Cybersecurity Threats & Management

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Scope of Discussion

- Threat Environment
  - Cybercrime Analysis
  - Kansas City Region Security Incidents
- Cyber Threat Governance
  - Information Security Program
  - Domain 1 – Cyber Risk Management and Oversight
  - Domain 2 – Threat Intelligence and Collaboration
  - Domain 3 – Cybersecurity Controls
  - Domain 4 – External Dependency Management
  - Domain 5 – Incident Management & Resilience
- Director Responsibilities
- Resources

Threat Environment
Cybercrime Analysis

2,760,044 Total Complaints

$18.7 Billion Total Losses

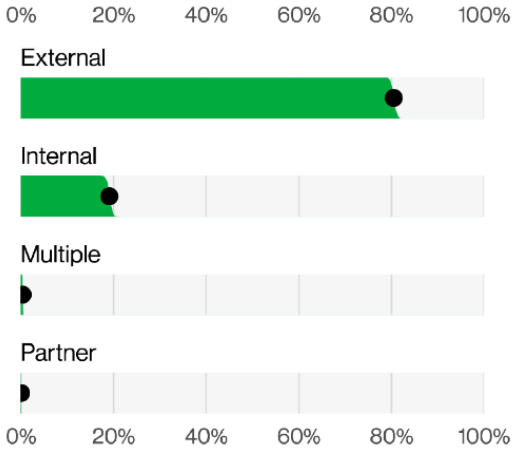
IC3 Complaint Statistics 2017-2021
The Internet Crime Complaint Center (IC3) receives complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

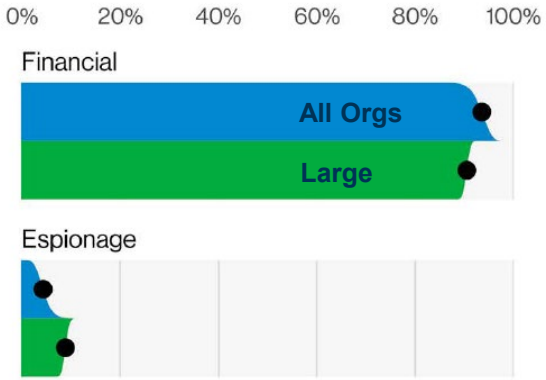
Threat Environment
Cybercrime Analysis

Verizon 2021 Data Breach Investigations Report

Perpetrators



Commonalities



"Most data thieves are professional criminals."

Top Breaches

Phishing	70%
Stolen Credentials	30%

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Threat Environment
Cybercrime Analysis

Employees are the leading cause of ransomware events

Causes	Controls
Phishing (leading cause) Cybersecurity Training Weak Passwords Mistakes	Education Awareness Strong Authentication Practices

Source: Datto 2020 Global State of the Channel Ransomware Report

Threat Environment
Cybercrime Analysis

Source: Microsoft Digital Defense Report – October 2021

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Threat Environment
Cybercrime Analysis

- Phishing
  - More than 75% of phishing emails include malicious URLs to phishing sites.
    - Other variations include malicious phishing attachments and links in attachments.
- Drive-by Downloads
  - User is browsing a website and an ad, banner, or script runs malicious code on the system.

Source: Microsoft Digital Defense Report – October 2021

Cyber Incidents at Banks
Kansas City Region Security Incidents – Case 1

Under $300 Million Asset Bank

- Compromised / Malicious Ad Content
- Ransomware
  - Network
  - Loan Document Imaging System
- Identified, Isolated, and Removed
- Paid Ransom and Decrypted Backup

