Cyber attacks increasingly target small business

Many issues can keep a small business owner up at night, but one threat near the top of the list is a cyber attack. According to a 2024 report by the U.S. Chamber of Commerce, 60% of small businesses indicate cyber security threats, such as phishing, malware and ransomware, as among their top concerns.

Those concerns are well founded, especially as cybercriminals are becoming more sophisticated as they incorporate artificial intelligence to test systems or send fake messages that sound just like an executive. **Larry Zelvin, Executive Vice President and Head of the Financial Crimes Unit at BMO Financial Group,** is one of the foremost authorities on cyber risk. Having worked as the Global Head of Cyber Security at Citigroup and Director of the National Cybersecurity and Communications Integration Center with the U.S. Department of Homeland Security, he uses his extensive experience to help clients increase their security knowledge.

We've all seen headlines of large organizations being hit by a cyberattack, but do small and mid-sized businesses face just as much risk?

Yes, in fact small- and medium-sized businesses are being targeted more frequently than larger companies. If your organization is connected to the internet, it's at risk. In some cases, threat actors actually prefer targeting smaller companies because they don't necessarily have the resources in place to actively be detecting and mitigating attacks.

In some cases, threat actors actually prefer targeting smaller companies because they don't necessarily have the resources in place to actively be detecting and mitigating attacks.

What can small and mid-sized companies do to protect themselves?

The harder a target you make your organization—the better off it will be. Increasingly, attacks are becoming automated, so it's important to protect yourself against this type of threat. This includes putting initiatives such as multi-factor authentication and encryption in place, as well as installing security patches to remove vulnerabilities within your network. In many cases, moving information to the cloud can make securing your information more effective than maintaining a server on site. We keep reinforcing password best practices because strong, complex passwords remain an important tool to protect against threat actors.

Many small companies don't have a dedicated IT team, so how should they approach cyber security?

It's important to identify someone with in the organization, such as a CFO, to be the point of contact on cyber security. They may start by establishing security best practices required by employees and an incident response plan that lists steps to take in the event of an attack. That incident response plan should include details about any cyber insurance, outside legal counsel and other external partners or resources to work with in an emergency. Here at BMO, we have plans and playbooks in place and run tabletop exercise drills to test our procedures.

Continued

Larry Zelvin is the Head of the Financial Crimes Unit at BMO Financial Group where he is responsible globally for cyber security, fraud, physical security and crisis management. Prior to BMO, Larry was a Managing Director and the Global Head of Cyber Security at Citigroup. Larry has also held several roles in the U.S. Government that include Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security; Senior Director for Response, National Security Council, The White House; and, Director, Homeland Defense Integration, Office of the Secretary of Defense, The Pentagon. He served as a U.S. Naval Officer and Aviator for 26 years and retired as a Captain. Larry has a Bachelor of Arts from Boston University, a Master of Arts from the U.S. Naval War College and a Master of Science from the U.S. Defense Intelligence College.

What about organizations looking to set up a security office to focus on cyber security?

If you're a small-sized business, you may consider working with a third party to conduct a cyber evaluation, advise you on vulnerabilities and then then help mitigate what is found. Again, it's also advisable to establish an accountable executive within the organization.

If you're a medium-sized business with a large geographic footprint and critical points of exposure, you may want staff or resources focused on security day to day. The decision depends on how you assess risk. One of the challenges today is finding people to take on this role. There is more demand for cyber security talent than there are experienced people to meet the demand. Sometimes, companies hire cyber "experts" only to find out later that the individual isn't up to the task.

How much extra work would it be if someone like a CFO is tasked with managing a company's cyber security?

For businesses that are just starting to think about cyber security, the time required is likely a couple of hours a week. The more time you spend getting ready with legal counsel, conducting assessments, and putting risk mitigation initiatives in place, the better off you'll be. As they say, a pound of prevention is worth two pounds of cure. Once you're through that process, you may spend a couple hours a month to review security capabilities and make updates as needed.

Is there a place to start that conversation?

A good place to start is with your legal advisors. Then, you can talk to your industry groups and suppliers.

There are many excellent resources online; BMO provides general security information and resources on BMO Security, including security tips, articles on threats and how to help stay protected, updates on fraud scams and more.

What are some other threats that small business owners need to consider?

You're only as strong as your weakest link. Ensure that you scrutinize your vendors and supply chain, especially if you work with smaller suppliers. In some cases, your interconnectivity with these organizations may expose your organization.

Ask some basic questions. Do you have a cyber security program? Do you know who leads your cyber program? When was the last time you had an outside assessment? Have you done any exercises? You've got to have those difficult conversations.

What other threats are you seeing?

There's a new phrase out there that goes: "Why hack in when you can log in?" Instead of using phishing emails with the links or attachments, cyber criminals are using social engineering techniques to obtain your username and password, and then they just log in as you. From a security perspective, organizations can't identify the bad actor as quickly because a legitimate username and password were used. Ultimately, all of us must be very careful about who we're sharing information with.

BMO | Wealth Management

CAS00000000 (5/25)