Impending Regulatory Changes for Cybersecurity

cyber security regulatory leadership

Summary: As regulators step up their oversight of cybersecurity and prepare to impose new regulations, CFIs need to review their cybersecurity programs and plug any gaps accordingly. Regulatory proposals provide the perfect guide for where CFIs should focus their efforts.

Aretha Franklin's song "Respect" is one of the most recognizable songs of all time, so much so that it was ranked number one on Rolling Stone's 2021 list of "The 500 Greatest Songs of All Time" — 54Ys after Franklin first sang it. Yet, Franklin wasn't actually the song's original singer. Otis Redding first sang and recorded "Respect" on his third studio album in 1965. But while his rendition of the song made it to the top five on Billboard magazine's Black Singles Chart, it never got beyond number 35 on the pop radio charts.

Aretha Franklin's success with a reworked version of "Respect" is just one of countless examples of artists who scored mega hits by reinventing other artists' songs. Building on the work of others doesn't stop within the music world, either. With varying regulators working on their own interpretations of the rules that should govern financial institutions' cybersecurity efforts, community financial institutions (CFIs) should be aware of proposed changes from some of the highest profile regulators, whose directives may be mimicked over time.

Change at the Top

The New York Department of Financial Services (NYDFS) released Proposed Amendments in November of 2022 for cybersecurity regulation that would require the implementation of specific administrative and technical controls and regulate corporate behavior by mandating certain cybersecurity governance practices. The Securities and Exchange Commission (SEC) is also proposing requirements that would mandate greater transparency for organizations' cybersecurity programs, including the board's role in overseeing and managing cybersecurity strategies, policies, and procedures.

Not only are regulators looking to see stepped-up cybersecurity efforts within an organization's technology department, but they also want to ensure that digital security practices are heightened throughout an entire establishment. Ensuring board member involvement and accountability increases the likelihood that organizations will devote adequate resources to cybersecurity efforts and enact better practices throughout their entire operations.

Top of the Radar

In an attempt to stay ahead of the regulatory curve, CFIs should ready themselves for enhanced oversight and requirements regarding their cybersecurity initiatives.

The following are some of regulators' key concerns that CFIs should look at within their own organizations, and where they should prepare for greater oversight:

- **Increased controls.** Since phishing emails, unpatched software, and faulty remote desktop protocols (RDP) are the most common ways that criminals breach a company's cybersecurity, the NYDFS would

require organizations to put mandatory practices and controls in place to protect these vulnerabilities. On top of monitoring these areas, company-wide cybersecurity training would also be a requirement.

- **Access requirements and privileges.** To prevent unauthorized system access, another focus area will involve implementing stronger remote access requirements and policies. Greater oversight of high-level accounts also ranks high among the NYDFS' concerns. As such, the regulators want to see the following standards enacted:
  - Stronger limits surrounding the number of people with high-level access.
  - A better match between the access granted to employees and the needs of their role.
  - Annual reviews of user access privileges and purging of unnecessary access.
  - Multifactor authentication.

- **Backup recovery plans.** Ensuring business continuity is also a major concern of regulators. The NYDFS would require organizations to make backup recovery plans for ransomware attacks in their emergency response plans. Specific measures would include regulator tests to ensure the ability to restore operating systems from backups and annual penetration tests performed by qualified third parties, among others.
- **Cybersecurity event notification.** Heightened transparency among financial institutions is another area where the NYDFS is focusing. The regulator would require organizations to notify it, and other officials, within 24 hours of making any sort of ransomware payment. Then, within 30 days of any such incident, organizations would need to provide a written explanation detailing why the payments were made, any alternatives considered, and the due diligence involved in assessing the actions taken.
- **Greater board accountability.** This is a major concern of both the NYDFS and the SEC. In the case of the NYDFS, additional requirements would include annual board approval for written cybersecurity procedures and policies, to receive regular reports, and to receive documentation regarding any concerns found in penetration or vulnerability testing. Board members would also need to demonstrate a sufficient level of cybersecurity expertise, as well as take part in periodic testing. The SEC's requirements would require boards to disclose the following:
  - The cybersecurity expertise of board members.
  - Board oversight of digital risks and management's role in assessing risks and implementing cybersecurity strategies, policies, and procedures.
  - Regular cybersecurity discussions with management, which would include creating a simplified way of discussing complex cybersecurity risk and resilience issues that can make an organization's vulnerabilities clear to all board members.

While cybersecurity is already a major focus area within the banking industry, CFIs would be wise to take a close look at the areas where regulators may increase oversight. By putting their own efforts on these fronts under the microscope, CFIs can be prepared well ahead of time to ensure their cybersecurity programs meet any new regulation standards.

YOUR TRUSTED PARTNER FROM COAST TO COAST

PCBB provides high-quality, competitively-priced solutions with personalized service. Designed to help community financial institutions thrive, our services include: cash management, international banking, lending, and advisory services. Contact us to learn more.

ECONOMY & RATES

Rates As Of: 04/05/2023 12:22PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg

3M	4.88	0.03	0.46
6M	4.80	-0.14	0.04
1Y	4.41	-0.19	-0.30
2Y	3.78	-0.24	-0.65
5Y	3.36	-0.22	-0.65
10Y	3.30	-0.18	-0.58
30Y	3.56	-0.09	-0.41

FF Market	**FF Disc**	**IORB**
4.83	5.00	4.90

SOFR	**Prime**	**OBFR**
4.83	8.00	4.82