CSBS

CYBER HYGIENE FUNDAMENTALS FOR FINANCIAL INSTITUTIONS

December 15, 2025

CEO Letter

I am pleased to present *Cyber Hygiene Fundamentals for Financial Institutions*. This guide is the culmination of a CSBS campaign to raise awareness about the importance of developing and maintaining fundamental cyber hygiene practices and controls as an effective defense against the many cybersecurity threats facing financial institutions.

This document provides management and IT security personnel with ten cyber-hygiene fundamentals to help them better understand today's most common cyber threats and how to defend against them. It also provides questions specifically crafted to encourage awareness and meaningful cyber hygiene discussions between management and the board. The Guide is appropriate for both bank and nonbank institutions.

On behalf of CSBS, I want to personally thank you for taking the initiative to make your institution, your customers, and your community safer. Your leadership and vigilance remain instrumental in protecting your institutions from cyber threats, safeguarding the security of your customers' data, and strengthening the overall safety of the financial sector.

Brandon Milhorn

President & CEO, Conference of State Bank Supervisors

Introduction

For bank and nonbank financial institutions, the modern threat environment presents an ever-expanding horizon of significant adversaries and attack methods – all aimed at crippling operations, extorting money from the institution, or stealing customers' sensitive personal information. In addition, the expanding world of artificial intelligence (AI), while introducing exciting new possibilities for institution efficiencies, also introduces new attack vectors and even AI-enhanced malware attacks for threat actors.

The Guide highlights the following ***critical threats*** against bank and nonbank financial institutions:

- Ransomware
- Geopolitical and hacktivist threats
- Social engineering and phishing
- Third-party risks
- Denial-of-service attacks (DoS/DDoS)
- Corporate account takeover (CATO)

The unavoidable truth is that today's cyber threats evolve at such speed that constant attention is needed to protect the institution and its customers from potentially devastating consequences. Ensuring that your institution has a program of ***strong, fundamental cyber hygiene practices*** in place today can significantly increase security protections against these (and other) threats and make your institution a less attractive target for cyber criminals. In fact, according to former CISA director Jen Easterly, ***"Basic cyber hygiene prevents 98% of cyberattacks."***[1]

The ten fundamental cyber hygiene controls and practices addressed in this Guide are:

- Vulnerability and Patch Management
- End-of-Life Management
- Multi-Factor Authentication (MFA)
- Logging and Threat Detection
- IT Asset Management (ITAM)
- Cybersecurity Awareness Training
- Data Backup Programs
- Threat Intelligence Programs
- Third-Party Risk Management
- Incident Response Planning

Cyber Hygiene Fundamentals: A Guide to Securing Your Financial Institution Against Cyber Threats contains a catalog of ***fact sheets*** designed to provide a fundamental overview of how each of these controls and practices are critical to protecting institutions against existing and emerging cyber threats. In addition, the Guide also contains accompanying ***board questions*** that complement each fact sheet topic and arm board members with relevant and thoughtfully explained questions to ask senior management. These documents aim to improve communication and harmony between management and the board, thereby strengthening awareness of the importance of basic cyber hygiene throughout all layers of the institution.

> ***"Basic cyber hygiene prevents 98% of cyberattacks."***
> ***- Former CISA Director Jen Easterly***

[1] CISA. Press Release: CISA Unveils New Public Service Announcement – We Can Secure Our World. May 2024.

The Cyber Threat Environment

The cyber threat environment has evolved significantly over the last decade. The cybercriminal landscape has expanded beyond one-off attacks against businesses into a dangerous ecosphere of sophisticated threat actor groups, politically or socially motivated hacktivist organizations, and even nation state attackers that threaten both the financial sector as well as other elements of our critical infrastructure. Ransomware remains a dangerous weapon leveraged far too often against financial institutions, and geopolitical and hacktivist threats are fueled by ever-changing political and social climates across the world. Cyber criminals continue to develop and use advanced phishing and social engineering techniques to establish a foothold in our organizations, and denial-of-service and business email compromise attacks create disruption and exposure of sensitive customer and company information. Finally, an ever-increasing reliance on technology and third-party vendors and services has introduced less visible but equally dangerous risks to the entire financial sector.

