# Fizzy IT Connections

cyber security technology

**Summary:** According to a 2018 IT survey by Safe Systems, about 50% of community institutions said they had more than 100 devices connected to their networks. We provide learnings from this survey.

There is nothing like a good fizzing drink to better enjoy your meal. However, that isn't likely the case in areas that have glaciers and icebergs. You see, in those parts of the world, when such icy behemoths melt, they reportedly make a unique fizzing noise that researchers call a bergy seltzer - plop, plop, fizz, fizz, everyone.

When it comes to banking, some would say the fizz and sizzle of the branch has gone flat. After all, remember the good old days when a bank kept its valuables in a vault? Things are different in the digital age, particularly when it comes to the actions and efforts of cyber thieves. These modern day bank robbers slip into the bank without ever setting foot in a branch.

Understanding how many digital doorways there are into a typical community bank's data gold mine might come as a surprise. According to a 2018 IT survey by Safe Systems, about 50% of community banks and credit unions said they had more than 100 devices connected to their networks. Another 33% said they had 51-100 devices.

Respondents to the survey identified various devices including: laptops, printers, fax machines, servers, routers and switches. This scares technology security people because each new device brings with it a new potential vulnerability point that must be secured. Given so much electronic access, it is no wonder so many modern day bank robbers prefer to come in through a digital back door.

Not surprising, 80% of survey respondents said cybersecurity is their biggest security challenge. Meanwhile, 77% said they had experienced fraudulent activity related to debit cards in the previous 18 months, and 72% stated they had been victims of phishing attempts. There were also reports of account takeovers, malware/ransomware attacks and data breaches.

The real wakeup call in the survey is contained in a key metric for security monitoring. Here, 50% said they conducted a full vulnerability scan of their networks only once a year. Recall that these are banks and credit unions, so that seems strikingly low.

The good news is that 85% said they use security event log monitoring. Here, a healthy 59% review these logs on a weekly basis. Further, 99% use firewalls and 98% use anti-virus.

One additional layer of security is employee training. Bankers know that phishing is one area where cyber thieves regularly try to fool bank staff. Here, banks appear to be making headway, with 47% saying they require employees to take online training and 86% saying they run periodic tests to see if employees get tricked by phishing attempts.

To get your team thinking about how much things have changed, consider IBM research that finds: the average loss per individual burglary in the US is $2,300; the largest bank robbery in US history was $30mm; and the annual cost of cybercrime to the global economy is about $445B.

Clearly, there is still a lot of work to be done. Cyber criminals only seem to get craftier, so bankers must keep changing and trying different things to surface potential issues, before they fizz into something that becomes difficult to handle.

## DEPOSIT OPPORTUNITIES

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 1.85%, subject to availability. Contact operations@pcbb.com.