CYBERSECURITY

Incident Response and Risk Management

Federal Reserve Bank of Dallas

Given the increase in both sophistication and frequency of successful cybersecurity breaches, as your primary regulator, we would like to remind you of our expectations for effective cybersecurity incident response and risk management.

How to Proceed

When is cyber incident reporting required?

- There is a possible or confirmed compromise of sensitive customer information
- Indicators of "possible" compromise
  - Threat to confidentiality, integrity, and/or availability of information systems or data
  - Presence of malicious software on network
  - System outages
  - Reporting of other incidents that may have safety and soundness implications is encouraged.

"Sensitive" customer information includes:

- Name, address, or telephone number and one of the following:
  - Social security number
  - Driver's license number
  - Account number
  - Credit or debit card number
  - Personal identification number or password

Collaborate with Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Department

- Let your bank's BSA/AML Department know the details of the event so that it may take appropriate action.
- Provide your BSA/AML staff with important cyber details such as the IP address.

How do I report?

- Email the Dallas BS&R incident mailbox:
  - BSR.Incident.Report@dal.frb.org
- Contact Meeoak Cho, IT Director of Examinations or Drew Wilson, IT Supervision and Risk Coordinator
  - meeoak.cho@dal.frb.org / 214.922.5960
  - drew.wilson@dal.frb.org / 214.922.6252
- Mail correspondence to the Federal Reserve Bank of Dallas:
  - Meeoak Cho, IT Director of Examinations, Federal Reserve Bank of Dallas, 2200 N. Pearl St., Dallas, Texas 75201

For more information

- SR 05-23 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- FFIEC Information Technology Examination Handbook Infobase
- FIN-2016-A005 FinCEN Advisory to Financial Institutions on Cyber Events and Cyber-Enabled Crime
- FIN-2019-A005 FinCEN Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes

See the reverse side for information on effective cybersecurity risk management practices.

EFFECTIVE CYBERSECURITY PRACTICES

HYGIENIC PRACTICES

IT Asset Management

Updated asset inventory is maintained. The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, repurposed and sunset assets.

Access and Data Management

Ensure controls for user access. Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.

SURVEILLANCE

Threat Intelligence and Information

Threat intelligence is collected and assessed. The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). Threat information is used to monitor threats and vulnerabilities.

RISK MANAGEMENT AND GOVERNANCE

Cyber Risk Management and Oversight

Ensure proper oversight. The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.

Incident Response Planning

Document and test cyber incident response plans. A plan for detecting, containing and responding to cyber or other information security incidents has been documented and tested.

Threat and Vulnerability Detection

Security assessments are conducted. Independent testing (penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.

Due Diligence

Due diligence is conducted. Risk-based due diligence is performed on prospective third-party vendors before contracts are signed, including reviews of their background, reputation, financial condition, stability and security controls.