Texas Security Banks increases cybersecurity precautions

By Catherine Leffert – Staff Writer, Dallas Business Journal
3 minutes ago

Texas Security Bank has spent the past 18 months revamping its cybersecurity system as phishing attacks and network breaches pose a continued threat in efforts.

Since it began making changes, the Dallas-based bank's leaders estimate it has added 25 percent more cost for its networking system related to cybersecurity alone, in hardware, third-party vendors and an extra information technology employee.

"At a financial institution, cybersecurity is one of the most important things in a bank," said Scott Hester, information technology director. "We've got to keep the bank secure, we've got to keep our customers secure. Really day-to-day, it's one of my main focuses...Because it really does just take one event to have a huge impact."

Founded in 2008, advancing the bank's technological capabilities was a relatively recent priority to prepare for a potential disaster situation, which the COVID-19 pandemic proved necessary, Hester said. He said as much as it could be, the bank was prepared when it had 80 percent of its workforce working from home during the lockdown.

Though Texas Security Bank isn't alone in increasing investments in cybersecurity, Hester added Texas Security Bank invests more in cybersecurity than most other banks of its size. There are certain marks that banks need to meet to keep in line with cybersecurity regulations, and Hester said the bank does about five to six times what's required.

In November 2019, co-founder, EVP, CFO and COO Drew Keith told *Dallas Business Journal* that the bank was upping its technology solutions both internally and customer-facing on all levels.

One of the strategies to enhance cybersecurity was giving employees laptops and "jetpacks," or mobile wifi technology. This allows the bank's folks to get on the internet without compromising security by attaching to a public wifi. Hester added that every week, patches — or extra updates to the various systems — come through to find holes in the security.

According to the Deloitte Center for Financial Services Outlook Survey 2020, cybersecurity remains a persistent challenge for the banking industry. Forbes reported although breaches were down in 2020 year-over-year, 2019 saw 1,506 separate incidents resulting in consumers' data being compromised.

"Financial institutions were some of the first entities that were attacked from a cyber security standpoint, because it's why you rob the bank. That's where the money is," Keith said.

Enlarge

Drew Keith

COURTESY OF TEXAS SECURITY BANK

Since the Payment Protection Program forced a lot of banks to work rapidly on a high volume of loans, it affected cyber attacks risks nationally, Hester said. In April, Bank of America (NYSE: BAC) reported a breach that possibly compromised PPP business applicants' information to other SBA-authorized lenders and their vendors. Bank of America is the largest bank in North Texas with $85 billion in local deposits. In May, the Financial Services Information Sharing and Analysis Center said that phishing attacks designed for bank employees increased by about 30 percent in the first quarter, especially using the pandemic-related bait, Bloomberg reported.

The community bank mostly serves small business owners, and is the 50th largest bank in North Texas by local deposits, with $414 million, *Business Journal* data shows.

Texas Security Bank works with Roland Technology, a local firm that streamlines much of the day-to-day IT tasks. The bank also contracts Solis Security, an Austin-based company.

To train employees, Texas Security Bank partners with KnowBe4, a company to teach people how to detect phishing scams, or emails that pose as credible sources with the intention of hacking or gathering personal information. Hester said KnowBe4 provides 10 to 20 times more training that most other programs of its ilk.

Lastly, the bank works with CoNetrix, a Lubbock-based software firm to run a cybersecurity assessment test. Hester said the bank wants multiple outside eyes to constantly be monitoring its penetration and vulnerability assessments.

The bank also hired a second in-house IT employee a month before the pandemic hit the U.S.

Hester said the virtual work environment is here to stay, at least in some capacity, so Texas Security Bank will continually update its cybersecurity precautions and training, more than quarterly.