ThinkAdvisor

Fintech, Cybersecurity Among Key Risks to Banks: OCC

By Danielle Andrus JULY 14, 2017 1

Technology intensifies the strategic and operational risks to banks, according to a report

The Office of the Comptroller of the Currency recently issued its Semiannual Risk Perspective for Spring 2017, identifying areas where technology is increasing the strategic and operational risks the banking industry faces.

Increased competition from fintech firms and consumer demand for new products have increased the strategic risks banks face, according to the report.

For example, alternative payments tools that are less transparent increase the risk of money laundering schemes going undetected. In addition to having to address compliance risks associated with new technology, some banks are struggling just to keep up with the technology.

“Risks related to changes in technologies and typologies are often cumulative, requiring banks to enhance processes to address these risks while maintaining existing controls,” according to the report.

OCC also named cybersecurity as a key risk for banks of all sizes. “Cybersecurity and fraud continue to pose risk from the increasing volume and sophistication of cyber threats and IT vulnerabilities,” the report said of large banks, while noting that it’s increasingly important for midsize and community banks to develop “cyber resiliency” as malware and extortion schemes become more complex and these banks are more likely to rely on third parties for cyber protection.

(Related: Targeting US, Mobile Ransomware Follows the Money: Kaspersky)

In fact, OCC warned that more banks are outsourcing their cybersecurity function to a small number of providers. Risk is getting more concentrated, especially around specialized functions like card processing or denial-of-service mitigation, creating “concentrated points of failure for certain lines of business or operational functions for a large segment of the banking industry.”

The speed at which cyber incidents occur, as well as their sophistication, are increasing, according to the report. Furthermore, cybercriminals are more willing to act aggressively with the information they extract.

The cybercriminals themselves are changing their business model as hackers start selling ransomware as a service, the report noted.

Phishing is the primary means of access for hackers, the report found, though ransomware and denial-of-service attacks are also among the threats banks face.

“Effective risk management promotes timely detection, response and escalation of operational issues to reduce customer impact due to product failures, possible fraud and potential unfair or deceptive acts or practices,” Keith Noreika, acting comptroller, said in remarks published with the report.

The report stressed the role of culture in combating this threat. “Sophisticated cyber threats continue to pose high inherent risks to an interconnected financial services marketplace. Boards and management play a critical role in establishing a sound culture and implementing effective resiliency practices,” according to OCC.

A report from Kaspersky Lab and B2B International found that half of IT security incidents are caused by employees within a firm, and 40% of employees hide their role in an incident for fear of retribution.

OCC recommended updating software and hardware frequently to stay on top of evolving cyber threats, and using strong authentication protocols as "part of a layered security approach." OCC noted, "A sound systems development life cycle including regular maintenance is essential to protecting against these weaknesses."

Brian Clark, CEO of Ascent Technologies, expressed concern that OCC appears to be analyzing firms' strategic risks rather than setting "clear rules that banks and institutions can follow."

"What they've essentially done is create a standard of strict liability. That's a legal term [that means] regardless of the outcome, you are liable," Clark said. "Whether or not that is the right standard, it is concerning because it establishes the potential boundary through an administrative process rather than a legislative process."

He added that while OCC "should be aware of capital risk, liquidity risk and prudential style overview — that's their purpose … starting to push into strategic implications of the firm is the purview of the business."

Clark recommended banks make sure they understand the capabilities and shortcomings of the technology they use. "No technology will solve every single one of your problems. Some will solve more than others. But really understanding what you're implementing is key."

It's also important for banks to understand where data is coming from and where their technology integrates with their providers'. "I'm sure there are cybersecurity services out there that will help analyze these touchpoints, but even more than that, understanding the data you are utilizing in your analysis and where it comes from, and how that integrates with third-party algorithms or services offered and their data, is going to be key," Clark said.

--- Read Cybersecurity Requires a Collaborative Approach on ThinkAdvisor.