CSBS

The Fundamentals of Cyber Hygiene for Financial Institutions

Jan 05

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.

"Basic cyber hygiene prevents 98% of cyberattacks."
Jen Easterly, former CISA director

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.

The fact sheets do not introduce new guidance to the institution but are intended to amplify best practices from existing regulatory guidance, CISA, NIST, the FFIEC IT Handbook booklets, and other authoritative sources. They were developed 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.

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

Cyber Hygiene Fundamentals Guide

- Cyber Hygiene Fundamentals: A Guide to Securing Your Financial Institution Against Cyber Threats

Fact Sheets

- IT Asset Management (ITAM)
- Threat Intelligence Programs
- Data Backup Programs
- Cybersecurity Awareness Training
- Event Logging & Threat Detection
- End-of-Life (EOL) Management
- Multi-Factor Authentication
- Third-Party Risk Management (TPRM)
- Incident Response Programs

- Vulnerability and Patch Management

Board Questions

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

Top Category

Opinions & Insights

202.296.2840
newsroom@csbs.org
1129 20th Street, N.W., 9th Floor, Washington, DC 20036