WHY YOUR SMALL BUSINESS CAN BE A BIG TARGET FOR HACKERS

BY MIKE REMER, FOUNDER AND PRESIDENT,
COMPUTERCARE LLC

For the last couple years, the trend has been for hackers to move away from the "big score" of hacking a big business. More and more small and medium businesses have become the targets of all sorts of cyber attacks, with over 70 percent of the reported breaches for the last year targeting small businesses.

This shift can be attributable to a number of things, but the key is the concept of "the path of least resistance." This concept is pretty easy to understand, but in a nutshell, smaller businesses generally have lax to non-existent security in place, more vulnerable IT systems and security is minimal or average at best. Also, hackers don't get as much attention as compared to trying to hack into more complicated, state-of-the-art systems with bigger firms and businesses, and that means easy money for hackers.

Let's be clear: a hacker does not have to be someone sitting in a basement of a non-descript run-down apartment building in a former eastern-bloc country. A hacker is anyone who uses a computer to gain unauthorized access to data. This can be someone outside the company, outside the country, or an employee or vendor. In fact, one of the country's large-scale data breaches was hacked by gaining entry through a maintenance technician who had access to the physical building. There was a reported breach of a small newsstand in Chicago, where cyber-thieves were able to install a trojan in the cash registers. This piece of malware sent swiped credit card numbers to the hackers without the owner's knowledge.

SHUTTERSTOCK.COM

While there was no "loss" to the business owner because the money was taken from the credit cards of the customers, the credit card company demanded an investigation into the breach at the expense of the business owner, who had to shell out over $20,000.

So, what's the gain for the hackers?

Well, in addition to money, either in the form of ransom-ware style malware or directly from a credit card or other financial institution scanning, hackers can go after a business's intellectual property or any other personal identifiable information belonging to the business or the businesses patrons. This information can be used to steal money or, in some cases, to steal identities.

Among small businesses that suffer a breach, 60 percent of them go out of business after six months.

What can you do to protect your business?

Talk to your employees about cyber security — your people should know the policies and practices you expect them to follow in the workplace regarding Internet safety. Focus on what needs to be protected by creating a risk management plan. Forecast the consequences if a successful attack happened by quantifying those risks. Create a culture of cybersecurity within your organization: Teach your people to understand the value of protecting not just your data but your customers' data as well. Work with your IT department or managed service provider to identify areas of risk within your computer and network systems. Devise a plan to protect those systems, including properly maintaining systems and using more robust computer and networking equipment.

MICHAEL REMER is founder and president of ComputerCare LLC, an IT services company providing a full spectrum of IT solutions and services to small and medium businesses.