Ransomware

Cybercrime in the financial sector continues to be prevalent and, to no one's surprise***, ransomware remains a top concern for both industry and regulators***. Financial institutions face ransomware threats from a wide variety of threat actors, including sophisticated threat groups, nation state threat actors, and politically or socially motivated hacktivist organizations. Despite some successful takedowns of ransomware organizations by international law enforcement, ransomware threat groups remain resilient and nebulous. Many criminal organizations operate in countries where cybercrimes are tolerated or, in some cases, even condoned or supported by foreign governments. Although many groups have short life spans, other groups have historically emerged – often with key players from other defunct organizations.

Today's threat actors continue to be persistent and often ruthless in the tactics they use. While more "traditional" encryption-only ransomware attacks still occur, there is a rise in popularity of double extortion tactics using encryption and exfiltration of data, as well as triple extortion tactics where a threat actor deploys a simultaneous denial-of-service attack to create chaos on multiple fronts for the targeted organization. Some threat actor groups will also contact or even extort the victim's customers directly in an attempt to generate more voices pressuring the victim to pay. In a growing number of instances, threat actors simply exfiltrate sensitive customer or company information from the victim organization, completely bypassing the deployment of malware.

To understand the nature of the ransomware threat, it is helpful to briefly examine the operational structure of the threat actor landscape. Ransomware has evolved into a sophisticated threat, and many of today's most active ransomware threat groups operate in a surprisingly similar fashion to that of legitimate businesses. These groups typically operate under a hierarchical leadership structure and often feature specialized business units such as administration, core product development, and marketing. Some threat groups interact with their victims in much the same way a legitimate company may interact with a customer, with some even utilizing tools like AI chatbots to facilitate smother negotiation and payment of ransoms. Threat groups often pay bonuses to their members, and many offer incentives such as profit sharing, training, and recruitment incentives.

Another important facet of the ransomware landscape is the emergence of ***Ransomware-as-a-Service***, or ***RaaS***, which has transformed into its own functioning, competition-driven criminal ecosystem. In simplest terms, the RaaS model works much like a legitimate franchise operation. Ransomware creators offer their ransomware infrastructure and support for sale or lease to other criminals, or “affiliates,” who actually carry out attacks. Once the victim pays a ransom, the profits are split between the two, with the affiliate generally taking the largest share. To further streamline the model, RaaS operations can also include the use of initial access brokers who provide compromised access to the targeted organizations. A primary concern of this model is the elimination of some of the barriers to entry for less sophisticated threat actors and a significant increase in the number of capable threat actors who might not otherwise possess the ability and expertise to infiltrate organizations, create and deploy their own malware, and negotiate ransom terms with the victim organization. In addition, the more RaaS developers can outsource their code and services to affiliates through the RaaS model, the more the size and scope of their attacks can grow.

In the age of connectivity and social media, ransomware attacks - particularly those that involve prominent threat actor groups - don’t stay hidden from public view for very long. Ransomware threat groups understand social media and marketing very well and, while their operations are shadowy and secretive, news of their exploits and the names of their victims are quickly publicized via social media chatter on LinkedIn, Telegram, X, and other outlets, as well as through posts on their own victim websites.

A financial institution generally looks at the decision to pay a ransom based on a number of critical factors, including the criticality of impacted systems; estimated losses from downtime; potential implications of disclosure of stolen sensitive information; legal risks; and ethical considerations. An unprepared institution might be caught without usable backups to restore data to an acceptable point, or it might simply make a business decision attempting to avoid some of the embarrassment that comes with a successful attack (although customer and regulatory notifications would still be required, regardless of whether the accessed data was published by the threat actor). Organizations may also decide that payment to a threat actor might prevent data from being publicly published.

