Exercising Cybersecurity

cyber security business customers risk management

Summary: Cisco reports that many small and medium-sized businesses can go out of business due to a cyberattack. How to help keep your business customers safe.

The Bureau of Labor Statistics (BLS) reports the average percentage of the US population 15Ys and older that is engaged in sports or exercise each day is about 19% overall. That has been roughly about the same over the past decade. In case you were wondering, the most popular sports or exercises people do in order are: walking (30%); weightlifting (13%); using cardiovascular equipment (13%); swimming, surfing or water skiing (8%); running (7%); basketball (5%); golfing (4%). Enjoy this info no matter your exercise of choice.

Speaking of information to share, community bankers do great business with both small and midsized businesses (SMBs). Given so much usage of technology, this adds risk to the community bank business model, so we wanted to alert you to some areas of specific interest perhaps.

We begin with research by Cisco, whose report is based on findings from SMBs responding to its 2018 Security Capabilities Benchmark Study. It notes that SMBs can be put out of business by a massive cyberattack, as more than 50% of all cyberattacks can run up a tab of $500k or more. This includes lost revenue, customers, opportunities and out-of-pocket costs.

Cisco cited a Better Business Bureau survey, which asked small business owners how long their business could remain profitable if it permanently lost access to critical data. It wasn't long: about 67% said only 3 months and more than 50% said less than 1 month. It is critical community banks not only keep SMB customers informed, but also help out where possible.

SMBs said they are most concerned about phishing and other kinds of targeted attacks against employees, advanced malware and other new threats, and ransomware. Further, SMBs are more likely to just pay the ransom so they can get back to business right away. They worry the downtime and the inability to get to their data could kill their business.

Cisco also notes that companies should be concerned about "cryptomining," growing in popularity because the loot can't be traced, and hackers may not face as much criminal liability. Additionally, SMBs must protect themselves against employees stealing intellectual property as well as sensitive financial and client data on the company's cloud-based online platforms.

Businesses told Cisco that if they had adequate staffing, they would be more inclined to invest in better technology. Specifically, they focused on adding more advanced malware protection and endpoint detection and response solutions; enhanced online application security; and better intrusion prevention systems.

Many SMBs turn to cloud-based security solutions. But, as we know by now, due diligence on vendor systems is a must. Additionally, it should be remembered SMBs need to also prepare for potential cyberattacks on their on-premises software. Many SMBs outsource their security processes, but they should still train employees on how to conduct threat intelligence and incident response in-house, of course.

Community banks may want to take some of the advice from Cisco's report, as well as pass it on to your SMB customers. By working together on this, your bank and your customers will not only strengthen relationships, but keep everyone safe.

INTERNATIONAL SERVICES FOR COMMUNITY BANKS

Our international services are designed for community banks to help you capture more customers and fees. Contact us today for more information.

Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.