

Community Banks and Protecting Against Cyber Criminals



By their very nature, banks are an attractive target for cyber criminals because of the assets they hold and the personal information of customers that they keep. Due to the evolving threats and uncertainty in today's cyber landscape, it is vital for banks to take the necessary steps to guard against vulnerabilities and exposures, and to protect themselves from malicious attacks that can cause serious harm. A single breach can result in significant losses, and the damage is often not limited to lost data. It can extend to loss of customer confidence, financial harm, legal challenges and business interruption.

Much like cyber threats such as ransomware, social engineering and phishing, cyber security has also evolved. Many insurance companies, including Travelers, offer risk management services that feature pre-breach cybersecurity expertise. These services go a long way toward strengthening

the systems that banks use to keep cyber criminals at bay. In the event of a cyber attack, post-breach assistance kicks in, provided a bank has secured appropriate insurance coverage.

Over the past few years, banks have increased their focus on preparing for a cyber incident - in other words, recognizing that when it comes to a network compromise, "it's not if, it's when," even for a well-defended network. Banks are doing a better job of updating their incident response plans, business continuity plans, and disaster recovery plans, at least every one or two years, and they are conducting periodic tabletop exercises to make sure that the right people respond when an incident does occur. Staying up-to-date on cyber insurance coverage is another important part of being prepared.

The tough thing about cyber security is that defenders have to be vigilant at all times, while attackers only have to get through the defense once to create havoc. For that reason, it's important to have well-designed change control procedures in place to ensure that changes to network configurations and controls do not inadvertently introduce security vulnerabilities. Many network compromises can be traced back to change control procedures that either did not exist or were not properly followed. Implementing - and diligently following - established change control procedures can help prevent the mistakes that may lead to a data breach.

How can banks best prepare for a potential cyber incident? There are many "best practices" for cyber security, but let's highlight one that is particularly valuable for preventing complacency. Banks - all industries, really - should rotate their cyber-security assessment and testing providers. If the same team is used for penetration testing year after year, they will likely find the same kinds of vulnerabilities year after year. Sometimes a new set of eyes can be beneficial. If a rotating group of trusted cyber-security assessment and testing providers consistently reports that a bank's networks and systems are clean, the bank can feel more confident that nothing important has been overlooked.

Being proactive is key - educating employees and putting proper risk management systems in place should be a high priority. Banks should work with an independent insurance agent to identify coverage to manage potential cyber exposures and ensure that employees are exhibiting behaviors that limit cyber risks. Finally, banks should utilize resources such as Travelers.com/cyber to help understand and navigate the growing threat of cyber risks.

A specimen policy is located in "Product Resources" on www.bigimarkets.com.

Travelers SelectOne®, underwritten by Travelers Casualty and Surety Company of America, is endorsed by the Independent Community Bankers of America. To find your local community bank, visit ICBA's community bank locator at www.icba.org/locate. Simply type in your zip code and the app will show you all the community banks in your area.



www.bigimarkets.com

[Forget Password?](#)

[BIM Help Desk](#)

[TFT Archives](#)

Travelers is committed to managing and mitigating cyber risk, and does so backed by financial stability and a dedicated team - from underwriters to claim professionals - whose mission is to insure and protect a company's assets. For more information, visit www.travelers.com/cyber.

The product and eligibility may have been revised or discontinued since the original article was written. Review the Information page for each product on Big "I" Markets for current content and instructions.