Nonbank Supervision & Enforcement Update

Aligning Bank & Nonbank Cybersecurity Supervision

- CSBS IT Advisory Team
- InTREx and FFIEC IT Handbook Booklets
- Model Data Security Law
- Examination Tools
- Industry Tools
- Training Training Training

Cybersecurity Supervision

Model Data Security Law

- Based on FTC Safeguards Rule (with limited additions)
- Modeled largely on NYDFS rule and to meet most states' needs
- Adoption/implementation adds little additional regulatory burden in compliance

State Adoption Methods

- Full law adoption (states with existing laws likely do not need this model)
- Rule or Guidance

Optional Notice Requirements – You don't know what you don't know

- State Attorney General = 30
- State Regulator = 12
- Bank and Nonbank need is same

Cybersecurity Supervision

Nonbank Exam Workprogram (Baseline and Enhanced)

- Developed, Piloted, and issued Baseline Version 1.0 in August 2019
- NEW RELEASE: Roll-out in May 2022; public release in August 2022 (tentative)
    - 2 Versions: Baseline and Enhanced
    - Sorted according to URSIT components (Audit, Management, Support & Delivery, Dev and Acquisition)
    - Contains citations to FTC Safeguards Rule (where applicable)
- Baseline vs Enhanced
- Industry Use - Review (cyber planning and exam preparation)

Cybersecurity Supervision

Ransomware Self-Assessment Tool (R-SAT)

- Released in December 2020
    - Developed in conjunction with US Secret Service and Bankers Electronic Crimes Task Force (BECTF)
- Goals: Evaluates entity preparedness towards:
    - Identifying, protecting, detecting, responding, and recovering from a ransomware attack
    - Can also assist third parties (auditors, consultants, regulators) that might review security practices
- Periodic internal reevaluation of security practices relative to ransomware preparedness
- **UPDATE COMING**: CSBS is currently working with BECTF to review and update

Ransomware Awareness

- **Ransomware** presents a serious and growing threat to ***all businesses across all industries***
- Numerous notable ransomware incidents have garnered headlines recently
    - Many more occur that we never hear about
- Ransomware attacks occur across the globe every few seconds, every day of the year
- Businesses of all sizes are subject to attack
    - No longer the problem of big business alone
- Attacks have grown more sophisticated over time
    - Ransomware-as-a-Service (RaaS); multiplied capable bad actors and potential victims
- Has evolved from simple ransom demands to multiple extortion schemes
    - Attackers often threaten to release sensitive company or customer data on the Dark Web
- Costs associated with a ransomware attack vary widely but can be significant.
    - Can result in high reputation costs, legal costs, regulatory impacts, etc.

Cyber Hygiene

- PATCH, PATCH, PATCH!
- Know your data and systems, and who has access to them (including third-party access)
- Use of Multi-Factor Authentication (MFA); at a minimum, for:
  - All employees for administrative access
  - Accessing information stored in a cloud environment (outside of the firewall)
- Encrypt sensitive data
- Anti-virus/anti-malware software…update virus definitions regularly
- Develop basic procedures for reporting and reacting to incidents
  - What will we do when something happens? Who do we contact?
- Train all employees on basic cyber hygiene practices
  - Avoiding potentially malicious Internet links, phony emails (phishing), attachments
  - Weakest link (must be good custodians of data; train <u>often</u> to maintain awareness)
- Backups of critical data (periodically tested to ensure reliability)

FOR QUESTIONS OR ADDITIONAL INFORMATION, PLEASE CONTACT:

BRAD ROBINSON

SENIOR DIRECTOR, CYBERSECURITY POLICY AND SUPERVISION

brobinson@csbs.org

(205) 535-2220