1] developed this statement to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs. This statement does not contain any new regulatory expectations. Use of cyber insurance may offset financial losses resulting from cyber incidents; however, it is not required by the agencies. Financial institutions should refer to the *FFIEC Information Technology (IT) Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

The increasing number and sophistication of cyber incidents affect financial institutions of all sizes, and remediation of cyber incidents can be costly. Traditional insurance policies for general liability or basic business interruption coverage may not fully cover cyber risk exposures without special endorsement or by exclusion not cover them at all. Coverage may also be limited and not cover incidents caused by or tracked to outside vendors. Cyber insurance may offset financial losses from a variety of exposures, such as data breaches resulting in the loss of sensitive customer information.

The cyber insurance marketplace is growing and evolving in response to the increasing cyber-attack frequency, severity, and related losses. Many aspects of the cyber insurance marketplace, such as terminology, claims history, legal precedents, and risk modeling continue to evolve and are shaping the nature and scope of cyber insurance.

Cyber insurance coverage options vary greatly and may be offered on a stand-alone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions, or directors' and officers' policies. Further, cyber coverage options may be structured as first-party or third-party coverage. First-party coverage insures against direct expenses incurred by the insured party and may address costs related to customer notification, event management, business interruption, and cyber extortion. Third-party coverage

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

protects against the claims made by financial institutions' customers, partners, or vendors as a result of cyber incidents at financial institutions. Understanding the scope of coverage is critical for making an informed risk management decision.

RISKS

Financial institutions face a variety of risks from cyber incidents. These can include financial, operational, legal, compliance, strategic, and reputation risks resulting from fraud, data loss, or disruption of service.

RISK MITIGATION

While cyber insurance may be an effective tool for mitigating financial risk associated with cyber incidents, it is not required by the agencies. Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. An effective system of controls remains the primary defense against cyber threats.

If institution management is considering cyber insurance, the assessment of cyber insurance benefits should include an analysis of the institution's existing cybersecurity and IT risk management programs to evaluate the potential financial impact of residual risk. As institutions weigh the benefits and costs of cyber insurance, considerations may include:

- **Involving multiple stakeholders in the cyber insurance decision**
    - Include appropriate departments across the institution such as legal, enterprise risk management, operational risk management, finance, information technology, and information security management.
    - Assess the sufficiency of existing control environments to address the potential impact of cyber risk exposures and attestation requirements for the insurance policy.
    - Communicate the cyber insurance decision-making process, including the assessment of cyber insurance options, to the appropriate level of management.

- **Performing proper due diligence to understand available cyber insurance coverage**
    - Review the scope of existing or proposed insurance coverage to identify gaps.
    - Understand insurance policy terms, coverage, exclusions, and costs for cyber events.
    - Consider the potential benefits and costs to assess the insurance coverage appropriateness.
    - Avoid overreliance on insurance coverage as a substitute for sound operational risk management practices.
    - Recognize that policy terms and language may not be standardized. Coverage may be different among insurance providers and tailored for institutions.
    - Consider how the coverage is triggered, if certain types of cyber incidents (e.g., cyber terrorism) are excluded from coverage, and the impact that sub-limits may have in the total coverage and claims process.
    - Assess the financial strength (ratings) and claims paying history of insurance companies providing coverage and their ability to fulfill obligations under the policy if multiple institutions file claims.

  - Assess how the proposed policies fit within the business strategies, insurance programs, and risk management programs.
  - Understand risk management and control requirements outlined in the policy and ensure the institution would be able to comply.
  - As appropriate, engage outside advisors, such as attorneys and brokers, to assist in the due diligence process to assess the benefits of cyber insurance relative to the cost.

- **Evaluating cyber insurance in the annual insurance review and budgeting process**
  - Assessing the benefits of cyber insurance relative to the cost.
  - Determining the sufficiency of existing insurance coverage as cyber risk exposures, insurance products, and the threat landscape evolve.
  - Confirming that any cyber insurance includes coverage expected by the institutions.
  - Engaging the board to assess these factors in insurance program reviews.

Financial institutions ultimately remain responsible for maintaining a control environment consistent with the guidance outlined in the *FFIEC IT Examination Handbook.*

ADDITIONAL RESOURCES

The following cyber insurance resources provide institutions with practical information that may help in understanding cyber insurance.

