The Fundamentals of Cyber Hygiene for Financial Institutions

BLOG POST

The Fundamentals of Cyber Hygiene for Financial Institutions

January 5, 2026
|
Download PDF

Access CSBS's Complete *Cyber Hygiene Fundamentals for Financial Institutions Guide*

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.

Having fundamental awareness of how to protect your institution from cyberattacks is important. In fact, according to former CISA director Jen Easterly,

> "Basic cyber hygiene prevents 98% of cyberattacks."

That's why we've issued the *Cyber Hygiene Fundamentals for Financial Institutions Guide*. The Guide contains a catalog of ***fact sheets*** designed to provide a fundamental overview of how certain controls and practices are critical to protecting institutions against existing and emerging cyber threats. In addition, it contains accompanying ***board questions*** that complement each fact sheet topic to 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.

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)

In addition, the following ten fundamental cyber hygiene controls and practices are addressed in this Guide:

- 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

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.

Read more on the Guide, fact sheets, and board questions below.

Cyber Hygiene Fundamentals for Financial Institutions Guide

Fact Sheets and Board Questions