Federal and state banking regulators, as well as federal law enforcement, discourage the payment of ransoms to threat actors for a number of reasons. ***There are <u>never</u> any guarantees that paying a ransom to a criminal organization will result in the destruction of stolen information or the decryption of encrypted data.*** Ransomware threat groups may also target organizations willing to pay ransoms with re-extortion at a later date. From a legal perspective, ransom payments provide funding directly to criminal organizations, which may violate prohibitions on transactions with OFAC-sanctioned entities. Finally, paying ransoms perpetuates the cycle of cybercriminal activity and further enables the larger ransomware ecosystem. As long as financial institutions and other companies are willing to pay ransoms, the ransomware threat will continue.

Strengthening networks and security surrounding systems and data, robust employee training, and strong incident response procedures are the most obvious defenses against ransomware, but ransomware attacks can and do happen in even the most well-defended institutions. The CSBS Ransomware Self-Assessment Tool, or R-SAT, was created by CSBS back in December 2020 in collaboration with state bank regulators, the Bankers Electronic Crimes Task Force, and the United State Secret Service to help financial institutions periodically assess their efforts to mitigate risks associated with ransomware and identify gaps for increasing security. The R-SAT effectively provides executive management and the board of directors with an overview of the institution’s preparedness towards identifying, protecting, detecting, responding to, and recovering from a ransomware attack.

Geopolitical and Hacktivist Threats

Financial institutions are also exposed to emerging risks associated with the actions of state-sponsored threat actors. The activities of nation state threat actors, particularly those from Russia, China, Iran, and North Korea, have become increasingly prominent in news headlines across 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, particularly Russian and Chinese groups, leverage ***"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. Other nations are particularly skilled at executing attacks against cryptocurrency exchanges with, most notably, a state-sponsored threat actor claiming responsibility for the largest cryptocurrency heist in history.

Nation state threat actors are driven to engage in or sponsor criminal activity by a number of factors. Some governments are motivated by the desire to establish a presence or assert dominance on the world stage, while others may engage in criminal activities in response to political or economic sanctions. In fact, some nation state cyberattacks help to fund ongoing government and military development. Nation state activities may also be motivated by the desire to progress ideological or political perspectives. Espionage and the theft of military, business, or technological trade secrets are common drivers for some successful nation state cyber intrusions. Finally, cybercrime has been woven into overall military strategy in some governments who view cyberattacks as a "hybrid" alternative to conventional or even nuclear warfare.

Financial institutions in the United States face threats from both ***direct intrusion by nation state actors***, as well as ***secondary affects from attacks on critical infrastructure sectors*** upon which we so heavily rely. The financial sector does not operate in a vacuum, as we have dependent and interdependent relationships with the energy, communications, and information technology sectors, among others. While every financial institution in the United States bears some risk of direct involvement in a nation state cyberattack, it is important to also consider responses to incidents that might impact any critical infrastructure segment(s) with which we share these dependent relationships. For example, even a local or regional disruption impacting electricity or telecommunications providers might affect the ability of all financial institutions (and society in general) to operate normally in the impacted area.

Similar threats exist from ***hacktivist organizations*** around the world. The groups often operate behind religious, political, social, or even attention-seeking motivations, and typically rely on distributed denial-of-service (DDoS) attacks, website defacement, and ransomware to accomplish their protest aims. Hacktivist organizations operate globally and may be loosely or tightly organized. They often target high-value organizations and governments, and their activities are often timed around significant global events, including wars, regional conflicts, or notable policy changes or cultural events. With most hacktivist organizations, visibility is important to outwardly emphasize their positions on issues and, like ransomware threat actors, public promotion of successful activities via social media and the internet is common.

