Nutter uncommon law

INSIGHTS
JANUARY 2018

"Your preparation for a cyber attack should be modeled after how you plan for a natural disaster...All companies need to plan for how they will respond to a breach and must regularly test that plan through realistic simulations."

How Community Banks Can Overcome Cybersecurity Paralysis

Q: WHY SHOULD COMMUNITY BANKS PRIORITIZE CYBERSECURITY?

A: A data breach at a bank could have a significant impact on the solvency of an institution and confidence in the larger financial system. Of course, not all cyber crime is new. Community banks should be wary of old fashioned fraud that is Internet-enabled, such as being spoofed by wire transfer requests or attacked by ransomware, which can shut down operations.

Community banks are particularly vulnerable to certain types of attacks because of their emphasis on individual customer service. However, community banks must not let this customer-friendly attitude blind them to the importance of appropriate internal controls to avoid falling victim to fraud.

It is important to point out that community banks are not the only banks at risk from cyber attack and are better prepared for cyber attacks than most other types of businesses. Federal agencies regularly evaluate all banks, including community banks, with a cybersecurity assessment tool as part of their IT examination programs. A similar level of oversight is applied to banks' core processors.

Q: WHAT PREVENTATIVE STEPS CAN COMMUNITY BANKS TAKE AGAINST CYBER ATTACKS?

A: Your preparation for a cyber attack should be modeled after how you plan for a natural disaster. As with natural disasters, cyber attacks cannot always be prevented. Thus, all companies need to plan for how they will respond to a breach and must regularly test that plan through realistic simulations. Do not overlook the basics, such as patch management of known vulnerabilities.

It is important to encourage an employee culture of cyber awareness – cybersecurity is not a problem that can be solved through technical measures alone; it requires all employees to be educated, vigilant, and prepared.

Finally, to safeguard against ransomware and other threats to business resumption, keep back-up files to that you will not become hostage to demands. Banks also may participate in industry sponsored programs such as **Sheltered Harbor.**

Q: IF A COMMUNITY BANK DOES EXPERIENCE A CYBER ATTACK, WHAT NEXT?

A: Business resumption and recovery requirements are the first priority, meaning that a cyber attack must be investigated and responded to as soon as it is discovered. Banks should also promptly share information about the nature of a cyber attack with the industry and regulators through communication channels like **FS-ISAC.**

As soon as you suspect a successful attack, you should engage outside counsel to oversee the investigation. The outside counsel will then engage a cyber incident response firm to allow for privileged communications about the investigation, and if need be can assist in preparing for litigation. Indeed, it is best practice to engage outside counsel before a breach even occurs, so that they can help shape and review your incident response plan.

Once a breach is confirmed, communicating with your business and retail customers becomes paramount. If data containing Personal Identifiable Information (PII) has been improperly accessed, federal and state breach notification requirements may be triggered.

Public announcements about breaches can be a minefield. You need to be able to describe for customers what happened, how you are going to fix it, and what affected consumers can do, which can be challenging before you have completed the investigation. On the other hand, you don't want to wait so long to notify customers that you are perceived to be evading responsibility. It is important to prepare for such contingencies now and to think through how your statements will be perceived. Finally, equip your customer-facing representatives with talking points so that they can relay accurate information and provide answers to concerned consumers.

Thomas J. Curry

PARTNER
617.439.2087
tcurry@nutter.com

Thomas J. Curry is a partner in Nutter's Corporate and Transactions Department and a co-leader of the Banking and Financial Services group. Previously, he served as the U.S. Comptroller of the Currency until May 2017.

Seth P. Berman

PARTNER
617.439.2338
sberman@nutter.com

Seth P. Berman leads Nutter's Privacy and Data Security practice group. He advises clients on the legal, technical and strategic aspects of data privacy and cybersecurity risk, and to prepare for and respond to data breaches, hacking and other cyber attacks.

PRESS CONTACT:
Heather Merton
Senior Communications Manager
617.439.2166
hmerton@nutter.com