Staying Safe In A Complicated World

by Steve Brown

According to the most recent data from the FBI, the number of burglaries in the US has declined. We welcome this news, but point out that a burglary still happens once every 15 seconds, so homeowners should be mindful not to let down their guard and take action to reduce the likelihood of such an event.

While many home security best practices found easily on the Internet may seem like no-brainers, many people are surprisingly na?ve that something bad could happen to them. Why else would they not lock their doors or windows when more than 30% of burglars easily enter residences through an unlocked door, window or other opening?

In similar fashion, many banks may have a false sense of security when it comes to cyber crime. The simple fact is that these faceless bandits continue to grow stronger, so community bank defenses against them must also continually improve.

If improvements are not made, the bank invites heightened risk should something bad happen. Consider the case of a TN industrial maintenance and construction firm that sued their bank to recover funds stolen by such cyber thieves. In its suit, the company charged the bank with negligence and breach of contract. The lawsuit occurred after cyber thieves managed to steal hundreds of thousands of dollars from the company's bank accounts. As this case continues to work its way through the courts, it will be worth watching to see whether the case makes it to trial. If so, we wonder whether the outcome will make it easier for companies to recover losses from their bank.

Given the threat of looming legal challenges, it behooves all community banks to ensure they have strong security methods in place to detect and prevent fraud. We know nothing's full-proof and cyber thieves are getting more and more sophisticated, but banks must make a reasonable effort to stay out of harm's way to keep customers feeling safe and secure.

It almost goes without saying that bankers need to employ sophisticated software products to monitor and protect against unwelcome intruders. That said, not all safeguards have to be ultra high-tech.

For instance, one easy way to boost your defense is to do away with weak passwords that are easy-to-guess or can be easily obtained in cyberspace by would-be criminals. Equally important is to train employees how to safeguard their computers, iPads, smartphones and other devices. Finally, simply ramp up training around manual call-back procedures and role-play using real life examples staff may encounter. Explain the consequences of not following procedures and be sure everyone understands the very best result of a large cyber theft is that your bank is going to lose that customer. Be sure to also address topics like how to create secure passwords, avoid various scams and sidestep viruses and malware.

Nowadays with virtually everyone bringing their own devices to work, protecting data has become even more difficult. One suggestion here is to closely monitor the use of personal devices so they don't become your weakest link. At the very least, employees need to be held accountable for the security of their personal devices if they are using them for business.

Staying safe in an increasingly dangerous cyber world is admittedly a challenge. Banks have to be willing to engage multiple locks so thieves don't have open-door access to customer money or data.

BANK NEWS

Testing

The FDIC indicates smaller banks with non-complex balance sheets may do their own independent reviews. Examples include: appraisal reviews - can be done by outside board members with expertise in real estate development or valuation (as long as the individual does not participate directly in the bank's real estate lending or appraisal function); loan reviews - can be done by outside directors or staff independent of the loan function (if they do not participate directly in the credit approval process); loan loss reserve methodology - can be done by an accounting or finance officer (if they are independent of the credit approval and loan loss estimation process); HMDA audit compliance - can be done by an outside director (if the director does not participate in the lending function under review); BSA/AML compliance - can be done by internal audit or a qualified staff person or director (if they are not involved in the BSA/AML compliance program); interest rate risk measurement and reporting - can be done by lending staff; liquidity risk management - can be done by lending staff.

Debit Fees

MyBankTracker reports the cost to replace a lost debit card at the Top 10 largest U.S. banks is: $7.50 at PNC, $5 at Bank of America and $5 at BB&T, while the rest do not charge. For customers seeking a rush replacement, BB&T is the most expensive at $30, followed by SunTrust, PNC and U.S. Bank at $25 each.

IT Projects

A KPMG banking industry outlook survey of 100 bank executives in the U.S. finds the primary areas these executives say they are focusing on related to IT projects over the next 12 months are: mobile payments (37%); risk data aggregation (21%); regulatory spending (12%); social media (11%); customer, front office interface (8%); investing in online banking platform for laptops/desktops (8%) and leveraging data to optimize customer development (3%).

Customers

A study by Oliver Wyman finds people who switched banks that also said marketing or advertising impacted their decision, mentioned the following Top 7 methods: direct mail (32%); digital sources (31%); TV (21%); email (16%); bank location/ATM (14%); newspaper (11%) and radio (10%).