Vol 4. Issue 3 | 2018

PCM

Your gateway to the world of payments

ATLANTA SPECIAL: THE ATLANTA FINTECH ECOSYSTEM

THE BITE OF BREACHES AND THE OVERCONFIDENCE TRAP

Community Banks and Credit Unions

By Sean Feeney, Chief Executive Officer, DefenseStorm

Astronaut Neil Armstrong knew a thing or two about managing risk. In speeches he gave after retiring, he frequently cautioned against overconfidence. He said of his career at NASA and of his journey to becoming the first man to walk on the moon, "We tried very hard not to be overconfident, because when you get overconfident, that's when something snaps up and bites you."

When it comes to cyber threats, community banks and credit unions would be well served to heed Armstrong's advice. Despite hard facts to the contrary, too often community financial institutions reason that they are "fine" and don't need more than a minimal investment in cybersecurity or cybercompliance. While rationales vary, overconfidence is typically at the root.

Some believe they aren't large enough to be a target for bad actors, or that they are protected because they haven't yet experienced a breach (at least one of which they are aware – research firm Gartner has noted generous time lags between when a breech occurs and when its impact is detected). Bank CEOs and Boards of Directors are held accountable for cybersecurity and cybercompliance practices, yet still might deny funding requests despite alarming data. Cyber breaches (not simply attacks) were up nearly 50 percent in 2017, and the number of U.S. enterprises reporting in 2018 at least one breach "in the past year" nearly doubled to 46 percent, while a whopping 71 percent reported at least one breach "over the past few years." Cybersecurity has been cited as a top focus for federal bank regulators, and experts project a global shortage of two million cybersecurity professionals by 2019. In fact, 70% of cybersecurity professionals in 2017 reported their organizations have a cybersecurity skills shortage. In the face of such "pay attention" data, it's a wonder this level of overconfidence exists.

However, progressive community financial institutions are paying attention and are realizing that when it comes cybersecurity, like many things in life, the best time to deal with a disaster is before it happens.

C-Level Insight

One such forward-thinking community bank leader is Ron Quinn, president and CEO of Peach State Bank in Gainesville, Georgia. Information shared at an FDIC-sponsored cybersecurity conference inspired Quinn to launch an initiative to optimize the bank's cybersecurity and cybercompliance capabilities.

Quinn tasked Charles W. Blair, the bank's CFO, with spearheading the effort. Peach State Bank ultimately decided to partner with DefenseStorm, a banking-focused cybersecurity and cybercompliance company, for the technology, policy and people

support the bank identified as important to achieving its objectives. Blair commented, "(Our decision) was a direct reaction to hearing from the regulators about what they were going to be requiring banks to do," Blair says.

While Peach State already had firewall and server traffic monitoring in place, the bank lacked an all-encompassing view of its network. They also lacked enough in-house cybersecurity experts to sort through, prioritize and act on the volumes of information the monitoring company was sending them with little or no explanation, leaving the IT staff overwhelmed and in a quandary as to what actions to take. Often, that meant calling to place a support ticket with the monitoring firm, hoping somebody would call back quickly.

Finding the Right Fit

Steven Pettit, an assistant vice president with day-to-day responsibility for Peach State's cybersecurity program, appreciated Quinn's commitment to strengthening the bank's capabilities using resources tailored to banking needs. "Our previous provider couldn't separate routine, run-of-the-mill information from critical threat detection," Pettit noted. "We couldn't limit alerts we received to only those we cared about. I don't really care about seeing alerts on port scans, unless someone is actually able to penetrate the firewall," he explained.

Upon deploying the DefenseStorm GRID for cybersecurity and cybercompliance, Peach State Bank was able to expand coverage beyond its servers and firewalls to its entire network, plus take advantage of the additional resource power provided by DefenseStorm's TRAC (Threat Ready Active Compliance) Team of cyber professionals. Now Pettit's team works in tandem with TRAC, seeing the same intuitive command center screens tailored to Peach State Bank's needs. DefenseStorm's TRAC Team also delivers actionable recommendations and insights to help prioritize alert handling.

Pettit's team also can configure alerts based on factors they care most about. One example is alerting the team when calls are forwarded, a proactive measure to prevent cybercriminals from hijacking the bank's telephone system in order to redirect customer calls and steal information obtained during them.

