SOUTH DAKOTA
DIVISION OF BANKING

1714 Lincoln Avenue, Suite 2
Pierre, SD 57501
Phone: (605) 773-3421
Fax: (605) 773-3460

DATE: FEBRUARY 28, 2025

TO: ALL STATE-CHARTERED BANKS AND TRUST COMPANIES

FROM: BRADY SCHLECHTER, CHIEF INFORMATION SYSTEMS EXAMINER

RE: CYBER HYGIENE: ACTIONS YOUR INSTITUTION SHOULD TAKE TODAY

Financial institutions in the United States continue to face threats on many fronts. Ransomware threat actors remain prolific in utilizing social engineering tactics and exploiting hardware and software vulnerabilities to gain a foothold into financial institution systems. In addition, geopolitical threats from state-sponsored actors from China, Russia, Iran, North Korea, and others continue to pose both direct and indirect risks to financial institutions, as well as the third-party providers who provide critical services to them.

Ensuring that your institution has a program of strong cyber hygiene practices in place today can significantly increase security protections and make your institution a less attractive target for cyber criminals. This memo reviews some fundamental controls that your institution should have in place to significantly reduce the risks posed from these threats.

Ransomware Remains a Significant Threat

Ransomware continued to cause havoc in financial institutions in 2024, and there are no signs that the threat is waning. We continue to see successful data exfiltration from victim organizations- either with or without the encryption of data. Successful attacks involving the unauthorized access to or theft of customer and/or company data can create a nightmare scenario for a financial institution, as traditional methods of recovering and restoring data cannot address impacts to reputation, potential regulatory implications, and liability associated with the disclosure or theft of sensitive customer or company data. Ransomware threat actors are skilled at utilizing phishing and other social engineering tactics against unsuspecting employees and executives to gain access to systems or system credentials. In addition, unpatched vulnerabilities in software and hardware, as well as the utilization of unsupported assets that have reached the end of their usable life, offer a convenient avenue for threat actors to gain a dangerous foothold into company systems.

Geopolitical Threats Pose Additional Risk to Financial Institutions

Financial institutions are also exposed to risks associated with the actions of state-sponsored threat actors. You may have heard recent news regarding Russian threat actors compromising Microsoft email systems or reports of Chinese threat actors compromising nine telecommunications companies in the United States. These actions are widely believed to be only a portion of what state-sponsored threat actors can do to disrupt financial institutions and other elements of critical infrastructure in the United States. State-sponsored threat actors today engage in criminal cyber activities to enable espionage and access sensitive customer and company data. In addition, some state-sponsored actors, such as the Chinese threat actor Volt Typhoon, use “living off the land” techniques to

remain undetected in networks and systems for purposes of disrupting systems and networks, gaining lateral access to critical operational control systems, and creating societal chaos. Financial institutions in the United States are at risk from both direct intrusion by these actors, as well as secondary effects from attacks on critical infrastructure sectors (energy, water, transportation, communications, etc.) upon which the financial sector heavily depends.

Cyber Hygiene Practices Are Effective Deterrents to These Threats

According to Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly, "Basic cyber hygiene prevents 98% of cyber attacks." Cyber hygiene programs generally include well-known controls that have been employed in financial institutions for years; however, ongoing attention is needed to ensure that these programs are consistently implemented and managed across the entire organization.

To ensure that a strong cyber hygiene program is maintained, institutions should:

- Implement an **asset inventory management program** that captures all organizational IT assets, including all assets that make periodic or continuous connection to the institution's network. A comprehensive inventory management program is necessary to support vulnerability and patch management, as well as end-of-life management programs.
- Develop and maintain a comprehensive and robust **vulnerability and patch management program.** Unpatched hardware and software provide an attractive and frequently exploited attack vector for cyber criminals and state-sponsored threat actors.
- Implement an ongoing **end-of-life management program** to identify and manage software and hardware assets that are nearing the end of their useful life.
- Use **strong passwords** supported by a robust password management policy.
- Implement and properly configure **phishing-resistant multi-factor authentication (MFA)** for control of privileged access; access to cloud-based services (including email); access to external applications hosting nonpublic information; VPN/remote desktop access to the network; third-party vendor access to the network; access to internal service accounts; and customer access to nonpublic information such as eBanking services and remote deposit capture.
- Develop a comprehensive **third-party risk management program** that identifies and categorizes by risk all third-party vendor relationships, including those with managed service providers (MSPs).
- Ensure that **logging** is enabled for application, access, and security logs, and store logs in a central location for convenient access and review. While all institutions log network activity, cyber criminals often exploit short log retention periods and the lack of logging of routine administrative activity.
- Maintain effective **backups** for core processing, network administration, and other critical services.
- Maintain a robust **cybersecurity awareness training program, including periodic phishing testing,** for all employees, including executives.
- Ensure that the institution has a program to receive, evaluate, and disseminate **active threat information**. Subscribing to alerts from FS-ISAC, FBI InfraGard, and CISA can provide valuable active intelligence on current ransomware and geopolitical threats.
- Develop and regularly test an **incident response plan** that enables a rapid response to different types of cyber incidents.

As a complement to these foundational cyber hygiene practices, CISA provides beneficial, no-cost cyber hygiene services to financial institutions. These services consist of two offerings:

- **Vulnerability Scanning**, which continuously monitors and assesses public-facing, internet-accessible network assets to evaluate their host and vulnerability status. In addition to weekly reports of all findings, participants receive ad-hoc alerts about urgent findings, such as the identification of potentially risky services and known exploited vulnerabilities.
- **Web Application Scanning**, which takes a deeper dive into publicly accessible web applications to uncover vulnerabilities and misconfigurations that attackers could exploit.

We strongly recommend that you consider implementing these free services from CISA in your institution. To learn more about these services or to enroll, visit CISA's Cyber Hygiene Services page.

Industry and Regulators Must Work Together to Stop These Threats

Continued cooperation between the financial sector and regulators is necessary to address the significant ongoing threats from ransomware and state-sponsored threat actors. For financial institutions, ongoing attention is needed to maintain and strengthen institutional IT security practices, including the foundational cyber hygiene practices identified here. It is important for institutions to address these recommended actions now since many of the techniques described here are being actively exploited by criminal organizations.

In consideration of the threats, as well as the likely emergence of future threats impacting the financial sector, institutions and regulators alike must develop and maintain the agility to efficiently receive, evaluate, and prioritize threat information and appropriately mitigate these and other emerging threats on an ongoing basis. The significance and persistence of current threats warrants your ongoing attention to the aforementioned cyber hygiene practices.

RESOURCES:

CSBS Ransomware Self-Assessment Tool
CISA's Shields Up Program
CISA's Stop Ransomware Program
CISA's Cyber Hygiene Services | CISA
(VIDEO) Strengthening Cyber Defenses: CISA's Free Vulnerability Scanning Explained
People's Republic of China Threat Overview and Advisories | CISA
Russia Threat Overview and Advisories | CISA
North Korea Threat Overview and Advisories | CISA
Iran Threat Overview and Advisories | CISA