Increasing Cybersecurity: 3 Steps to Mitigate the Hacker’s Heist

Heading back from Las Vegas following ICBA’s annual convention, I can’t help but think about that heist flick, Ocean’s Eleven, as I consider today’s fraud landscape. The movie’s premise is this: A group of guys set out to steal an exorbitant sum from three casinos. Somehow, they are successful in outsmarting security systems, and they walk away with a cool $150 million.

Contrast that with today’s cyber version of vault-busting thieves. Most often, these criminals don’t stray far from the digital comfort of sophisticated tech and the dark web, taking advantage of the weakest link in the financial transaction: the customer as a point of entry. In fact, the [FBI reports](https://pdf.ic3.gov/2016_IC3Report.pdf) that cybercrime losses in 2016 were $1.33 billion, with email account compromise the number one source of loss.

With threats continuing to emerge, I sat down with ICBA’s cyber expert, Jeremy Dalpiaz, assistant vice president of cyber and data security policy, to discuss what community banks can do to thwart cyberattacks. Our conversation uncovered three important tips for banks in navigating today’s cyber landscape.

**1.** **Ensure the authentication procedures match the current risk environment.** After the Equifax breach, hackers took hold of an enormous amount of information that, when cobbled together, can give thieves the keys to a person’s identity. Banks need to be one step ahead, updating their customer authentication procedures to ask for verification points that have not already been breached.

“Banks have to look at the type of information that was released and the type of information that they hold that they can use to authenticate customers,” Jeremy notes. “We haven’t seen the Equifax information on the dark web yet, but that really shouldn’t comfort anybody. If anything, that should raise the red flag.”

Asking the right authentication question, unique to your data, remains one of the best things a bank can do. More insights for how to strengthen internal processes can be found in the resource, “[Tips for Community Banks Following the Equifax Breach](https://myicba.icba.org/eweb/DynamicPage.aspx?WebCode=LoginRequired&Site=icba&URL_Success=http%3a%2f%2fwww.icba.org%2fdocs%2fdefault-source%2ficba---general-(secure-members)%2fequifax-breach%2ftips-for-community-banks.pdf%3fsfvrsn%3d6%26userToken%3d%7btoken%7d).”

**2. Elevate cybersecurity to an enterprise-wide initiative.** Everyone within the bank has a responsibility to watch out for cybercrime. Because it often happens at the point of entry, every department from customer service to executive management needs to be on the lookout for anomalies in customer behavior or inconsistent requests.

“Cybersecurity is a field that has gone from a technical focus to a whole bank focus,” Jeremy shared. “It is in every line of business and in everyone’s interest that bank employees become familiar with how fraud can occur – whether that’s through hacking, phishing, spoofing or another method.”

As an enterprise-wide activity, banks also should test their incident response policy. Every year, FS-ISAC offers a free [Cyberattack Against Payment Systems (CAPS) exercise](https://www.fsisac.com/Exercises-CAPS) that allows financial institutions to identify gaps in their processes.

This year’s exercises take place Oct. 9-10 or Oct. 16-17, and it’s worth considering for your institution.

“These exercises are good not only for cybersecurity resiliency but for business resiliency in general,” Jeremy says. “We receive great feedback from banks that participate.”

**3. Share information with one another—and with your customers.** One of the simplest ways to counter cybercrime is to participate in information-sharing with other banks. When banks communicate with each other, each entity strengthens. Individual financial institutions get to know hacker tactics, techniques and procedures and identify ways to address potential vulnerabilities.

“With FS-ISAC, you can share information in a trusted environment,” Jeremy points out. “Everybody is sharing information about how to better protect each other’s systems. It’s a pretty unique opportunity.”

In terms of sharing with customers, ICBA is involved in [Operation Stop It!](https://www.operationstopit.org/) which is a joint initiative between the International Association of Chiefs of Police, the Identity Theft Council, and the Identity Theft Resource Center, to help protect communities from identity theft and to make sure victims get the help they need. This group is a great resource for your customers as issues arise, and there are opportunities for community bank involvement as well.

While these tips provide support in updating your fraud mitigation procedures, financial institutions must stay vigilant against cybercrime in ways that align with their organizations’ strategic direction.

No matter the approach, todays cyberattacks call for something more sophisticated than the surveillance found in an old-school casino caper. A bank’s job is to identify ways to outsmart cybercriminals and stay a step ahead to safeguard customer accounts.

**Cybersecurity Resources for Community Banks**[ICBA Cybersecurity Resource Center](https://myicba.icba.org/eweb/DynamicPage.aspx?WebCode=LoginRequired&Site=icba&URL_Success=http%3a%2f%2fwww.icba.org%2fsolutions%2ftools%2fcyber-data-security-toolkit%3fuserToken%3d%7btoken%7d) & [ICBA Data Security Resource Center](http://www.icba.org/advocacy/industry-issues/data-breach) – Provides tools and resources for community banks to stay up-to-speed, including a data breach information center and a cyber and data security toolkit

[FS-ISAC](https://www.fsisac.com/) – Offers a Community Institution Council for information-sharing

[Operation Stop It!](https://www.operationstopit.org/) – Community-based identity theft initiative

[Krebs On Security](https://krebsonsecurity.com/) - A daily blog covering computer security and cybercrime, published by American journalist and investigative reporter, Brian Krebs.

[Verizon Threat Intelligence Report](http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/) - A comprehensive analysis of breaches and incidents investigated by Verizon personnel or reported by one of their 65 partner organizations.

[FireEye](https://www.fireeye.com/) - FireEye is an intelligence-led security company.