Cybersecurity Trends In 2020

cyber security risk management

Summary: In a recent survey, 96% of community bank CEOs named cybersecurity risk as a top concern. With this in mind, we highlight the cybersecurity trends for 2020.

It has been said that 80% of the jobs we will be doing in 2040 aren't even around today. That is just crazy when you think about it, as is the growing role of artificial intelligence (AI) in hiring for these types of jobs. Technology has many benefits to be sure, but the incredible boom is also causing cybersecurity problems.

Not surprisingly, a recent survey finds an overwhelming number of community bank CEOs (96%) cited cybersecurity risk as a very important or important risk factor to their bank. Given this being top of mind for so many execs, here are three cybersecurity trends to be aware of for 2020.

Pay attention to mobile app and web-based security risks. As cash usage is diminishing, there are an increasing number of customers turning to mobile and web-based applications. This shift is only likely to accelerate, giving community financial institutions (CFIs) ample incentive to vigorously protect applications from cyber-thieves. Consider a 2018 Accenture study that found at least one known security risk in all 30 banking apps it examined. CFIs need to be careful not to get behind the eight-ball here, especially as you continue to unlock your institution to third parties through open banking initiatives. The security of your online and mobile channels will be even more critical for customer data protection.

Watch those third parties. We're all for collaboration, but banking regulators have made it abundantly clear that CFIs cannot outsource their responsibility and accountability for outsourced services. A good course of action is to proactively ensure your management of third-party vendors is tip-top, and that you are taking an active role in due diligence and engaging in ongoing monitoring, among other best practices. If you are lax with third-party management, you could find yourself in regulatory hot water, not to mention the adverse impact on your customers.

Beware of targeted ransomware. Symantec says ransomware groups are all around you and more have emerged in the past few years. They warn that means more organizations are being hit with attacks. Still other cybersecurity players expect criminals to focus on institutions because they have deeper pockets to make payments and may also threaten to publish sensitive corporate data that has been stolen. Still another approach that one criminal ring has tried is publicly naming on a website the businesses that refused to concede to demands, according to Krebs on Security.

No matter what, be sure not to make the mistake of thinking your institution is immune from risk. Certainly, cyber-criminals have been known to target institutions when they find cyber-defenses that are less robust than at other institutions. So, make sure you use cybersecurity tools such as those available on the Financial Crimes Enforcement Network (FinCEN) site as you stay up to date on the latest threats.

WHITE PAPER: TRANSITIONING TO SOFR

Bankers have heard that SOFR will replace LIBOR as a benchmark in 2021. But, what is involved in this transition? To learn more about the impact and how your institution can plan for it, download our white paper,

"Moving from LIBOR to SOFR: Smoothing the Transition for your Financial Institution" now.