Joint Statement on Heightened Cybersecurity Risk

January 16, 2020

Purpose

The Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency are issuing this statement to remind supervised financial institutions of sound cybersecurity risk management principles. These principles elaborate on standards articulated in the *Interagency Guidelines Establishing Information Security Standards*[1] as well as resources provided by the Federal Financial Institutions Examination Council (FFIEC) members, such as the FFIEC Statement on Destructive Malware.[2] When financial institutions apply these principles and risk mitigation techniques, they reduce the risk of a cyber attack's success and minimize the negative impacts of a disruptive and destructive cyber attack. While preventive controls are important, financial institution management should be prepared for a worst-case scenario and maintain sufficient business continuity planning processes for the rapid recovery, resumption, and maintenance of the institution's operations.

Highlights

Implementing and maintaining effective cybersecurity controls is critical to protecting financial institutions from malicious activity, especially in periods of heightened risk. Sound risk management for cybersecurity includes the following:

- **Response and resilience capabilities:** Review, update, and test incident response and business continuity plans.
- **Authentication:** Protect against unauthorized access.
- **System configuration:** Securely configure systems and services.

Background

Heightened risk from cybersecurity threats, such as increased geopolitical tensions and threats of aggression, may result in cyber attacks against U.S. targets and interests. In recent years, disruptive and destructive attacks against financial institutions have increased in frequency and severity. Cyber actors often use malware to exploit weaknesses in a financial institution's computers or networks. They often obtain access to financial institution systems and networks by compromising user credentials and introducing malware through social engineering financial institution employees and contractors with phishing or spear phishing attacks. Another method of attack is to introduce infected external devices to computers and networks through removable media.

Destructive malware introduced into a financial institution's systems has the potential to alter, delete, or otherwise render production data and systems unusable. Depending on the scope of

[1] See 12 CFR 364, appendix B (FDIC), and 12 CFR 30, appendix B (OCC).
[2] See https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf.

the attack, the type of backup processes used, and other controls employed, the financial institution's data and system backups may also be similarly affected by a destructive malware attack, severely affecting the financial institution's ability to recover operations. A financial institution's continuity and resiliency planning should appropriately consider the threats and vulnerabilities to backup processes and systems, including those involving mirroring and data replication capabilities that back up production systems on a near real-time basis. Mirroring and data replication implemented by many financial institutions in recent years have enabled shorter recovery time frames and have improved business resumption capabilities, but these capabilities can expose the financial institution to the risk of quickly replicating malware that can corrupt both production and backup data or introduce processing errors, potentially making the damage irreversible.

Risk Management

Given the heightened threat environment, senior management should reevaluate the adequacy of information technology safeguards against threats, especially safeguards against ransom and other destructive malware. The growing number of attacks highlights the critical importance of making cybersecurity preparedness and resiliency a top priority. Implementing and maintaining effective cybersecurity controls, including threat monitoring, are critical to protecting financial institutions from malicious activity. Key controls include the following:

Response, Resilience, and Recovery Capabilities

Even with preventive controls in place, financial institutions may fall victim to destructive malware attacks. Financial institution management should consider measures to enhance the resilience of systems and operations against cyber threats and physical events. This can include maintaining system backups either on segmented[3] portions of the network or offline, such as on tape media. Logically segmenting and, as appropriate, establishing physical air gaps between critical network components and services (e.g., core processing, transaction data, account data, and backups) and highly sensitive elements of the network environment reduces the risk that malicious activity will spread across the network. Testing recovery capabilities to respond to ransomware or other destructive malware that encrypts or corrupts data, including backup data, helps financial institutions mitigate attacks. Uninfected backup data is essential to recovery capabilities in scenarios where destructive malware corrupts not only the primary data but also backup systems. Additional response, recovery, and resilience controls and principles can include the following:

- Maintain comprehensive, documented, and current incident and business resilience plans that include responding to and recovering from a destructive cyber attack.
  - Integrate elements necessary for recovering from a cyber event into the business continuity management program.

