Lazy, Impatient Or Prudent Cyber Risk

by Steve Brown

A study by the Brain and Spine Institute in France finds that people are strongly influenced by the people around them and may unknowingly tend to imitate behaviors. The researchers found that after watching how someone else made a given choice, people tended to act more like the person they had observed. If the person they observed was lazy, they tended to act that way too and put off making the decision. Meanwhile, if the person was impatient, they tended to act that way, and if the person was prudent in their choice, the person tended to act that way. Guess this just reinforces the old phrase - monkey see, monkey do. When it comes to cyber risk, bankers cannot monkey around.

While inside cyber breaches are not new, these can still be a challenge to battle. As insiders gain a higher and higher level of trust, some portion may turn to the dark side. In fact, IBM research finds that whether intentional or not, 95% of all security incidents involve some kind of human error.

Most community banks already have a system in place that trains, monitors and educates employees regularly on the latest cyber threats and issues. This is important because employee education cannot be over-stated and should be part of an ongoing effort to control bank risk.

That said, continuous training cannot be done simply through an email blast or an annual training session. Here, CyberScout points out that for frontline and mid-level employees, it is important to share stories about people who have fallen for tricks and conduct penetration tests with white-hat hackers.

Further, cyber security training should be conveyed through a variety of methods that can map to all types of learning styles. These include webinars, live simulations of attacks and even newsletter tips. This approach helps drive the messages and information home for employees as it stays fresh and top of mind. For executives, the same awareness should apply, if not more so. That's because executives are often targeted for fraud because they have the greatest access and authority.

Another option for community banks to boost cyber security is to track employee behavior. An unusually large file download could warrant cause for concern, as could an employee logging on at an unusual time. Checking work behavior regularly could prevent a small breach from turning into a big event.

A bank-wide cyber risk crisis management plan needs to be in place as well. This should include the steps taken within the bank when a cyberattack occurs, the responsibilities of each department and the content and timing of communications sent to customers and law enforcement. The CIO should be the guardian of this plan and ensure it is updated regularly.

While community banks only have so much control over the cyber behavior of customers, it is critical to help educate them on cyber etiquette. After all, customers have many potential breach points not only through their financial online practices, but also through their entire online footprint. Communicating regularly through a variety of media including email, newsletters, mobile

notifications, statement inserts and your website help to educate and remind your customers of the safety precautions needed to keep both your bank and your customer cyber safe.

Every community banker knows the importance of cyber security. Although it is constantly changing as new threats arise, the key is to remain watchful, while regularly providing system updates, training and communications for insiders and customers. Make sure that specific guidance on attack types and scams are pervasive and consistent. This prudent approach will help you protect your bank, employees and customers, by sending lazy or impatient thieves away for another day.

BANK NEWS

OCC Change

The Wall Street Journal reports the Trump administration is preparing to replace Comptroller of the Currency Curry as early as this week.

M&A Activity

1) First Bank ($4.4B, NC) will acquire Asheville Savings Bank ($795mm, NC) for about $175mm in cash (10%) and stock (90%). 2) MainSource Bank ($4.1B, IN) will acquire investment management firm Capstone Investment Management (IN) for an undisclosed sum.

Cybersecurity Changes

A Bank Director survey finds the following areas of cybersecurity programs have been improved by banks over the past 2Ys: investment in technology to better detect/deter cyber threats and intrusions (82%), improved training for bank staff (81%), increased focus on cybersecurity at the board level (80%), improved internal controls related to information security (75%), improved and tested cyber incident management and response plan (75%), increased investment in cybersecurity personnel (62%) and improved intelligence on emerging cyber threats (56%).

Cash Out

A survey by ING Bank finds almost 40% of Americans say they could go without cash entirely and just rely on electronic forms of payment.

Less Cash

An Accenture survey finds the use of cash is projected to decline from 67% of transactions today to about 56% by 2020.