Neglecting Cyber Security Can Cost Your Business Dearly

Jim Orr, CISSP

Cybercrimes, including ransomware, phishing and various other scams, are a continual threat to both businesses and individuals. If your organization has fallen behind in upgrading its online and email security, it could become an easy target for cyber criminals.

Americans lost a staggering $6.9 billion to cyber criminals in 2021 according to the recently released FBI Internet Crime Complaint Center. This marked a 55% spike from 2020.

Occurrences of online fraud were particularly numerous over the past two years as the world dealt with the COVID-19 pandemic. While businesses and individuals struggled to adjust work schedules and establish work-from-home arrangements, fraudsters took advantage of weak security systems and targeted both personal and business accounts.

Sadly, in 2021, Texas ranked second nationally with more than $606 million in victim losses, while Colorado ranked 14th nationally with more than $130 million in victim losses.

One of the costliest cybercrimes has been Business Email Compromise (BEC) schemes, also known as email account compromise, which resulted in $2.3 billion in losses to American companies last year.

BEC fraudsters use sophisticated techniques to infiltrate a business email system. Often a business will be unaware that a criminal has compromised their email system, allowing the criminal to monitor their emails, seeing private ongoing and current communications.

With this information, fraudsters can use a spoofed email account of a chief executive officer or other high-ranking employee to request wire payments. If the criminal has monitored the email system, they may even use a legitimate transaction that those inside the organization are familiar with but change the payment destination.

This method has also been used by cyber criminals to gather vendor email addresses, requests for W-2/SSN information and other sensitive details used in identity theft. This is particularly true in smaller businesses which may lack more sophisticated security.

Phishing scams, where fraudsters send fake or spoofed emails to trick individuals into revealing sensitive information or authorizing payments, is the most common form of cyber theft. The scams aren't a new phenomenon, as the FBI indicates that more than $18.7 billion has been stolen online over the past five years. Call it unarmed robbery.

March 30, 2022

Another common scheme is impersonating government officials, bank contacts, official offices (via email) or others that consumers and business contacts may otherwise consider trustworthy sources. Through social media, emails or phone calls, scammers trick individuals into revealing personal information or possibly even sending electronic payments.

Ransomware is another cybercrime on the rise that continues to negatively impact businesses. A form of malware, ransomware is used to lock down a company's computer files and data, making it inaccessible and creating a disruption to company operations. Companies who rely heavily on data to conduct their business or maintain customer accounts are then often told a ransom must be paid for their files to be unlocked. In some instances, a business may agree to pay a ransom and still not get their files unlocked.

Although law enforcement is improving its technology and policing capabilities, criminals are also becoming wiser and more daring in their schemes for defrauding individuals and businesses for either money or stolen identities.

So what can you do to protect your business?

Make your network security a priority. The criminal activity never stops, and fraudsters are continually devising new ways to attack your systems. Many companies make the mistake of upgrading their systems once but fail to make this a budgetary item for keeping their systems up to date every year.

Install anti-virus and anti-malware solutions and keep them up to date. Establish effective and regular network backups for your business data, as well as installing firewalls to prevent unauthorized access.

Perhaps most importantly, educate your employees on phishing scams and how to identify fraudulent emails or phone calls. After all, the weakest links are often in human form. You can install state-of-the-art security, but just one person clicking on the wrong link or providing formation over the phone can help a criminal achieve their goal.

Jim Orr is a certified information security systems professional (CISSP) and Senior VP, IT Governance & Information Security, at Independent Financial™.

March 30, 2022