Cyber Incidents at Banks
Kansas City Region Security Incidents – Case 1

Under $300 Million Asset Bank

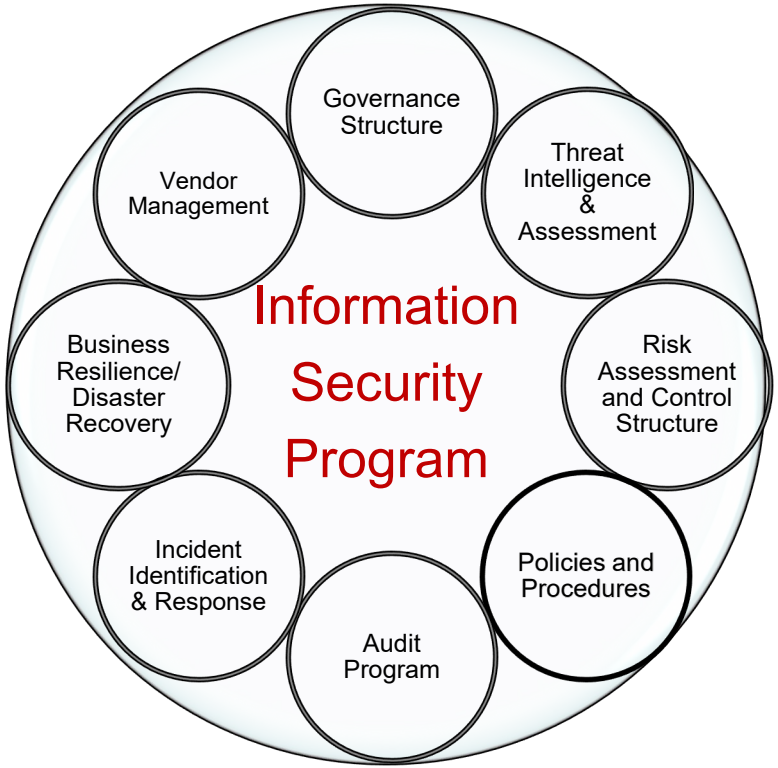
- Lessons Learned
  - Utilize anti-virus and anti-malware scanning for file downloads
  - Implement web browsing controls
  - Ensure frequent back-up of critical data
  - Consider limiting personal use of bank systems

Cyber Incidents at Banks
Kansas City Region Security Incidents – Case 2

Under $1 Billion Asset Bank

- Client and loan officer email compromise
- 3 fraudulent wires
  - $1.6 Million Gross Loss
  - $1.0 Million Net Loss
- No call back verification

Cyber Threat Governance
Information Security Program



Cyber Threat Governance

Domain 1 – Cyber Risk Management & Oversight

Strong Governance is Essential

- **Establish robust governance policies and risk management strategies based upon the risk assessment.**
- **Commit sufficient resources including expertise and training.**
- **Establish an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation.**
- **Provide for regular independent testing of the key controls.**

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Cyber Threat Governance
Domain 1 – Cyber Risk Management & Oversight

Audit Program Components

- IT General Controls
- Vulnerability Assessment
  - Authenticated vs. Unauthenticated
- Penetration Test
- Social Engineering Testing
- Independence
- Outsourcing

Cyber Threat Governance
Domain 2 – Threat Intelligence & Collaboration

Strength in Numbers

Establish a monitoring and tracking system.

- Join information sharing forums such as FS-ISAC, FBI Infragard or others.

Develop preventative and responsive strategies.

Share crucial threat information and intelligence with partners and stakeholders.

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Cyber Threat Governance
Domain 3 – Cybersecurity Controls

More Than One Kind of Control

Incorporate physical, logical, and administrative controls to prevent, detect, and mitigate cyber attacks.

Implement preventive controls to minimize the impact and likelihood of successful attacks.

Implement detective controls to identify attacks in early stages.

Implement corrective controls to mitigate the impact.

Cyber Threat Governance
Domain 3 – Cybersecurity Controls

Control Types	Preventive	Detective	Corrective
Physical	Procedures Locks / Cameras Disposal Procedures	Security Systems Physical Environment Monitoring	Offsite Facilities Compromised Data / Hardware Disposal Process
Logical	**Multi-Factor Authentication** Firewalls & Routers / Configs Encryption Workstation Timeouts Strong Passwords Restrict Removable Media **Patch / EOL Management**	Antivirus Alerts & Anti Malware Data Loss Prevention Vulnerability Scans Penetration Testing Customer Fraud Alert Detection System	Update Access Privileges Recover System Functions
Administrative	**Policies & Procedures** User Agreements Separation of Duties **Training / Awareness** Clear Organizational Structure	Review Access / Security Logs Rotation of Duties Reconciliations Audits / Independent Testing Process to Monitor & Report Suspicious Activity	Business Resumption Plans Penalties / Termination Report Incidents to Board Process to Address Audit / Examination Weaknesses

Cyber Threat Governance
Domain 4 – External Dependency Management

Your Security Starts with Their Security

- Identify and risk assess your critical external dependencies.
- Perform risk-based due diligence on prospective third parties.
- Define third parties' contractual responsibilities and associated service level metrics.
- Perform ongoing risk-based monitoring of critical third parties.

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Cyber Threat Governance
Domain 4 – External Dependency Management

Outsourcing - Responsibility

Board and management are responsible for identifying and controlling risks arising from activities conducted through third parties to the same extent as if the activities were handled within the institution.

Managed Security Services/Patching

Be clear on who is responsible for what, and what you are buying / not buying.

