Office of the Comptroller of the Currency

Independent Bankers Association of New York State

Pittsford, NY - June 19, 2018

Bank Information Technology Matters Requiring Your Attention

Stephen Kunzinger, Northeastern District BIT Lead Expert Support

Office of the Comptroller of the Currency

Agenda

- **Cyber-Threats**
- **Cybersecurity Control Measures**
- **Notable Cybersecurity Risk and Control Gaps**
- **What to do After an Intrusion**
- **Cybersecurity Preparedness**
- **Recent Trends**
- **Cybersecurity Assessment Tool (CAT)**
- **Common Cyber/Technology Exam Findings**

Office of the Comptroller of the Currency

Cyber - Threats

Top Cyber-Threats

- **System Disruption**: DDoS, Infections, Ransomware
- **Identity Theft**: Unauthorized retrieval of private data
- **Financial Frauds**: Account takeover, phishing, e-mail scams
- **Intrusions Trends**: Invasive ---> Disruptive

Office of the Comptroller of the Currency

Cyber - Threats

Attack Vectors

- **Phishing –** a form of e-mail deception used to obtain sensitive information.
- **DDoS -** In a DDoS attack, the attacker seeks to overload resources that provide access to the bank's Internet site.
- **Ransomware –** Malware that encrypts data on the target system making it unusable.
- **Malware** infection on network components primarily by e-mail attachments or downloads from internet sites.

Office of the Comptroller of the Currency

Control Measures

Detect/Prevent Cyber-Intrusions

- Understand the types of attacks and intrusions
- Know the warning signs
- Log & Monitor systems performance and traffic
- Implement administrative and technical safeguards and controls
- Implement stronger access control measures for e-Banking applications that process financial transactions

Office of the Comptroller of the Currency

Control Measures

Administrative Safeguards

- Document a BOD approved cyber-security plan
- Document a network infrastructure security policy
- Perform a cyber-threat vulnerability analysis
- Document a cyber-security policy and program
- Document procedures for network and system administration
- Evaluate effectiveness of cyber-security controls & measures
- Periodic reviews of systems access authorities
- Employees' awareness and cyber-security education program

Office of the Comptroller of the Currency

Control Measures

Technical Safeguards

- Maintain robust configuration of IDS/IPS and firewalls
- Patch & upgrade systems / Replace Obsolete systems
- Update network configuration-Deactivate unused interfaces, services, devices
- Protect system configuration files.
- Restrict remote administration of the network.
- Antivirus and anti-malware solutions.
- Implement network segmentation-isolate critical systems.
- Restrict administrative access to network & critical systems.
- Log and monitor network access activities

Office of the Comptroller of the Currency

Notable Risks/Control Gaps

- Poorly configured components
- Unpatched systems
- Use of systems that have reached EOL
- Lack of critical security components (i.e. Firewalls, IDS/IPS)
- Poorly configured security devices
- No vulnerabilities assessment and intrusion detection tests
- No monitoring systems
- Inadequate access control procedures
- Inadequate change management and patching procedures
- Unsecured connection and facilities

Office of the Comptroller of the Currency

What to Do After an Intrusion

- Maintain up-to-date Incident Response Program – OCC Bulletin 2005-13 (https://occ.gov/news-issuances/bulletins/2005/bulletin-2005-13.html)
- Notify Regulators and law enforcement agency
- File SAR
- Capture and store system logs for analysis and forensic review
- Patch the affected systems and update software patches on all systems
- Perform scan and vulnerability assessments on back-up systems
- Restore the primary systems using backed-up files
- Change all passwords
- Communicate the breach (to customers, other affected stakeholders)
- Install missing security controls

Office of the Comptroller of the Currency

Cybersecurity Preparedness

- Strong user awareness and testing programs on:
  - Phishing, data loss prevention, secure connections, secure devices
- Patch, Patch, Patch….
- Stronger Authentication for: Privileged users, money movers, high profile users (Database admins, system admins, wire/ACH)
- Network Segmentation and data encryption (Prevent intruders from moving or identifying critical data if inside)
- Resilience, to be able to recover.
- Engagement with Law Enforcement and FBI

Office of the Comptroller of the Currency

Recent Industry Trends

Verizon Data Breach Investigations Report

- 2017 saw 53,000 incidents with 2,216 Confirmed Data Breaches.
- Phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%).
- 58% of breaches to small businesses (your clients)–Risk to client AND banks

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

M-Trends 2018 by FireEye

- Top industries with most significant attacks: ***financial***, high-tech and healthcare.
- Spear-phishing continues to be the most effective initial compromise method,
- Social media links to compromised websites using news/tips as lure continue to increase as an initial compromise method
- Re-targeting of organizations after being compromised is now 56%.
- In addition 49% of customers with at least one significant attack (data theft, compromised accounts, credential harvesting, lateral movement and spear phishing) were successfully attacked again within one year.

https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

Office of the Comptroller of the Currency

Bank Reported Issues

- **ATM Skimming**
- **Phishing Scams**
  - Bank employees
  - Bank customers

Cybersecurity Assessment Tool (CAT)

Office of the Comptroller of the Currency

June 2015:

- FFIEC developed a self assessment tool

October 2015:

- OCC - CAT as an examination tool

Office of the Comptroller of the Currency

Matters Requiring Attention

THE PAST 3 YEARS:

- Information Technology MRAs outstanding Nationwide have increased by 25%
- Cyber/Information Security remains the number one area of concern.
- Business Continuity is 2nd
- IT Operations and Vendor Management round out the top four concerns.

Office of the Comptroller of the Currency

Information Technology MRAs

NATIONWIDE

TOTAL OUTSTANDING CONCERNS	2016 Rank	2018 Rank	Overall 25% Increase
Cyber/Information Security	1	1	140%
Management Oversight	2	5	
Business Continuity	3	2	129%
Vendor Management	4	4	122%
IT Operations		3	
Audit		6	

Office of the Comptroller of the Currency

Information Technology MRAs

CYBER/INFORMATION SECURITY
Internal Controls (Access Management, MDM, Patch Management, Incident Response, Firewall Rules, DLP)
Risk Assessment (Information Security Risk Assessment)
Third Party Management (Ongoing Oversight, Vendor Policy, Business Continuity, Audit)
Board and Management Oversight (Information Security Program, Patch Management/EOL)
MIS/Reporting (Information Security Program, Patch Management, Incident Response)

Office of the Comptroller of the Currency

Information Technology MRAs

BUSINESS CONTINUITY
Policy Development & Approval
Risk Assessment
Testing

IT OPERATIONS
Vendor Management
Board and Management Oversight

Office of the Comptroller of the Currency

Information Technology MRAs

VENDOR MANAGEMENT
Policy/Board and Management Oversight
Business Continuity
Audit
Initial & Ongoing Due Diligence

Office of the Comptroller of the Currency

Something to Review

FFIEC Joint Statement:

Cyber Insurance and Its Potential Role in Risk Management Programs

https://www.occ.treas.gov/news-issuances/bulletins/2018/bulletin-2018-8.html

Office of the Comptroller of the Currency

Resources

OCC Bank Information Technology Bulletins

https://www.occ.gov/topics/bank-operations/bit/issuances.html

FFIEC Cybersecurity Assessment Tool

https://www.ffiec.gov/cyberassessmenttool.htm

Verizon Data Breach Investigations Report

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

M-Trends 2018 by FireEye

https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

Office of the Comptroller of the Currency

Thanks for your attention

&

Enjoy the rest of the conference

Stephen Kunzinger

BIT Lead Expert Support

Stephen.Kunzinger@occ.treas.gov