Cybersecurity Is Everyone's Job

cyber security risk management

Summary: Bankers know cybersecurity continues to be a top priority. To protect your bank, here are some tried and true ways to do so.

A Harris Poll conducted on behalf of Glassdoor took a look at the top things job seekers want to see in any advertised position. Those ranked highest were: salary (67%), benefits (63%), location (59%), commute time (43%) and employee reviews (32%). Now you know, just in case you need to find a new employee this year.

Speaking of things to do in 2019, bankers know cybersecurity ranks right at the top. To protect your bank, here are some tried and true ways to do so.

Once a community bank determines that a bad actor has entered their system, the IT security team then must determine how to respond. The focus is on the best way to mitigate damage, limit the exfiltration of important data, and help remediate.

Even at larger banks, the volume of flagged incidents and unknown files that need to be investigated is often overwhelming. Nevertheless, community banks must continue to plan for these sorts of attacks because they will eventually happen. Taking steps now to minimize the impact of a cybersecurity breach is just a good idea. To help, consider these tips:

Develop a robust breach response plan. A critical step to minimize the impact of a cybersecurity breach is to develop a robust breach response plan that provides a step-by-step guide to assessing the threat, containing it, communicating to all stakeholders and implementing solutions. Each bank needs to tailor its breach response plan to its specific geography, customer base and risk tolerance. However, key elements typically include: the basic security framework evaluated and installed such as firewalls, intrusion detection and other security measures, and a tool to evaluate the bank's response to a breach, so the entire company can benefit from lessons learned.

Continue to support security education and training. It may be trite, but it still holds true - most banks require increased and more frequent training throughout their organization to help stave off cyber attacks. It is important to continually educate all staff, inclusive of customer-facing, the C-suite and the board of directors. For the average employee, regular IT security training keeps threats top-of-mind. For the top brass, risk education can help them better understand the breadth and enormity of the actual cybersecurity risk, and ensure buy-in.

Test the plan. A community bank, as with any business, not only needs to create an incident response plan that details how it will respond to a potential incident from start to finish, but also to test it. This should include: revamping the plan every few months to determine when and how an incident should be escalated to senior management; determining who internally has overall responsibility for the investigation and who else within the bank must be involved in the investigation; detailing the outside technical and legal advisers; communicating protocol with customers and other affected outside parties; and sharing any cybersecurity incident information with the appropriate regulators and law enforcement.

Cybersecurity is everyone's job and most issues come from humans trying to help, so be aware and prepared. Then train, train and train again, as you help keep your bank and customers safe.

HEDGING SERVICES FOR COMMUNITY BANKS

Community bankers seeing long-term fixed rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP). Contact us today for more information.