[3] NIST defines network segmentation as "[s]plitting a network into sub-networks, for example, by creating separate areas on the network which are protected by firewalls configured to reject unnecessary traffic. Network segmentation minimizes the harm of malware and other threats by isolating it to a limited part of the network." https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

  - Develop and maintain relationships with federal and local law enforcement cybersecurity resources.
  - Identify cybersecurity forensic and recovery expertise that can be engaged to assist with an event.
  - Conduct periodic cyber recovery exercises or plan testing to demonstrate that recovery capabilities function as expected.
  - Consider the use of cyber insurance[4] as a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure.
- Implement a comprehensive system and data backup strategy.
  - Conduct regular backups of all critical data and system configuration information at an appropriate frequency (e.g., daily) consistent with the volume, type, and criticality of data.
  - Securely store system and data backups off site at separate geographic locations and maintain off line or in a manner that provides for physical or logical segregation from production systems.
  - Periodically test the ability to reconstruct data in the event of a destructive attack.
  - Consider whether backup and restoration practices are consistent with industry standards and frameworks, such as Sheltered Harbor[5] (a voluntary industry initiative), for data vaulting to safeguard critical data in the event of a destructive malware attack.

Identity and Access Management

The proliferation of phishing attacks and threat actor success in compromising login credentials warrants financial institutions having appropriate identity and access management controls, including authentication controls, for customer, employee, and third-party access to systems. Examples of identity and access management controls include the following:

- Use and validate the effectiveness of authentication controls, such as multifactor authentication,[6] to segment and safeguard access to critical systems and data on the network.
- Ensure that strength of authentication and controls for access are based on risk.
- Implement role-based access controls on user privileges and limit user permissions to those necessary for job functions.
- Limit and monitor administrator and other privileged user accounts.
- Regularly review appropriateness of assigned access.

[4] See the FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs: https://www.ffiec.gov/press/pr041018.htm.
[5] Additional information is available at Sheltered Harbor: https://www.shelteredharbor.org/images/ShelteredHarbor/Documents/ShelteredHarborAtAGlance.pdf.
[6] National Institute of Standards and Technology (NIST) Special Publication 800-63B, *Digital Identity Guidelines*, states that "[s]tronger authentication requires malicious actors to have better capabilities and expend greater resources in order to successfully subvert the authentication process."

Network Configuration and System Hardening

Network and software system settings should be reviewed and configured in a safe and sound manner. Financial institution management should review the appropriateness of default system settings, change default user profiles, configure security settings, and implement security monitoring tools. Security updates and system patches are critical to maintaining secure systems and should be implemented in a timely manner. Additional system configuration controls and cyber hygiene principles include the following:

- Securely configure network components to ensure that only approved ports, protocols, and services are allowed and disable all unnecessary services, ports, and protocols. Document and approve security configuration standards for operating systems and system components.
  - Review and disable or adjust default user accounts and settings as needed before system use.
  - Limit removable media access to the network.
  - Perform vulnerability scans that cover all network components, hardware components (laptops, desktops, mobile devices, routers, and firewalls), firmware, and operating systems to confirm critical patches are installed.
  - Regularly implement and update anti-malware software to continuously monitor and defend the network and all connected devices.
  - Configure email systems to detect and prevent common email attack vectors, such as spoofed or phishing emails containing malicious links or attachments.
  - Logically segment critical network components and services (e.g., core processing, transaction data, account data, and backups) and, where appropriate, physically air gap critical or highly sensitive elements of the network environment.
- Consistent with risk, configure and continuously monitor internal networks that connect to service providers, particularly those providing critical services.

Management should also consider the following areas when evaluating the financial institution's risks associated with destructive malware and operational resilience:

Employee Training

- Understand that employees are a critical control point for a financial institution's cybersecurity program and that social engineering is a primary tactic that malicious actors use to gain entry to systems. Key considerations for employee training related to social engineering risks include the following:
  - Ongoing employee training on recognizing cyber threats, phishing, and suspicious links.
  - Measuring the effectiveness of such cybersecurity training programs.

Security Tools and Monitoring

- Employ qualified cybersecurity staff in house, or a qualified managed security service provider firm, to actively monitor systems for network threat and vulnerability information available from industry sources, such as Financial Services Information Sharing and Analysis Center (FS-ISAC) and the U.S. Computer Emergency Readiness Team (US-CERT). Maintain a process to use the threat and vulnerability information to identify and respond to potential cyber threats.
- Review system and network audit logs for anomalous activity either manually or through use of a security information and event management tool. Review should occur regularly by qualified personnel.
- Implement a sufficiently scoped penetration testing program that includes periodic internal and external testing of the bank's ability to detect and respond to attacks. Track and correct findings from such testing in a timely manner.

Data Protection

- Maintain a data classification program to identify sensitive and critical data.
- Encrypt or tokenize sensitive and critical data in transit and at rest.

This joint statement provides examples of key risk management and control considerations and is not an exhaustive list. Financial institution management should leverage available resources to develop and maintain an effective cybersecurity risk management program, including close coordination with service providers, software vendors, contractors, and other third parties.