Cybersecurity

Inherent Risks and Preparedness

Regional and Community Banks

Disclaimer

The opinions expressed in this presentation are intended for informational purposes, and are not formal opinions of, nor binding on, the Federal Reserve Bank of Boston or the Board of Governors of the Federal Reserve System.

Definition

Cybersecurity

"measures taken to protect a computer or computer system (as on the **Internet**) against unauthorized access or attack" - Merriam-Webster

Computer network component of an information security program

Data Security Breaches

- 37% affected financial organizations (+)

Organizations with fewer than 1000 employees

- 88% perpetrated by outsiders
- 19% committed by insiders; however
  - 54% incorporated malware (common in financial)
  - 32% leveraged social tactics (+)

* Verizon 2013 Data Breach Investigations Report (+ increasing)

Discussion Approach

- FFIEC General Observations (11/3/2014)
- Threats: Not a technical deep dive
- Reality Check: In the news
- Discuss opportunities and best practices
  - Existing programs and controls
  - Limited IT resources
  - From a business perspective

- *In short, what I'd want to discuss with my IT leaders*

FFIEC General Observations

- key findings from the 2014 cybersecurity assessment pilot (500 community banks)

- provides questions directors and senior management at community banks and thrifts should be asking

- Cybersecurity Inherent Risks
- Cybersecurity Preparedness

Cybersecurity Inherent Risks

FFIEC General Observations

- Comprehensive Inventory?
- Products and Services
  - Hardware
  - Software
  - Connections !

Cybersecurity Inherent Risks

Reality Check: Target breach

- 3rd party connection
- Not IT support or services, but a billing service
- “one off”

Cybersecurity Inherent Risks

Existing IT and GLBA risk assessments

- Is it comprehensive?
- BYOD (bring your own device)
- Internet services
- Guest access
- Vendors / 3rd Parties connections
- Threats evolve, so should the mitigating controls (frequency and changes)
- Risk appetite (Business, not IT)

Cybersecurity Preparedness

- Risk management and oversight
- Threat intelligence and collaboration
- Cybersecurity controls
- External dependency management
- Cyber incident management and resilience

Cybersecurity Preparedness

1. External dependency management

2. Cybersecurity controls

   Cyber incident management and resilience

3. Threat intelligence and collaboration

   Risk management and oversight

Cybersecurity Preparedness

1. External dependency management

   FFIEC General Observations

- Ensuring third parties have effective cyber security controls?
- Role and responsibilities?

Cybersecurity Preparedness

1. External dependency management

   <u>Vendor Management Program</u>

- Risk Rating process (information and access)
- SOC* Reports (SOC1 vs. SOC2; Type-1 vs Type-2)
- Complimentary End User Controls (CEUC)
- FFIEC Technology Service Provider (TSP) Reports
- Due Diligence (new vendors)
- Safeguarding customer information
- Alerts and notifications
- Exit Strategy (decommissioning - data)

* Service Organization Controls

Cybersecurity Preparedness

2. Cybersecurity controls / Cyber incident management and resilience

   FFIEC General Observations

- Preventive, Detective and Corrective
- Scenarios and Response (IRP and BCP)

Cybersecurity Preparedness

2. Cybersecurity controls / Cyber incident management and resilience

   Reality Check : Unlimited Operations

- Malware “inside” the bank
- Admin control of ATM application
- Change Limits and fraud detection
- ATM skimming primarily targets large banks
- 3D printers on the rise

Cybersecurity Preparedness

2. Cybersecurity controls / Cyber incident management and resilience

Vulnerability Assessments (Penetration Testing)

- Frequency
- Exception Tracking

Event Correlation

- Anomalies – access and log reviews
  - Manual “human” anomaly detection can be effective
- IT and the Business side – correlation

Cybersecurity Preparedness

2. Cybersecurity controls / Cyber incident management and resilience

   Reality Check : CATO (Account Takeover)

- Due Diligence – i.e., KYC
- Limits and notifications
- Limited multi-factor authentication

Cybersecurity Preparedness

2. Cybersecurity controls / Cyber incident management and resilience

Corporate Accounts

- Limits and notifications
  - Are these part of the customer agreements?
  - Are they monitored?
- Multi-factor Authentication
  - out-of-band
  - out-of-wallet challenge questions
- What exceptions have been made?

Cybersecurity Preparedness

3. Threat intelligence and collaboration
   Risk management and oversight
   FFIEC General Observations

- Monitor and maintain sufficient awareness of cyber threats and vulnerability information.

- Establish procedures for how to evaluate and apply information.

Cybersecurity Preparedness

3. Threat intelligence and collaboration
   Risk management and oversight
   Reality Check: JPMorgan

- **FS-ISAC** circulated JPMorgan's data to help other companies assess whether they had been attacked.
- The information included Internet protocol addresses linked to servers that the hackers had used to communicate with the bank's computers and then to extract data.

Cybersecurity Preparedness

3. Threat intelligence and collaboration
   Risk management and oversight

<u>Technical Awareness</u>

- US-CERT, DHS, Anti-virus and other security services
- Industry news sites, e.g. krebsonsecurity.com, bankinfosecurity.com

Cybersecurity Preparedness

3. Threat intelligence and collaboration
   Risk management and oversight

<u>Situational Awareness</u>

- Financial Services-Information Sharing and Analysis Center (**FS-ISAC**) – different levels of membership
- Financial industry associations
- FFIEC joint statements
- SMB's have 'AsktheFed' sessions; other agencies have similar reference material

Cybersecurity Preparedness

3. Threat intelligence and collaboration
   Risk management and oversight

Employee Education

"Tone From the Top"

Test it (Social Engineering) – the "other" insider threat

Customer Education

Pro-active outreach and tools

Don't allow customer security education to get stale

Summary of “Quick Wins”

1. IT Asset Inventory (HW/SW/Connections)
2. Vulnerability Assessments and Remediation
3. Customer Access (Authentication and exceptions)
4. Social Engineering Tests
5. Cybersecurity Awareness “Education”
   - Threat Intelligence (IT and Fraud)
   - IT Policies and Agreements (All Employees)
   - Outreach (Customers)

References

- SR 11–9, “Interagency Supplement to Authentication in an Internet Banking Environment”

FFIEC Press Releases/Joint Statements

- FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center, November 3, 2014
- “State and Federal Regulators: Financial Institutions Should Move Quickly to Address Shellshock Vulnerability”, September 26, 2014
- “FFIEC Launches Cybersecurity Web Page, Promotes Awareness of Cybersecurity Activities”, June 24, 2014
- “FFIEC Promotes Cybersecurity Preparedness for Community Financial Institutions”, May 7, 2014
- “Financial Regulators Expect Firms to Address OpenSSL “Heartbleed” Vulnerability”, April 10, 2014
- “Cyber-attacks on Financial Institutions’ ATM and Card Authorization Systems”, April 2014
- “Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources”, April 2014

References

ISACA Journals

- “The IS Audit Transformation”. Volume 2, 2014
- “Language of Cybersecurity”, Volume 4, 2013
- “Legal and Regulatory Challenges”, Volume 2, 2013

- The Institute of Internal Auditors Research Foundation, ”Cybersecurity: What the Boards of Directors Needs to Ask”, Sajay Rai, 2014
- Geoff Collins, Four simple steps to protect the US from hackers
- http://www.usatoday.com/story/tech/2013/03/25/cybersecurity-simple-steps/2016243/
- Verizon 2013 Data Breach Investigations Report
- For additional information on the DBIR and access to related content, please visit www.verizonenterprise.com/DBIR/2013