Other advantages came from additional vulnerability testing and having a third-party view of the bank's environment. "DefenseStorm did vulnerability testing to become familiar with our environment and to get an initial assessment of any holes," Pettit said. Immediately upon going live, the DefenseStorm TRAC Team noticed several of the bank's devices were communicating with what appeared to be a rogue router in Texas. After the device was flagged as unapproved, the bank realized it had inadvertently omitted the asset from its list of approved devices, when in fact it was part of the bank's infrastructure. "Having an extended team working with us to make sure everything is in order from both a cybersecurity and cybercompliance standpoint is a tremendous benefit," Pettit said.

Defenses to Consider

Staying one step ahead of "bad actors" can seem daunting to community financial institutions, given the increasing complexity and frequency of attacks and the meaningful shortfall in cybersecurity professionals. When considering options, the following recommendations can help shape the right course of action.

1. Beware the Overconfidence Trap. It can be tempting to believe your institution isn't at risk. However, all data suggests that you are, and that the risk is escalating. Rather than hoping for the best, cyber aware leaders take note of John Chambers' observation when he was CEO of Cisco: "There are only two types of organizations: Those that have been hacked and those who don't know they've been hacked."

2. Make your C-level executives aware of risks and regulations. Information shared at an FDIC conference inspired Ron Quinn and Charles Blair of Peach State Bank to re-examine and refine the bank's cybersecurity strategy. That same data can help you secure funding for better initiatives at your bank or credit union. Financial institution executives and Boards of Directors are coming under increasing pressure to be more meaningfully engaged in, and accountable for, cybersecurity and cybercompliance effectiveness, regardless of an institution's size.

3. Find a way to link cybersecurity and cybercompliance. With cybersecurity named a top priority for regulators, proving your financial institution is compliant with bank and credit union cybersecurity regulations and guidelines is paramount. Many tools are built for cross-industry cybersecurity, but don't map your cybersecurity activities directly with regulatory elements outlined in the Federal Financial Institution Examination Council's

Cybersecurity Assessment Tool (the FFIEC-CAT) nor the National Credit Union Association's Automated Cybersecurity Examination Tool (the NCUA ACET). A solution built specifically for banking does that mapping for you, so you can easily prove complaince with what regulators recommend.

4. Cover everything. Some solutions are based on systems covered, data volume ingested, or both. Institutions might try to save on costs by leaving some systems uncovered, which invites vulnerabilities, or by limiting data history, which can make investigating incidents more difficult. Providers that have a predictable and affordable cost model for covering everything can be an advantage. Cloud-based solutions generally offer more capacity and flexibility than on-premise tools at a better price, especially when the cost of in-house resources to configure and manage the tool are factored into the investment.

5. Understand you need more than a tool. Analyst firm Gartner has noted that "Securing information has become less about having firewalls and policies, and more about complex interactions among people, machines and processes." Achieving cyber Safety & Soundness requires technology, but also people, processes, policy and, if possible, a community of peers to offer insights. Many institutions mistakenly believe investing in a Security Information and Event Management (SIEM) tool is sufficient, only to find their teams drowning in an onslaught of alerts that go uninvestigated because of resource constraints. Or, they might choose to outsource everything to a Managed Security Service Provider (MSSP), only to find, as Peach State Bank did, that they lose visibility and control over their security posture. Choosing a comanaged model, which has your team and a supplemental team of outside resources using the same system together to analyze, prioritize and investigate issues, gives you added bandwidth and expertise without sacrificing visibility and control. It also enables you to set the ground rules and priorities based on your institution's needs and goals.

Community financial institutions are just as vulnerable as large money centers are to cyber attacks, and increased regulatory pressure applies to all. Avoiding an overconfident "we're fine" viewpoint and examining best-in-class options for achieving cyber Safety & Soundness is advisable for all bank and credit union executives, as well as Boards of Directors and IT oversight committees. Many options are available to make modern protection, as well as improved compliance, available to even the smallest institutions. ●

SEAN FEENEY

Chief Executive Officer at DefenseStorm

Sean Feeney is DefenseStorm's CEO and a 30-year technology leadership veteran who has shaped strategic direction and high-growth performance for a variety of technology companies. In previous CEO roles he executed successful exit transactions for cloud-based supply chain management provider GT Nexus (acquired by Infor) and for business-to-business e-commerce pioneer Inovis (acquired by GXS, now OpenText), together valued at more than $1 billion.

DefenseStorm®

DEFENSESTORM

DefenseStorm is the only company that combines and automates in real time cybersecurity and cybercompliance built for banking, so financial institutions can achieve Cyber Safety & Soundness according to regulations and their own policies. The DefenseStorm GRID™ is the only co-managed, cloud-based and compliance-automated solution of its kind, operating as a technology system and as a service supported by experts in financial institution security and compliance.