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,[2] 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.

The primary method of ransomware infection is through the use of deceptive e-mails or malicious Web sites that imitate legitimate organizations or communications. Ransomware typically encrypts the data on the target machine, making data inaccessible. The victim is then prompted to make a payment in order to release or unlock the files. In some cases where a payment has been made, there have been reports the files have not been decrypted after payment, or their computer has been infected with the ransomware again shortly after being decrypted. Businesses affected by ransomware can suffer more than inconvenience and monetary loss. If critical information is permanently lost, operations could be severely impacted.

---

[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] Ransomware is a type of malicious software (malware) that encrypts data on a computer, making it difficult or impossible to recover. The attackers offer to provide a decryption key after a ransom is paid.

A DoS attack is an attempt by attackers to prevent legitimate users from accessing a service. This is generally accomplished by flooding a system with illegitimate requests. Extortionists often illustrate their capabilities by performing a small attack, such as shutting down a Web site for a period of time. This is followed by an e-mail to the victim requesting payment to prevent additional, larger attacks. If an attacker is successful in preventing customer or employee access to a resource or systems, the financial institution's reputation could be affected, in addition to potentially incurring operational and recovery costs.

There have been recent incidents involving theft of sensitive business and consumer data by activists. After stealing the data, the activists demand that the business take a particular action or the data would be publicly released. Such a release of information could affect an institution's reputation and have other serious consequences.

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 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.** Maintain an ongoing information security risk assessment program that considers new and evolving threats 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 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.

- **Securely configure systems and services.** Protections such as logical network segmentation, offline backups, air gapping, maintaining an inventory of authorized devices and software, physical segmentation of critical systems, and other controls may mitigate the impact of a

cyber attack involving ransomware. Consistency in system configuration promotes the implementation and maintenance of a secure network. Essential components of a secure configuration include the removal or disabling of unused applications, functions, or components.

- **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 that access critical systems. Review access rights periodically to reconfirm approvals are 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 systems and services (e.g., virtual private networks). 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.

- **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:
    - Follow software assurance industry practices for internally developed applications.
    - Conduct due diligence assessments 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.

- **Update information security awareness and training programs, as necessary, to include cyber attacks involving extortion.** Conduct regular, mandatory information security awareness training across the financial institution, including how to identify, prevent, and report phishing attempts and other potential security incidents. Ensure training reflects the functions performed by employees.

- **Implement and regularly test controls around critical systems.** 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 employee's access to only those Web sites necessary to perform their job functions, so as to reduce the risk of connecting to infected Web sites.
- Conduct incremental and full backups of important files and store the backed-up data offline.

- **Review, update, and test incident response and business continuity plans periodically.** Test the effectiveness of incident response plans at the financial institution and with third-party service providers to ensure that all employees, including individuals responsible for managing liquidity and reputation risk, information security, vendor management, fraud detection, and customer inquiries, understand their respective responsibilities and their institution's protocols. In addition:
  - Ensure processes are in place that update, review, and test incident response and business continuity plans address cybersecurity threats involving extortion.
  - Ensure incident response and business continuity plans are updated to address notification of service providers, including Internet service providers (ISP), as appropriate, if the institution suspects that a DDoS attack is occurring.

- **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 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 mitigate cyber attacks involving ransomware malware on its systems successfully. 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.

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.[3] 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

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:

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

https://www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf