Inject Your Bank With A Data Security Culture

cyber security risk management

Summary: Banks are recognizing that mitigating IT risk cannot be the sole responsibility of the IT department. Everyone, from the top down, at a bank needs to be involved.

Flu season this year is one of the worst in recent memory, which is why we were intrigued by work done by UCLA researchers. They have found a way to trigger longer lasting T-cells that can combat a variety of flu strains, instead of injecting a mix of several known virus strains to trigger antibodies that fight those specific viruses. While it will take some time for human testing of this vaccine, if all the other outcomes are good, it would be an amazing development for our health culture, because it would mean the days of an annual flu shot would disappear.

Much like avoiding the flu, community banks continually seek to avoid cyber viruses and threats. In this area, banks have recognized that mitigating such risks cannot be the sole responsibility of the IT department. Everyone at the bank from the top down needs to be involved.

As online breaches and threats to a bank's sensitive information are increasing, community banks are coming to grips with the fact that information security is too big, too pervasive and too pernicious for their IT teams to conquer on their own. In addition, it's not just sinister cyber-criminal outsiders who pose a threat. Indeed, almost 40% of data breaches are due to accidental loss or a malicious insider, according to the Breach Level Index.

As such, bankers are embracing the fact that they must teach and train all personnel in this area and embrace a "data security culture" throughout the bank. This culture is one in which all employees are not only aware of potential information threats internally and externally, but are well-versed enough to see the telltale signs of a potential breach, data theft or scam. Here are some tips on how to build that culture:

Raise security awareness throughout the year. Most community banks have an annual update which includes cyber etiquette along with some in-person or computer-based training. It may be worthwhile to remind employees of cyber security tips along with any education around major breaches throughout the year in regular company communications.

Make it interactive and positive. Training reviews, penetration testing and other security awareness drills should be as fun as possible and even rewarding. Perhaps it is time to offer a monthly gift certificate to the employee who reports a suspected phishing email to the IT department, or pizza for the department or branch that scored the best on a regular data security quiz. According to a 2017 report from Cybersecurity Ventures, using these types of regular, interactive and helpful techniques helped reduce successful phishing attacks on one large bank by more than 40%.

Enlist data security evangelists. Technology and security teams are constantly under fire. In order to help them, start by expanding their reach and extending the data security message. Perhaps consider appointing a data security ambassador or champion in each business unit or branch. This will not only help expand the data security culture, but it will put a familiar face on cybersecurity, and employees are more apt to listen to a member of their own team.

Consider engaging outside support. Sometimes, it pays to consult an external expert. This is especially true for banks that lack the depth of expertise or budget to have at least one committed full-time data security staffer. For the past 3Ys, the security awareness training market has been growing at 50% or more annually, according to Gartner, as both big and small organizations seek out the advice and support that can help them reduce the number and the impact of cybersecurity incidents. Also of note, companies that hired outside security awareness training professionals to help them develop or conduct their data security program saw an average 127% ROI in less than one month, according to Forrester.

There is no single shot that will prevent cyber breaches, but being prepared and working together will help keep your bank healthier and happier at least.

DEPOSIT OPPORTUNITIES

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 1.60%, subject to availability. Contact operations@pcbb.com.