Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2025-01
Date: January 24, 2025

Cybersecurity Threats: Actions to Take Today

As we move into 2025, 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 bank systems. In addition, cyber threats are intensified by geopolitical threats. 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 notice reviews current cyber threats while the Attachment: *Cyber Hygiene Practices-Focus on the Fundamentals* provides some fundamental controls that your institution should have in place to significantly reduce the risks posed from these threats.

As daunting as the challenge can seem for a community bank to defend against nation states and sophisticated cyber-criminal organizations, relatively simple measures, **when fully and consistently applied,** can mitigate most cyber risks. According to the Director of Cybersecurity and Infrastructure Security Agency (CISA), **"Basic cyber hygiene prevents 98% of cyber attacks."**

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. Successful attacks involving the unauthorized access to or theft of customer and/or company data can create a nightmare scenario for a financial institution. 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 life, offer a convenient avenue for threat actors to gain a dangerous foothold into an organization's systems. The Ransomware Self-Assessment Tool (R-SAT) contains Multi-Factor Authentication (MFA) practices that are critical for protecting against all cyber threats.

Geopolitical Threats Pose Additional Risk to Banks

Financial institutions are also exposed to risks associated with the actions of state-sponsored threat actors. Russian threat actors have compromised Microsoft email systems and Chinese threat actors have compromised 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 this country. 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 People's Republic of China (PRC) 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 when the state-sponsored actor chooses. Financial institutions are at risk from both direct intrusion by these actors, as well as secondary affects from attacks on critical infrastructure sectors (energy, water, transportation, communications, etc.) upon which the financial sector heavily depends.

In 2024, the heads of the top federal agencies responsible for monitoring cyber threats against the United States provided Congressional testimony that China is targeting our critical infrastructure throughout the United States. The outgoing FBI Director Christopher Wray noted in a recent interview that the greatest threat the Trump administration will face is the cyber threat from China. Texas Governor Greg Abbott signed an Executive Order in November 2024 relating to the protection of critical infrastructure from Chinese hacking. Additionally, the Director of CISA stated in Congressional testimony, "*This threat is not theoretical… CISA teams have found and eradicated Chinese intrusions into critical infrastructure across multiple sectors… And what we've found to date is likely the tip of the iceberg*."

CISA has recommended four primary actions to mitigate Volt Typhoon, which can best be summarized by focusing on the fundamentals:

(1) Patching,
(2) Multi-Factor Authentication (MFA),
(3) Logging, and
(4) "End of Life" management.

These are well known controls that have been employed for years. However, state-sponsored threat actors are using weaknesses in implementation of these controls to gain access. The implementation of these four controls will be closely reviewed at future information technology (IT) examinations. For example, even though network activity logging is enabled, the PRC exploits the short log retention periods and lack of logging of routine administrative activity. Chief Information Security Officers will need to closely analyze not just logging activity but all aspects of privileged access management. Bankers should begin addressing these issues immediately rather than waiting for an IT examination.

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. While none of the cyber hygiene practices listed in the attachment are new, the Department will be looking more closely at the effectiveness of the implementation of each of them. It is important for institutions

to **address these recommended actions expeditiously** since many of the techniques described 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 attached cyber hygiene practices.

To help address this and other threats, CISA provides beneficial, no-cost cyber hygiene services to financial institutions to assist in identifying vulnerabilities in networks and web applications and reduce exposure to threats. The Department of Banking uses this service and **strongly encourages Texas state-chartered banks to use it** as well. CISA will rapidly alert your institution of current vulnerabilities and potential attacks against the financial sector. It is important to note that signing up for this service does **not** give CISA access to your institution's network or data.

If you have any questions regarding this industry notice, please contact the Director of Cybersecurity and Technology Strategy via email.

Cyber Hygiene Practices - Focusing on the Fundamentals

Basic cyber hygiene prevents 98% of cyber attacks.

Although cyber hygiene programs are based on well-known controls employed in financial institutions, ongoing attention is needed to ensure that these programs are adequately implemented and consistently managed across the entire organization. Cyber threat actors have taken advantage of the weaknesses in implementation of the following controls to gain access to organizations.

Fundamental Controls

To ensure that a strong cyber hygiene program is maintained, institutions should focus on these fundamental controls:

1. **Patching:** Develop and maintain a comprehensive and robust vulnerability and patch management program. Such a program will require implementation of an asset inventory management program that captures all organizational IT assets, including all assets that make periodic or continuous connection to the bank's network. Inventory management is necessary to support patching as well as end-of-life management programs. Critical vulnerabilities should be patched within 30 days, unless an approved exception exits
2. **Multi-Factor Authentication (MFA):** 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.
3. **Logging:** Ensure that logging is enabled for application, access, and security logs, and store logs in a central, secure location for convenient access and review. While all banks log network activity, cyber threat actors are exploiting short log retention periods and the lack of logging of routine administrative activity.
4. **"End of Life" Management:** Implement an ongoing end-of-life management program to identify and manage software and hardware assets that are nearing the end of their useful and security supported life.
5. **Third-Party Risk Management Program**: Develop a comprehensive third-party risk management program that identifies and categorizes by risk all third-party vendor relationships, especially managed service providers (MSPs).
6. **Backups:** Maintain effective backups for core processing, network administration, and other critical services.
7. **Cybersecurity Awareness Training Program:** Maintain a robust cybersecurity awareness training program, including periodic phishing testing, for all employees, including bank executives. Phishing emails continue to be the leading source of compromise.

8. **Program for Active Threat Alerts:** Ensure that the institution has a program to receive, evaluate, and disseminate active threat information. Subscribing to alerts from CISA , FS-ISAC, and FBI InfraGard can provide valuable active intelligence on current ransomware and geopolitical threats.
9. **Incident Response Plan:** Develop and regularly test an incident response plan that enables a rapid response to different types of cyber incidents.
10. **Passwords**: Implement and maintain a strong password management program that particularly protects privileged access users.

CISA's Cyber Hygiene (CyHy) Services

As a complement to the above foundational cyber hygiene practices, the Department of Banking **strongly encourages** that your institution utilize two free Cyber Hygiene services from CISA, Vulnerability Scanning and Web Application Scanning.

- **Vulnerability Scanning.** This service 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.** This service takes a deeper dive into publicly accessible web applications to uncover vulnerabilities and misconfigurations that attackers could exploit.

Additional Resources:

CISA:

Shields Up Program

Stop Ransomware Program

Cyber Hygiene Services

Free Vulnerability Scanning Explained (Video)

People's Republic of China Threat Overview and Advisories

Russia Threat Overview and Advisories

North Korea Threat Overview and Advisories

Iran Threat Overview and Advisories

CSBS:

Ransomware Self-Assessment Tool