Banks and financial services firms continue to grapple with regulators’ growing demands to better manage cyber risks created by third-party vendors, but they should not focus solely on compliance, according to a panel of former regulators and cyber experts.

Viewing third-party risk within a wider risk management framework would lead to greater security maturity, agreed the banking, legal, and cyber experts, who participated in a December 2017 webinar hosted by the Independent Community Bankers of America® (ICBA) and CyberFortis™, a cybersecurity solution service provider for the financial sector.

The panel included a former state banking commissioner, a former regulator who helped create the recently-implemented New York DFS cyber regulations, and a nationally known legal expert who works on cybersecurity cases, including those involving the Securities and Exchange Commission (SEC).

Although headlines tend to be dominated by cyberattacks on large banks or financial firms, organizations of any size are at risk, said panelist David Cotney, former Massachusetts Banking Commissioner and advisor to CyberFortis™.

He said he hears daily reports of hackers attacking the defenses of banks both large and small, including looking for easy entry points such as third parties connected to banks’ systems.

These known vulnerabilities have forced federal regulators, including the Office of the Comptroller of the Currency (OCC), to require financial institutions to have a strong vendor risk management system. This includes establishing risk tolerance, ongoing monitoring, and independent reviews. There is also an expectation that boards will be actively involved throughout the vendor risk management process.

Cotney issued a warning about compliance versus security, noting that some regulators have expressed private concerns that too many bankers think simply meeting the baseline expectation under the FFIEC’s Cybersecurity Assessment Tool (CAT) is sufficient.

“Threats evolve and a bank’s environment is not static. They are changing their products and services, they are hiring and terminating employees, and their networks and IT environments are also undergoing changes and updates,” said Cotney.

“Instead of thinking of the CAT as a ‘check the box annual exercise,’ use it to reexamine your inherent risk profile and maturity level prior to introducing new products, services, or initiatives, which includes new third-party connections or mergers and acquisitions,” he suggested.

To secure the assets of both a bank and its customers, it is necessary to move from a baseline approach (compliance-driven) to a higher maturity level approach (enterprise risk), which Cotney said is something regulators are specifically looking for in a bank’s security program.

NY DFS REGS INFLUENCE OTHERS

The panel also addressed how the New York Department of Financial Services (NY DFS) regulation can be viewed as a bellwether for how all regulators are viewing cybersecurity risks and more specifically, third-party cybersecurity issues. “Must we be our brother’s keeper?” asked Alexander Sand, now an associate at Eversheds Sutherland and a former NY DFS regulator who helped create the new requirements. “To the extent that third parties are touching your network and holding your data, then yes,” he answered.
Because regulators want to see that financial institutions are making their decisions based on risk, having a risk assessment performed is crucial and will help with meeting strict NY DFS deadlines.

There are both internal and external risk assessments involved, said Sand. “Internally, what are the risks to the bank’s ability to operate if a significant operational vendor goes down, and externally, what are the risks of third party security practices?”

**Although the Third-Party Service Provider Security Policy deadline is March 1, 2019, Sand said NY DFS expects this to be a large undertaking that organizations will need to begin addressing immediately.**

The requirements are robust and include written policies and procedures based on the risk assessment that address:

- Identifying and assessing the risks of third-party service providers
- Setting out minimum cyber practices banks require
- Establishing due diligence processes
- Performing periodic assessments of the risks of third-party service providers

While this regulation does not require specific controls to be put in place for all vendors, Sand said it does emphasize certain controls that NY DFS wants organizations to consider, such as multi-factor authentication, encryption of data in transit and at rest, vendor breach notifications, and confirmation of vendor’s cybersecurity practices.

“At the end of the day what will be better for your customers and your bank is to be proactive and thoughtful so that you’re meeting your organizations’ specific risks rather than pulling something off the shelf.”

**START BY SETTING PRIORITIES & POLICY**

“Banks will say to me, ‘I have 120 vendors. How can I get my arms around this?’” noted Jack Hewitt, Partner at Pastore and Dailey, LLP. He recommended that banks identify all vendors and prioritize by importance. Then look at the auditor reports and reports of breaches.

But even before tackling that, Hewitt said it’s first necessary to create – or update – your vendor management policy, adding that harmonization is essential. “I recommend you blend together procedures based on the applicable regs from the relevant authorities such as the NY DFS, OCC, SEC, and FINRA. Your policy statement should provide vendors with appropriate guidance to ensure the bank’s security.”

**An organization’s vendor risk management program should be matched by that of their vendors’. This ensures that any connected systems are taking the same security measures that you are, helping mitigate risk and shoring up inherent vulnerabilities.**

The vendor management policy and its purpose should be communicated to both staff and vendors so that all involved parties are on the same page, said Hewitt, who also echoed Sand’s thoughts regarding the importance of a risk assessment.

This analysis will identify and provide insight into what elements of risk exist, which often includes threats stemming from existing vendors.

“Give yourself plenty of time to deal with this third-party issue,” Sand concluded.
Hewitt outlined a series of specific steps banks should take (available here), including recommendations on how to craft robust contracts, what detailed procedures vendors should be required to have, the management oversight and continuous monitoring practices every vendor program should include, and what types of records should be maintained.

“Many banks are beginning to use new technologies such as robo-advisors, artificial intelligence, and blockchain, which all involve third-party vendors,” said Hewitt. “Before you begin to engage actively with a vendor in these areas, complete your assessment ahead of time, have management controls in place, and be able to analyze on a continuous basis or it could compound problems in the event you do have an intrusion.”

The panelists concluded with a caution that regulators recognize the burdens on financial institutions, but will take action when they deem that an organization has actively chosen not to comply with regulations or improve its security posture.

They also agreed that while banks’ actions are often driven by compliance, achieving more mature security and the resilience it generates will require banks to look beyond checking the box.

CyberFortis™ provides specialized cybersecurity solutions to the financial sector, including enterprise security assessments, third-party cyber risk management, and managed security services. CyberFortis™ is a subsidiary of TSC Advantage, an enterprise security firm with more than a decade of experience protecting the sensitive information and business-critical assets of the federal government and Fortune 500 companies. For more information, contact David Cotney at 617-429-1755.