Skimping On Cybersecurity - A Risky Business

by Steve Brown

A high school senior's parents go on vacation leaving him behind. He decides to take advantage of his parents' absence and experiments with fast cars and fast women. He crashes his dad's Porsche and the prostitute he entertained steals his mother's expensive Steuben egg. The result is a predicable derailment of final exams and a Princeton admission interview. This premise is behind the popular 1980s Tom Cruise movie Risky Business, but it also reminds us of today's cyber situation - shirking accountability and control can be a risky business.

Banks spend a considerable amount of time in strategic planning mode, and a critical element of this relates to staffing issues. Indeed, banks must ensure they not only have an appropriate number of employees to serve their customers' needs and ensure productive and effective business operations - but also the right ones in the right jobs. Without the right staff, all sorts of troubles can ensue. These include disgruntled customers, temporary business interruption, regulatory intervention and potentially much worse.

This backdrop helps explain why we are so disturbed by recent research that suggests most companies still aren't properly staffed to handle cybersecurity issues. The research wasn't specific to banks, but it's worth taking note, since these could be your customers and given that banks are a major target for cyber-criminals. Further, attacks are becoming increasingly sophisticated and more expensive to remediate.

Consider a Spiceworks IT security report that found 80% of organizations experienced a security incident in 2015. Next, note that when the IT provider polled more than 600 professionals, only 29% of organizations said they have a security expert working in their IT department. Meanwhile, a measly 7% reported having a security expert in another department and only 7% said they have one on the executive team.

One silver lining perhaps is that 23% of organizations said they contract outside security experts to help with IT matters. Our comfort level dropped considerably, however, after reading that 55% of organizations claimed not to have regular access to any IT security experts at all, whether internal or third-party. Worse, a majority of companies said they have no plans to hire or contract a security expert within the next 12 months.

Another alarming trend is the lack of security credentials among people holding IT jobs. When Spiceworks surveyed more than 1K IT pros about their cybersecurity credentials, 67% said they do not have any security certifications. While certifications aren't necessarily the only way to assess an employee's prowess, they are one way for the lay person to ensure standardization and at least measure whether you have a well-trained and qualified team in place at some level.

Research consistently shows that company executives believe protecting their organization against cybercrime is a top priority. Yet many aren't putting words into action. Meanwhile, companies continue to be pounded by malware, ransomware and denial-of-service attacks. While many of the highly publicized attacks have been against large companies, community banks are not immune, and the cost of remediation can be detrimental to business.

While no system is ever full-proof, it seems evident from recent security breaches that banks should continue to work to improve and test to help thwart cyber-thieves. One way to do this is to make sure you have properly trained IT staff policing the gates. Check credentials regularly, and if you are outsourcing, ensure that you have regular meetings, ask tough questions about breaches and ensure your data is as safe and secure as it can be. Without this, you are leaving your bank even more vulnerable to attack, and that is risky business.

BANK NEWS

Tepid Wealth

Research by a group of Stanford economists finds only 50% of Americans born in 1984 earned more at age 30 than their parents at that same age vs. 92% in 1940. Adjusted for inflation, the bottom 50% of Americans earn the same now as they did in 1980.

Customer Analysis

A survey by Oracle and Efma of senior executives at global financial institutions finds the following types of data are used to get a complete view of customers: financial information at customer and account level (95%), online and offline interactions with the bank (53%), contextual information (46%), dynamic demographic data (37%), location information (36%) and social media information or trend data (20%).

IT Spending

Forrester projects IT spending growth (on products, services and staffing) in 2017 will be 4.3% vs. 5.1% projected earlier. The decrease comes after Forrester calculated in the effect of President-elect Trump's proposed tax cuts and other things.

Debt Ownership

Research by the Treasury finds Japan has moved into the top spot of ownership of US debt at $1.13T as of Oct, while China has dipped to the second spot at $1.12T. China's holdings as of Oct were the lowest in 6Ys.

Valuable Assets

Research by Korn Ferry finds CEOs rank the following as the most valuable assets they have right now (in order): technology (back office infrastructure); technology (product, customer channels); culture; inventory; and innovation/R&D.