PCBB BID® Daily Newsletter Oct 16, 2018

The Precision Of A Data Security Sweet Spot

cyber security technology risk management

Summary: A recent FICO study shows 80% of consumers don't see the need for what they consider unnecessary security procedures. How to strike a balance between security and customer satisfaction.

It seems our long lost relatives, the Neanderthals, were not just a bunch of grunting brutes. A study that analyzed bones found they had a precision grip very similar to our own more modern day variety. It seems we still have much to learn!

In the world of cybersecurity, bank teams are always learning to keep up with bad actors too. After all, it is often difficult to know how much security is too much. This is important when you consider a recent survey from FICO. It shows how fed up consumers are with the security hoops they need to go through to verify their identity. This is despite the constant barrage of information about data breaches and card compromises. It seems 80% of respondents don't see the need for what they consider unnecessary security procedures.

In addition, 47% said they are tired of having to answer endless security questions whenever they call customer service departments. Even worse, a startling 64% don't see the need for complex passwords featuring a mix of numbers, symbols and capital letters. Finally, 48% are frustrated with the use of two-step verification and 71% are frustrated by captcha codes.

Bank IT teams reading this are probably feeling queasy about now, but they aren't the only ones. Sales teams too should note that 22% of respondents said they would either give up on opening a bank account completely, or give up and try at a different bank, if they had to jump through too many hoops.

It's an interesting perspective, given that security--or lack thereof--is one of the top things keeping bank executives up at night. With good reason: cyberattacks and data breaches are more common than in any other industry. 45% of financial services organizations have had a data breach in the last 2Ys, and the severity and volume of cyberattacks continue to increase, according to a global cybersecurity study by Ponemon Institute.

Certainly, it's a balancing act. Customers may say they're willing to forgo security for convenience, but one wonders if they'd say the same after being part of a damaging data breach. In our view, banks have to find a happy medium. This is the sweet spot between protecting customer information and piling on too many layers of security that could push customers away.

This analysis starts with a risk assessment to ensure the necessary security precautions are in place, while at the same time allowing business to function smoothly and customers to bank effortlessly. Are you utilizing the most appropriate tools, technologies and procedures to meet this multi-faceted challenge? A little research on this could go a long way. But, more than likely, you have already started this.

Artificial intelligence (AI) is an option that is getting more reasonable for community banks. Your bank may want to explore how AI could help you more seamlessly analyze patterns that smack of fraud. Technology available today has the potential to spot trouble without putting customers through hoops, and this technology is only getting better over time.

To be sure, fraudsters are getting more sophisticated, especially as we move toward an increasingly digital world. Community banks will need to continue their diligence to ensure their data security efforts work for them and their customers.

LOAN SERVICES FOR COMMUNITY BANKS

PCBB is almost entirely owned by community banks and it does not compete for your business. Contact us to do loan participations as you protect your customer relationships.