Additional Cybersecurity Resources

FFIEC
www.ffiec.gov/cybersecurity.htm

The White House
www.whitehouse.gov/issues/technology
www.whitehouse.gov/issues/foreign-policy/cybersecurity

Department of Homeland Security
www.dhs.gov/topic/cybersecurity
www.dhs.gov/stopthinkconnect
www.us-cert.gov

Federal Bureau of Investigation
www.fbi.gov/about-us/investigate/cyber
http://www.ic3.gov/default.aspx

U.S. Secret Service
www.secretservice.gov/ectf.shtml
www.secretservice.gov/ntac.shtml

SANS Institute
www.sans.org

Financial Services Information Sharing and Analysis Center
www.fsisac.com

ISACA
www.isaca.org

Open Web Application Security Project (OWASP)
www.owasp.org

Software Engineering Institute CERT Division
www.cert.org/resilience/
www.cert.org/cybersecurity-engineering/

National Institute of Standards and Technology
www.nist.gov/cyberframework/index.cfm
http://csrc.nist.gov/publications/

For More Information, Contact Your FFIEC Agency

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
www.fdic.gov

Federal Reserve Board
20th and C Streets NW
Washington, DC 20551
www.federalreserve.gov

National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314
www.ncua.gov

Office of the Comptroller of the Currency
400 7th Street SW
Washington, DC 20024
www.occ.gov

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
www.consumerfinance.gov

State Liaison Committee through the Conference of State Bank Supervision
1129 20th Street NW, 9th Fl
Washington, DC 20036
www.csbs.org

Additional guidance is available at www.FFIEC.gov/cybersecurity.htm and through the FFIEC IT Handbook InfoBase at ithandbook.ffiec.gov.

Cybersecurity and Resilience Against Cyber Attacks

FFIEC

Federal Financial Institutions Examination Council

Cyber Threats

Cyber threats have evolved and increased exponentially, occurring on a more frequent basis and with greater sophistication than ever before. Because financial institutions are dependent on technology for critical operations, decisions related to new products and services, along with general technology investment decisions, may expose financial institutions to vulnerabilities that need to be anticipated and managed. Criminals increasingly exploit these weaknesses to attack financial institutions. Cyber threats expose institutions to operational, reputation, and financial risks.

Who are cyber attackers?

- Nation-states
- Terrorists
- Criminal enterprises
- Insiders

Why do they do it?

- Espionage
- Money
- Disruption/ destruction
- Political/social statement
- Notoriety

What are their strengths?

- Technical expertise
- Financial sponsors
- International reach
- Weak legal reach
- Anonymity

What is the impact to an institution?

- Lost financial assets
- Stolen customer information
- Stolen intellectual property
- Business disruption
- Damaged reputation

An institution should take a comprehensive approach to maintain the security and resilience of its technology infrastructure including the establishment of a robust cybersecurity framework. The framework should incorporate processes to identify, prevent, detect, respond to, and recover from technology-based attacks. Focusing on the following five key areas will improve your cybersecurity preparedness.

Cyber Risk Management & Oversight

Strong Governance is Essential

Establish robust governance policies and risk management strategies. Commit sufficient resources including expertise and training. Establish an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation.

Threat Intelligence & Collaboration

Strength in Numbers

Monitor timely threat information and intelligence to discover threats and identify attack methods. Leverage known intelligence sources to develop preventative and responsive strategies. Share crucial threat information and intelligence with partners and stakeholders to strengthen your security posture.

Cybersecurity Controls

More Than One Kind of Control

Incorporate physical, logical, and other cybersecurity controls to prevent, detect, and mitigate cyber attacks. Implement preventative controls to minimize the impact and likelihood of successful attacks, detective controls to identify attacks in early stages, and corrective controls to mitigate the impact.

External Dependency Management

Your Security Starts with Their Security

Identify your critical external dependencies. Establish rigorous vendor management controls, including ongoing due diligence and monitoring. Define third parties' responsibilities and associated service level metrics. Evaluate vendors' incident response and resilience.

Incident Management & Resilience

Mitigation and Recovery are a Must

Prepare for potential cyber attacks by establishing incident management procedures in order to speed your ability to respond and recover from a cyber incident. Mitigate the loss of customer confidence through timely and appropriate customer notification.

Develop policies and implement adequate incident response programs. Define capabilities and required resources to address threats and recovery. Use monitoring tools to capture events, and to identify anomalous behaviors and attacks. Escalate and report cyber incidents to the institution's board of directors and senior management when warranted.

Responding to an Incident

Take appropriate steps to respond to a cyber incident:

- Assess the nature and scope of an incident and identify what information systems and types of information have been accessed or misused.
- Promptly notify your primary regulator when you become aware of an incident involving unauthorized access to or use of sensitive customer information, and generally, following any incident that could materially impact your institution.
- Comply with applicable suspicious activity reporting regulations and guidance. Ensure appropriate law enforcement authorities are notified in a timely manner.
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to or misuse of information.
- Notify customers as soon as possible when it is determined that misuse of sensitive customer information has occurred or is reasonably possible.