Speaking The Language Of Data Security

cyber security risk management

Summary: The World Economic Forum projects the cost of cybercrime to businesses will hit $8T over the next 5Ys. We outline ways to stay safe.

A new study by MIT researchers finds that if you are interested in learning a new language, the best time to do so, to become as proficient as a native speaker, is before the age of 10. You can still learn languages after that, of course, and even understand them. But to truly master speaking, it looks like it is more child's play than anything else.

Bankers certainly don't play around though when it comes to protecting customer and bank data, but it is critical to stay vigilant. In fact, as of February 21st, there had already been 140 data breaches compromising almost 3mm records at companies, according to Identity Theft Resource Center. Although this number is flat compared to the same period last year, these attacks seem to get bolder and more expensive.

Ponemon Institute finds the average cost per breach is over $5mm. Also, the World Economic Forum projects that over the next 5Ys, the cost of cybercrime to businesses will hit $8T. This cost includes: loss of customers; post data breach response; detection and escalation and notification. Not only that, but according to Verizon Data Breach Investigations Report, 24% of all breaches last year affected financial institutions.

So, although we have provided tips to stay cyber safe before, we thought it was a good time for a refresher.

Passwords - This is the most vulnerable area for hackers still. Verizon reports 81% of hacking related breaches stem from weak or stolen passwords. Remind your customers and employees to change their passwords often and make them at least 10 characters long with a number and symbol included. Meanwhile, research by Pew finds 86% of people memorize their passwords, while 49% write them down on paper and 24% save them in a note on a computer or mobile device. Also, younger generations tend to be far more lax about the passwords they use than older generations, so special emphasis there is a good idea.

Phishing - These attacks are still done since they are valuable to hackers. Verizon notes that more than 75% of these attacks were financially motivated last year. In a blink of an eye, an employee or customer can download malware and do great damage. It never hurts to keep this on top of mind bank-wide through your regular communications.

Software and Hardware Exposures - Software and hardware needs to be updated or patched regularly, of course. When this is not done, vulnerabilities can be exploited. Regulatory scrutiny is high in this area, driven by research that finds roughly 99% of attempted malware attacks are for vulnerabilities where an update or patch is already available. Making sure your team has this covered is obvious but also critical.

Third Party - Your vendors, consultants, contractors and any other third parties are no doubt on your radar for cyber risk and managed accordingly. It is important to address both the access of third parties to sensitive data and your third party's own data management protocol and controls. Review these areas often to ensure they are firmed up.

While you may not have learned any new cyber languages here today, we hope some of these statistics and pointers at least get you thinking about the best way to translate actions into success for your community bank.

CREDIT STRESS TESTING SERVICES FOR COMMUNITY BANKS

Community bankers can credit stress test loans of all types from multiple perspectives and on a portfolio basis. Get professional help doing so and learn about credit stress testing here.