Phishing and Social Engineering

In most instances, the weakest link in every organization's security effort is ***the human element and our daily interactions with computers***. Cybercriminals understand very well that we are all typically very busy, often distracted, and occasionally lazy and are skilled at taking advantage of these weaknesses via social engineering and phishing to steal our credentials, trick us into bogus financial transactions, and make their way into our networks and systems. Unintentional, human-driven enabling of threat actor activities is consistently a top attack vector for successful cyberattacks in all types of businesses, including financial institutions. And because it capitalizes on normal, everyday human behavior and activities, it presents a more constant danger to our institutions.

Phishing is an extremely effective social engineering technique where threat actors use well-crafted emails, text messages, and even social media posts to deceive end users into believing that the messaging is legitimate. Over the last several years, the nature of phishing techniques (and successful attempts) has evolved rapidly; we have come a long way from the "Nigerian prince scam," an early version of behavior-based social engineering. Today, threat actors use AI and other tools to create more believable deceptions that appear legitimate even to the most cautious of individuals.

There are a number of phishing variations used by threat actors, all of which utilize some form of deception. Some techniques, such as ***spearphishing***, involve the targeting of a specific individual within an organization, while others such as ***vishing*** involve attempts to deceive using the telephone. A specialized but dangerous form of phishing that can create particularly significant issues for financial institutions is ***business email compromise***, or ***BEC***. Simply put, BEC attacks typically involve impersonating executives, vendors, or customers to deceive an employee to take a specific voluntary action(s), such as providing credentials or other sensitive information. Generally, this is accomplished through the use of spoofed email accounts that may be discretely modified to closely resemble legitimate services. BEC is a particularly useful tactic to commit ***wire fraud*** in targeted institutions.

Technical tools like email and web filtering, URL scanning, and endpoint protections offer some degree of safety when threat actors tempt us with suspicious content. However, there is ***no technical substitute for human vigilance and awareness*** when it comes to protecting our institutions against social engineering and phishing. In addition, ongoing cybersecurity awareness training, including robust phishing test programs, can help to ensure that employees know ***what to look for*** and ***how to respond*** when confronted with suspicious emails or other content. It's all about creating ***an ongoing culture of cyber awareness*** to provide a first line of defense against the threat of social engineering and phishing.

Third-Party Risks

Every day, financial institutions of all sizes and all types rely on tools and technology to operate. Today, even the smallest financial institutions can take advantage of technology that was once available only to the largest organizations. From software that helps us perform the most mundane of everyday tasks to complex core operating system platforms that form the very operational backbone of our institutions, there is no escaping the ever increasing impact of technology. And with the vast majority of those tools and technologies coming from external vendors and service providers, there is an expanding aspect of third-party risk that has been introduced into our institutions.

While maintaining security protections for internally managed tools and technology can be challenging enough, a greater difficulty lies in the management of risk from external vendors outside our immediate control – and ***given our heavy reliance on technology, these risks can be significant***. A security incident impacting a core service provider, for example, might trigger a number of issues for institutions ranging from full or partial system unavailability to the loss of sensitive customer data. In addition, static or intermittent connections to external service providers can create access control and data security issues if not managed properly. Botched or corrupted software updates from vendors can also create significant operational and security issues for the institution, and threat actors have historically demonstrated an ability to compromise seemingly legitimate vendor-issued hardware and software updates through direct infiltration and compromise of third-party providers or their downstream vendors.

Strong vendor management programs can help to reduce some of the risks associated with third-party relationships. The *Interagency Guidance on Third-Party Relationships: Risk Management*[2] outlines the federal banking agencies' views on ***sound risk management principles for all stages of the third-party risk management life cycle***. According to the guidance, financial institution third-party risk management practices should account for relationship planning activities; initial due diligence and selection of the third party; negotiation of contracts that are beneficial to the institution and allow for monitoring of measurable metrics; ongoing monitoring of the relationship; and processes to allow for the smooth termination of the relationship if necessary. To the extent possible, careful consideration should also be paid to contractual relationships third parties have with contractors, subcontractors, or other third parties to identify downstream supply chain risks where they may exist. A comprehensive understanding of all facets of these third-party relationships can help to ensure that the institution is both informed of potential risks throughout the life of the relationship and prepared to react to them, when necessary.

