Published on *The National Law Review* https://natlawreview.com

Top 10 Issues Facing Financial Institutions in 2017: #4 Cybersecurity

Article By:

Banks & Other Financial Institutions

Cybersecurity is emerging as one of the most significant and potentially dangerous risk areas facing financial institutions. As federal and state regulators continue to pepper financial institutions with new regulations, tools, and guidance, many institutions are struggling to create and maintain an effective cybersecurity risk management policy or program. To manage cybersecurity risk, companies must start by anticipating and preparing for the danger. There are two steps to this process: 1) conducting a cybersecurity risk assessment, and 2) creating a response plan to guide the institution through the aftermath of a cybersecurity breach or incident.

Step 1: Conduct Cybersecurity Risk Assessments

First, financial institutions should conduct ongoing security risk assessments. The assessments should be tailored to identify existing vulnerabilities and gaps in the institution's cybersecurity framework. To identify any vulnerabilities and gaps, the institution should have advisors familiar with new and evolving threats to customer accounts and the potential risk these threats pose to critical control systems.

A good tool available to financial institutions to perform this assessment is the Cybersecurity Assessment Tool (the Assessment), released by the Federal Financial Institutions Examination Council (the FFIEC), providing a repeatable and measurable process to inform management of the institution's cybersecurity preparedness. The Assessment consists of two parts: 1) identifying inherent risks faced by the institution, and 2) evaluating whether a company's cybersecurity preparedness is adequate and fully developed. While Part 1 focuses on external threats, vulnerability of delivery channels, and organizational characteristics, Part 2 focuses on the institution's current procedures related to cyber risk management, incident management, and oversight.

Step 2: Create a Response Plan

After a risk assessment is complete, a designated officer, such as a chief information security officer (CISO), should review the results and determine if the institution needs a response plan, or if its current infrastructure addresses the risk of a future cyber incident. Software systems, including intrusion detection controls and anti-virus and anti-malware protections, should be properly configured and up to date. The CISO and security team should also train employees on how to

prevent a digital breach.

Institutions must remain vigilant. No matter the strength of your institution's digital infrastructure, users can introduce threats by posting confidential information on social media or falling for phishing scams. Identity thieves like to go "phishing" for information by requesting sensitive information under false pretenses, such as pretending to be the Internal Revenue Service. Financial institutions should also remind their employees to avoid using insecure personal webmail and cloud storage and to change passwords frequently. Learning basic cyber hygiene and how to spot predatory email scams can help an institution avoid a cyberattack and protect consumer information.

Further, cybersecurity risk plans should be in writing and accessible to employees, vendors, and contractors. This written policy should include an incident response plan designed to promptly respond to, and recover from, any unauthorized access of customer information. The incident response plan should specify what actions the institution should take when the bank suspects that unauthorized individuals have gained access to customer information systems. For example, the plan might require filing Suspicious Activity Reports (SARs) and notifying the appropriate regulatory and law enforcement agencies. The written policy can also address data retention and destruction, frequency of testing, and vendor management.

New Regulations and Proposed Rules

In 2017, some financial regulators will make risk assessments and written cybersecurity policies mandatory for the institutions they oversee. The New York Department of Financial Services (the DFS) issued final regulations that became effective on March 1, 2017. The regulations require banks, insurance companies, and other financial services institutions regulated by the DFS to establish and maintain cybersecurity programs. Financial institutions have only a few months to comply: They must adopt a written cybersecurity policy by September 1, 2017, and conduct risk assessments by March 1, 2018. The final regulations mark the first of their kind in the cybersecurity space by any U.S. state or federal regulator, though other regulators appear to be following suit.

In October 2016, the Federal Deposit Insurance Corporation, the Federal Reserve System, and Office of the Comptroller of the Currency issued an advance notice of proposed rulemaking requesting comment on new cybersecurity regulations. The proposed rules would require banks with assets totaling more than $50 billion to develop a comprehensive cybersecurity strategy. Proposed regulations also include requiring companies to have written, board-approved cybersecurity strategies, protocols for secure storage of critical records, and audits to assess the institution's cybersecurity framework.

Top 10 Issues Facing Financial Institutions in 2017

Top 10 Issues Facing Financial Institutions in 2017: #1 Securities Compliance (for publicly traded and privately held banks)

Top 10 Issues Facing Financial Institution in 2017: #2 Mergers & Acquisitions

BSA/AML and OFAC Compliance: Top 10 Issues Facing Financial Institutions in 2017: #3

Top 10 Issues Facing Financial Institutions in 2017: #5 – FinTech

Top 10 Issues Facing Financial Institutions in 2017: #6 Third-Party (Vendor) Risk Management

Corporate Governance and the Culture of Compliance: Top 10 Issues Facing Financial Institutions in 2017 #7

Top 10 Issues Facing Financial Institutions: #8 – Capital Planning

#9: Customers' Nonpublic Personal Information Protection - Top 10 Issues Facing Financial Institutions in 2017

Top 10 Issues Facing Financial Institutions in 2017: #10 – Compliance with Consumer Laws

National Law Review, Volume VII, Number 79