U.S. Department of Homeland Security:

Cybersecurity Insurance
Cyber Incident and Analysis Working Group White Paper

REFERENCES

FFIEC IT Examination Handbook booklets:

"Audit"
"Business Continuity Planning"
"Development and Acquisition"
"Information Security"
"Management"

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Cybersecurity of Interbank Messaging and Wholesale Payment Networks

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members,[1] is issuing this statement, in light of recent cyber attacks, to remind financial institutions of the need to actively manage the risks associated with interbank messaging and wholesale payment networks. Financial institutions should review their risk management practices and controls over information technology (IT) and wholesale payment systems networks, including authentication, authorization, fraud detection, and response management systems and processes. The FFIEC members emphasize that participants in interbank messaging and wholesale payment networks should conduct ongoing assessments of their ability to mitigate risks related to information security, business continuity, and third-party provider management.

This statement does not contain new regulatory expectations. It is intended to alert financial institutions to specific risk mitigation techniques related to cyber attacks exploiting vulnerabilities and unauthorized entry through trusted client terminals running messaging and payment networks. Financial institutions should review their risk management practices (including services provided to clients) and refer to the appropriate *FFIEC IT Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management. Financial institutions should also review and adhere to the technical guidance issued by payments and settlement networks for managing and controlling risks to critical systems.

BACKGROUND

Recent cyber attacks against interbank networks and wholesale payment systems to commit fraud have demonstrated capability to:

- Compromise a financial institution's wholesale payment origination environment, bypassing information security controls.
- Obtain and use valid operator credentials with the authority to create, approve, and submit messages.
- Employ sophisticated understanding of funds transfer operations and

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

operational controls.

- Use highly customized malware to disable security logging and reporting, as well as other operational controls to conceal and delay detection of fraudulent transactions.
- Transfer stolen funds across multiple jurisdictions quickly to avoid recovery.

RISKS

Unauthorized transactions involving interbank messaging and wholesale payment networks may subject the originating bank to financial loss and compliance risk.[2]

RISK MITIGATION

Financial institutions should use multiple layers of security controls to establish several lines of defense. Financial institutions should also ensure that their risk management processes address the risk posed by compromised credentials. In taking these actions, financial institutions should reference the risk management information contained in the *FFIEC IT Examination Handbook,*[3] specifically the *Information Security,*[4] *Business Continuity Planning,*[5] *Outsourcing Technology Services,*[6] and the *Wholesale Payment Systems*[7] booklets. Additionally, institutions should consult their payment system provider's guidance for specific security control recommendations.

In accordance with regulatory requirements and FFIEC guidance, a financial institution should consider the following steps:

- **Conduct ongoing information security risk assessments.** Maintain an ongoing information security risk assessment program that considers new and evolving threat intelligence related to online accounts and adjust customer authentication, layered security, and other controls in response to identified risks. Identify, prioritize, and assess the risk to critical systems, including threats to applications that control various system parameters and other security and fraud prevention measures. In addition, ensure that third-party service providers:
    - Perform effective risk management and implement appropriate controls.
    - Properly maintain and conduct regular testing of their security controls simulating potential risk scenarios.
    - Are contractually obligated to provide security incident reports when issues arise that may affect the institution.

- **Perform security monitoring, prevention, and risk mitigation.** Ensure protection and detection systems, such as intrusion detection systems and antivirus protection, are up-to-date and firewall rules are configured properly and reviewed periodically. Establish a baseline environment to enable the ability to detect anomalous behavior. Monitor system alerts to identify, prevent, and contain attack attempts from all sources. In addition,

[2] e.g. U.S.A. PATRIOT Act, Bank Secrecy Act, Office of Foreign Assets Control (OFAC)

[3] See: http://ithandbook.ffiec.gov/

[4] See: http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[5] See: http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

[6] See: http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

[7] See: http://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx

  - Follow software assurance industry practices for internally developed applications.
  - Conduct due diligence of third-party software and services.
  - Conduct penetration testing and vulnerability scans, as necessary.
  - Promptly manage vulnerabilities, based on risk, and track mitigation progress, including implementing patches for all applications, services, and systems.
  - Review reports generated from monitoring systems and third parties for unusual behavior.

