GODFREY & KAHN S.C.

November 2020

Bank Strategy Briefing

Ideas and analysis for community bank executives

Four data security tips for community banks

Andrew F. Spillane

414.287.9351

aspillane@gklaw.com

Banks across the asset-size spectrum have increasingly transitioned product delivery to remote channels during the 2019 novel coronavirus (COVID-19) pandemic. These channels, while presenting new opportunities to serve communities in unprecedented times, create greater reliance on technology, increasing exposure to malicious cyberattacks and other security breaches.

Often, a large component of a community bank's IT infrastructure is outsourced as smaller banks often do not have the internal IT resources to implement an enterprise-wide security effort. Attackers know this and may target smaller institutions on the assumption that they have more vulnerabilities than large banks.

That said, by taking the following key steps you can help fortify your bank's resiliency to cybersecurity threats:

1. **Utilize the FFIEC cybersecurity assessment tool**: Information security risk assessments are nothing new. In fact, they are a regulatory expectation. The agencies have recently emphasized the importance of the FFIEC CAT, with its previously voluntary nature of the FFIEC CAT evolving into a requirement that institutions meet its maturity levels. Beyond the compliance angle, the FFIEC CAT's detail can assist institutions by identifying key risk points and methods to mitigate them. These risk assessments should be revisited whenever key personnel, products or systems change.

2. **Train your employees and customers to identify threats**: Malicious attacks garner the most public intrigue, but a solid majority of data compromises tie back to end user error. An employee may click a link on a legitimate looking email. A banker may provide personally identifying information or even execute a transaction for a pretext caller. Sensitive information may be stored on personal computers while working remotely, which may not have the protections of a business's network. A customer may share log-in or account data with a relative or employee who conducts unauthorized transactions. In these cases, training can go a long way to educate end users on protecting sensitive information. After all, bank management may be responsible for responding to the fallout if an incident does occur.

3. **Exercise oversight with your vendors**: Because outside providers play an outsize role in a community bank's software architecture, vendor management becomes central to an information security program. Management should resist the temptation to see the inclusion of certain security-related RFP questions and contractual provisions as a "check the box" compliance exercise. Weak points of a third party's information security program can be identified in due diligence, and properly negotiated confidentiality provisions can ensure that vendors will cooperate with your security needs and share in losses that occur.

4. **Engage independent third parties to perform security audits**: Without internal resources, the next best option is to bring in cybersecurity expertise from the outside. Consultants, audit firms and legal counsel can conduct social engineering exercises to gauge end user risk and tabletop exercises to determine how a bank will respond to an incident. These professionals bring an industry-wide perspective and can advise on the risk environment they regularly encounter.