Space-walking Around Cyber Risks

cyber security risk management

Summary: Ninety percent of cybersecurity budgets focus on securing the network while nearly 75% of all cyberattacks happen at the application level. The key threats in 2018.

A couple of Russian astronauts reportedly took a walk in space in a record setting event to repair an antenna. The only problem was that when all was said and done, the antenna was apparently installed in the wrong spot. Mission Control is now trying to figure out what to do to fix it, up to and including taking another walk in space perhaps. It just goes to show you that sometimes even the best laid plans can go awry.

In banking, the same holds true when it comes to protecting against cyber risks. After all, cybersecurity and cyber-attacks are fast-moving areas so it can be difficult, if not impossible, to keep up. In 2017 alone, the unprecedented takeoff of ransomware, phishing and other risks surged.

These fraudulent activities have worked their way into most industries, having a seismic effect on how employees communicate with customers and each other.

You would think given all of this risk that budgets would be rising too in an effort to combat the problem. Oddly, according to some studies, 90% of dollars spent on cybersecurity focused on securing the network. This is despite the fact that nearly 75% of all cyberattacks happen at the application level.

Given there is so much at risk here, we wanted to provide you with a list of potential cyber threats for 2018:

Third-Party Risks: Most businesses are becoming ever more reliant on third party vendors. Unfortunately, these same vendors have over the years also become an increasingly popular springboard for cyber-criminals too. According to a fall 2017 survey by the Ponemon Institute, 56% of organizations say they have already been hit by at least one breach initiated through a vendor. The study also found that the average number of third parties with access to an organization's sensitive information has also grown. Sadly, only 33% of respondents said they even had a list of all the third parties who had access to their information. Even worse, less than 20% knew if their own vendors were in turn sharing information with other vendors. While depending on third parties is a trend that is not likely to decrease, given the improved efficiencies and other benefits these relationships offer, it is recommended that banks do more due diligence vetting vendors to protect your data.

Large Scale Malware Attacks: These sorts of things include such names as WannaCry, NotPetya and Bad Rabbit that all became commonplace last year. These attacks locked down computer systems, shut down services at hospitals and major corporations, stole millions of pieces of personal information and, siphoned hundreds of millions of dollars from victims. As a wider base of attack endpoints occurs, with more devices becoming hooked up to the internet, bad actors are likely to find more potential areas to strike with their malware.

Ransomware Attacks: The seemingly boundless popularity and profitability of ransomware, as a means for cyber-criminals to steal with less heavy-lifting and less risk to themselves, is making these advanced malware threats more popular than ever.

Spear Phishing: Phishing is far from the newest game in town, and bank IT teams know all about it. Even its precocious younger sibling, the more targeted "spear-phishing", is a fairly well-worn exploit. However, after all these years, it still remains an effective and easy way for hackers to plant malware, access computers and even hijack corporate or personal computing devices. The goal is to get victims to send money to thieves. Sadly, a 2017 survey of IT decision makers finds only 25% believed their users could successfully identify a phishing attempt. Aided by machine learning and research culled from social media, phishing attacks promise to become even more sophisticated, complex and prevalent, according to predictions from McAfee Labs. Attackers are crafty and they are using more research to sound authentic, involving more steps and layers.

Risks abound in the cyber world for sure. As such, know that no matter how much you plan and prepare, your mission control IT team will remain under pressure.

HEDGING SERVICES FOR COMMUNITY BANKS

Community bankers seeing long-term fixed rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP).

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.