Denial-of-Service Attacks

Denial-of-service, or ***DoS***, attacks, are a tactic used by threat actors to negatively impact a financial institution's network or services, most typically by "flooding" the victim organization with a number of illegitimate requests that overwhelm the ability to handle network traffic. When critical resources such as network bandwidth, system memory, or CPU capacity are strained by this overwhelming traffic, the result can be an inability to access websites, servers, routers, firewalls, applications, or other online resources, including some that may be critical to operations. Threat actors also occasionally exploit unpatched vulnerabilities in web servers, APIs, or databases to overwhelm system memory or execute other resource draining actions.

Another variation of the DoS attack is the ***distributed denial-of-service***, or ***DDoS***, attack. The DDoS attack is different from a standard DoS attack in that it originates from multiple compromised systems, or "botnets" - networks of remotely controlled machines (bots) that work in concert with one another, potentially from locations all across the world. This, of course, can introduce additional difficulties to network defenders due to the typically wide dispersal of attacking locations. DoS and DDoS attacks are favored attack methods for many hacktivist organizations due to their immediate and often publicly visible effects.

Financial institutions can utilize a number of protections to reduce the impact of these attacks, including rate limiting techniques, network filtering, load balancing to manage network traffic, and even cloud-based DDoS protection services to identify and stop attacks before they can become problematic.

Corporate Account Takeover

Corporate account takeover**, or **CATO**,* attacks typically happen as a result of unauthorized access and control of a legitimate user's account(s) or systems – most often as the result of the use of valid, stolen credentials obtained through phishing, Dark Web credential purchases, or even via malware deployment. Although the end result of the CATO attack can be somewhat similar to that of ***business email compromise,

[2] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Interagency Guidance on Third-Party Relationships: Risk Management. June 2023.

CATO actually involves the actual compromise of an account via unauthorized credential use or an exploited vulnerability as opposed to impersonation.

When a successful CATO attack occurs, the attacker can operate under the trusted guise of a legitimate user, which can allow any number of malicious activities, including ***address changes, additional credential harvesting, unauthorized access to sensitive personal information,*** and ***fraudulent financial transactions***. This makes the CATO attack so difficult to recognize and remediate, which heightens the potential danger for the legitimate account holder and the institution.

CATO attacks are typically made more difficult for threat actors through the use of multi-factor authentication (MFA), regularly patching of systems, and by monitoring accounts for anomalous activity. Moreover, employee training is also important to enable better recognition of credential theft and phishing attempts that can enable future CATO attacks.

Conclusion

How do we defend our institutions against the myriad threats facing us today? While technology advances in sophistication and effectiveness offer prospects for more effective security protections, the simple fact is ***there is no one impenetrable security device, technique, or practice that can provide total security protection for our institutions***. Instead, we believe that the most effective security protections available to counter the threats presented in this Guide are a product of the ***consistent implementation and management of the ten fundamental cyber hygiene practices presented in this Guide***.

Cybersecurity has evolved from a back-office activity into a legitimate financial and operational concern that demands the ongoing attention of the entire organization – from the board of directors to the most junior staff in the organization. The controls and practices referenced in this Guide are not one-time, “fix it and forget it” solutions. Instead, they require an “all hands on deck” approach to ensure that they receive appropriate, ongoing attention within the institution.

The good news is that each of the ten controls and practices referenced in this Guide should not be new to financial institutions - in fact, they have been staples of security in financial institutions for years. To that end, the Guide is not intended to introduce new regulatory guidance to financial institutions but, rather, to inform institutions of basic fundamentals, highlight the importance of consistent implementation of each control and practice, and encourage level-setting discussions between IT security staff, senior management, and the board. We believe the controls and practices highlighted in this Guide, while fundamental in nature, can go a long way to secure your institutions and your sensitive customer data against these and other threats when they are ***well-understood, consistently applied, and managed effectively*** within the organization.