Small businesses vulnerable to cyberattacks, then don't act

18 June 2018, by Joyce M. Rosenberg

Small businesses suffered a barrage of computer invasions last year but most took no action to shore up their security afterward, according to a survey by insurer Hiscox.

It found that 47 percent of small businesses reported that they had one attack in 2017, and 44 percent said they had two to four attacks.

The invasions included ransomware, which makes a computer's files unusable unless the device's user or owner pays a ransom, and phishing, in which emails that look legitimate are used to steals information. The invasions also include what are called drive-by attacks, which infect websites and in turn the computers that visit them.

Despite the prevalence of the data invasions, only about half of small businesses said they had a clear cybersecurity strategy, the report found. And nearly two-thirds said they didn't bolster their security after an attack.

Hiscox estimates that seven out of 10 businesses aren't prepared to handle cyber attacks, although they can cost a company thousands of dollars or more and ransomware can shut down operations. Cybersecurity tends to get pushed to the back burner while owners are busy developing products and services and working with clients and employees. Or owners may see it as an expense they can't afford right now.

Some basic cybersecurity advice:

—Back up all of a company's data securely. This means paying for a service that keeps a duplicate of all files on an ongoing basis. The best backups keep creating versions of a company's files that can be accessed in the event of ransomware—eliminating the need to pay data thieves. Some backups cost just a few hundred dollars a year.

—Install software that searches for and immobilizes viruses, malware and other harmful programs. Also install firewalls and data encryption programs.

—Make sure you have all the updates and patches for your operating systems for all your devices. They often include security programs.

—If you have a website, learn how to protect it from hackers, using software including firewalls. But you might be better off hiring a service that will monitor your site with sophisticated tools that detect and disable intruders.

—Tell your staffers, and keep reminding them, about the dangers of clicking on links or attachments in emails unless they're completely sure the emails are from a legitimate source. Educate your employees about phishing attacks and the tricks they use. Phishers are becoming increasingly sophisticated and are creating emails that look like they really could have come from your bank or a company you do business with.

—Hire an information technology consultant who will regularly look at your systems to be sure you have the tools you need to keep your data safe.