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Cyber Threat Governance
Domain 5 – Incident Management and Resilience

Mitigation & Recovery Are Of Critical Importance

- **Develop policies and implement adequate incident response programs.**
- **Understand dependencies and critical third parties.**
- **Review cyber incidents during board meetings and the response strategy.**
- **Provide for and test backup / recovery plans.**

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

20

Cyber Threat Governance
Domain 5 – Incident Management and Resilience

Ransomware Vignette – Lessons Learned

- Establish adequate system configurations
- Formalize processes
- Complete data inventory and classification
- Ensure comprehensive backup processes

Cyber Threat Governance
Domain 5 – Incident Management and Resilience

Elements of Incident Response

- Assess nature / scope of the incident
- Contain and control the incident
  - Preserve records
  - Consider forensic engagement if warranted
- Communicate to Senior Management / Board
- Notify customers (if needed)
- Notify your primary Federal regulator
  - Unauthorized Access or Material Disruption

Cyber Threat Governance
Domain 5 – Incident Management and Resilience

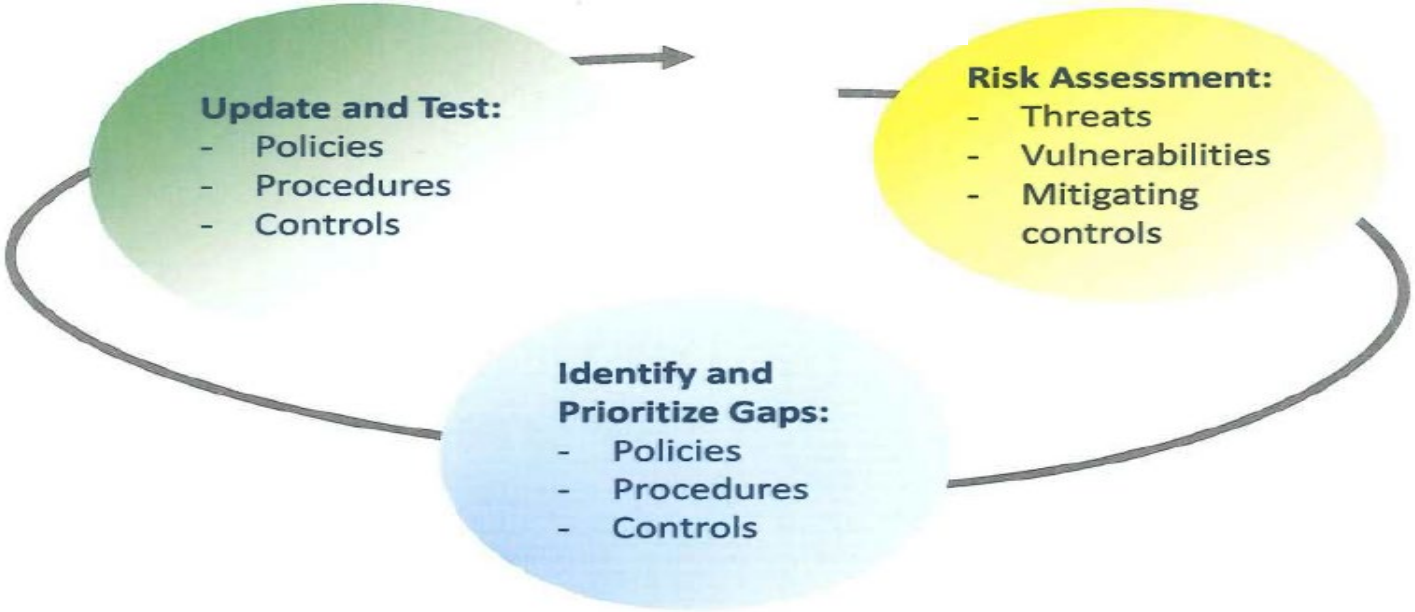
Resilience

- Effective backup solutions
- Network segmentation
- User access rights (UAR)
- Active monitoring and alerting
  - Intrusion Detection and Prevention Systems (IDS/IPS)
  - Anti-Virus / Malware
  - Patching
- Connectivity redundancy

The ability to prepare for and adapt to changing conditions and withstand and rapidly recover from disruptions.

Directorate Responsibilities

Ensure an Ongoing Cyber Threat Governance Cycle



Directorate Responsibilities

Examples of topics for regular Board reporting:

- Risk assessment conclusions and resulting policy / control changes
- Network security controls (e.g., firewalls, intrusion detection / prevention)
- Patch management / vulnerability remediation program
- End-of-life software / hardware management
- Network / system availability and capacity
- Security / cyber incidents
- Audit results and remediation status
- Vendor management reports
- Status of Major IT projects

Part 364

Appendix B

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Resources: Cyber Exercises

FDIC Directors' Resource Center

Cyber Challenge: A Community Bank Cyber Exercise

- Item processing failure
- Customer account takeover
- Bank internal error / phishing and malware problem
- Technology service provider problem
- Distributed denial of service attack
- ATM malware
- Ransomware
- Flood
- Supply Chain

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html

Questions?