- **Protect against unauthorized access**. Limit the number of credentials with elevated privileges across the institution, especially administrator accounts, and the ability to easily assign elevated privileges to access critical systems. Review access rights periodically to confirm approvals are still appropriate to the job function. Establish stringent expiration periods for unused credentials, monitor logs for use of old credentials, and promptly terminate unused or unwarranted credentials. Establish authentication rules, such as time-of-day and geolocation controls, or implement multifactor authentication protocols for web-based control panels. In addition,
  - Conduct regular audits to review the access and permission levels to critical systems for employees and contractors. Implement least privileges access policies across the entire enterprise. In particular, do not allow users to have local administrator rights on workstations.
  - Change default password and settings for system-based credentials.
  - Prevent unpatched systems, such as home computers and personal mobile devices from connecting to internal-facing systems.
  - Implement monitoring controls to detect unauthorized devices connected to internal networks.
  - Use secure connections when remotely accessing systems and services (e.g., virtual private networks).

- **Implement and test controls around critical systems regularly.** Ensure appropriate controls, such as access control, segregation of duties, audit, and fraud detection and monitoring systems, are implemented for systems based on risk. Limit the number of sign-on attempts for critical systems and lock accounts once such thresholds are exceeded. Implement alert systems to notify employees when baseline controls are changed on critical systems. Test the effectiveness and adequacy of controls periodically. Report test results to senior management and, if appropriate, to the board of directors or a committee of the board of directors. Include in the report recommended risk mitigation strategies and progress to remediate findings. In addition,
  - Encrypt sensitive data on internal- and external-facing systems in transit and, where appropriate, at rest.
  - Implement an adequate password policy.
  - Review the business processes around password recovery.
  - Regularly test security controls, such as web application firewalls.
  - Implement procedures for the destruction and disposal of media containing sensitive information based on risk relative to the sensitivity of the information and the type of media used to store the information.
  - Filter Internet access through Web site whitelisting where appropriate to limit employees' access to only those Web sites necessary to perform their job functions.
  - Conduct incremental and full backups of important files and store the backed-up data offline.

- **Manage business continuity risk.** Validate that business continuity planning supports the institution's ability to quickly recover and maintain payment processing operations. In addition,
  - Coordinate business continuity development and testing with all applicable third parties.
  - Coordinate testing with other industry players.

- **Enhance information security awareness and training programs.** Conduct regular, mandatory information security awareness training across the financial institution, including how to identify and prevent successful phishing attempts. Ensure training reflects the functions performed by employees.

- **Participate in industry information-sharing forums.** Incorporate information sharing with other financial institutions and service providers into risk mitigation strategies to identify, respond to, and mitigate cybersecurity threats and incidents. Since threats and tactics can change rapidly, participating in information-sharing organizations, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), can improve an institution's ability to identify attack tactics and to successfully mitigate cyber attacks involving destructive malware on its systems. In addition to the FS-ISAC, there are government resources such as the U.S. Computer Emergency Readiness Team (US-CERT) that provide information on vulnerabilities. The US-CERT portal may be found at www.us-cert.gov.

ADDITIONAL RESOURCES

The following are available payment systems risk management resources with practical information.

- FFIEC Joint Statement on Compromised Credentials. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
- FFIEC Joint Statement on Destructive Malware. https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf
- FFIEC Joint Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing. https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf
- "SWIFT Security Issues Update – New information." SWIFT: May 13, 2016. https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues
- "SWIFT customer communication: Cooperating on cyber-security." SWIFT: May 20, 2016. https://www.swift.com/insights/press-releases/swift-customer-communication_cooperating-on-cyber-security
- Committee on Payments and Market Infrastructures, Cyber resilience in financial market infrastructures. http://www.bis.org/cpmi/publ/d122.pdf
- Federal Reserve Banks Operating Circular No. 5 ELECTRONIC ACCESS Effective June 30, 2016. https://frbservices.org/files/regulations/pdf/operating_circular_5_06302016.pdf

REFERENCES

FFIEC Information Technology Examination Handbook, "Wholesale Payment Systems" *http://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx*

FFIEC Information Technology Examination Handbook, “Business Continuity Planning”
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

FFIEC Information Technology Examination Handbook, “Information Security”
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

FFIEC Information Technology Examination Handbook, "Outsourcing Technology Services”
http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Cyber Attacks Involving Extortion

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members,[1] is issuing this statement to notify financial institutions of the increasing frequency and severity of cyber attacks involving extortion. Financial institutions should develop and implement effective programs to ensure the institutions are able to identify, protect, detect, respond to, and recover from these types of attacks.

This statement does not contain any new regulatory expectations. It is intended to alert financial institutions to specific risk mitigation related to the threats associated with cyber attacks involving extortion. Financial institutions should refer to the appropriate FFIEC Information Technology (IT) Examination Handbook booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

Cyber criminals and activists use a variety of tactics, such as *ransomware*, *denial of service (DoS)*, and *theft of sensitive business and customer information to extort payment or other concessions from victims.* In some cases, these attacks have caused significant impacts on businesses' access to data and ability to provide services. Other businesses have incurred serious damage through the release of sensitive information.

RISKS

Financial institutions face a variety of risks from cyber attacks involving extortion, including liquidity, capital, operational, compliance and reputation risks, resulting from fraud, data loss, and disruption of customer service.

RISK MITIGATION

Financial institutions should ensure that their risk management processes and business continuity planning address the risks from these types of cyber attacks, consistent with the risk management practices identified in previous FFIEC joint statements and the *FFIEC Information Technology Examination Handbook* , specifically the "Business Continuity Planning" and "Information Security" booklets. Related FFIEC joint statements are titled "Destructive Malware," "Cyber

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

Attacks Compromising Credentials," and "Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources."

Consistent with FFIEC and member guidance, financial institutions should consider taking the following steps:

- *Conduct ongoing information security risk assessments.*
- *Securely configure systems and services.*
- *Protect against unauthorized access.*
- *Perform security monitoring, prevention, and risk mitigation.*
- *Update information security awareness and training programs, as necessary, to include cyber attacks involving extortion.*
- *Implement and regularly test controls around critical systems.*
- *Review, update, and test incident response and business continuity plans periodically.*
- *Participate in industry information-sharing forums.*

Institutions that are victims of cyber attacks involving extortion are encouraged to inform law enforcement authorities and notify their primary regulator(s). In the event that an attack results in unauthorized access to sensitive customer information, the institution has responsibility to notify its federal and state regulators in accordance with the Interagency Guidelines Establishing Information Security Standards implementing the Gramm–Leach–Bliley Act and applicable state laws. Additionally, institutions should determine if filing a Suspicious Activity Report (SAR) is required or appropriate, as in the case of an unauthorized electronic intrusion intended to damage, disable, or otherwise affect critical systems.[2] In instances where filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector.

ADDITIONAL RESOURCES

The following government resources assist institutions to mitigate cyber attacks involving extortion.

- *US-CERT Security Alert* "Crypto Ransomware" *(TA14-295A)* https://www.us-cert.gov/ncas/alerts/TA14-295A
- *FBI* "Ransomware on the Rise" https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise
- *FBI* "E-mail Extortion Campaigns Threatening Distributed Denial of Service Attacks" *(I-073115-PSA)* http://www.ic3.gov/media/2015/150731.aspx

REFERENCES

FFIEC Information Technology Examination Handbook, "Business Continuity Planning" http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

[2] Frequently Asked Questions Regarding the Financial Crimes Enforcement Network Suspicious Activity Report (SAR) http://www.fincen.gov/whatsnew/html/sar_faqs.html

FFIEC Information Technology Examination Handbook, "Information Security"
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

FFIEC Joint Statement on Destructive Malware
https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

FFIEC Joint Statement on Cyber Attacks Compromising Credentials
https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

FFIEC Joint Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing
https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf

FFIEC Joint Statement on Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources
https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf

PRINT THE ENTIRE STATEMENT
Please use the following hyperlink:
https://www.ffiec.gov/press/PDF/FFIEC_Joint_Statement_Cyber_Attacks_Involving_Extortion.pdf