Protecting companies' systems needs to be ongoing process

September 4 2019, by Joyce M. Rosenberg

Credit: CC0 Public Domain

Small businesses can take steps to make their computers and websites less vulnerable to cybercriminals, but owners also need to be vigilant about protecting their data.

Cybersecurity has some basic components, such as using anti-virus and anti-malware programs on all devices, and making sure that updates and

patches that hardware and software makers periodically send out are installed, says James Goepel, CEO of Fathom Cyber, a cybersecurity consulting firm.

Another aspect of cybersecurity is education for everyone, including the owner, about the dangers of clicking on links and attachments in emails. That's a common way for phishing scams to occur; these attacks use realistic-looking emails to trick computer users into downloading harmful software onto computers, phones and other devices.

There are plenty of resources online to help owners understand what they need to do. The website for the Federal Communications Commission lists the basics, and also has links to organizations and technology companies that supply more details. Visit www.fcc.gov/general/cybersecurity-small-business .

Goepel recommends owners visit the website for the Center for Internet Security, which has a comprehensive description of cybersecurity practices. It can be found at www.cisecurity.org .

But protecting a company against cyberattacks must be a thorough and ongoing process to be effective. An owner trying to stay on top of patches, updates and changes while also dealing with all the aspects of running a business is likely to need help. Unless there is a dedicated technology staffer in the company, the best strategy is to hire professionals whose work is to monitor companies' systems and be sure their protection is up to date. Similarly, websites need to be monitored to be sure they're not hacked—and if they are, to deal with the invasion immediately.

One issue small companies face is that owners may not know how many devices, programs and apps are in their systems—any of them could be vulnerable.

"You can't patch everything if you don't know what you have on your network," Goepel says.

Small firms are increasingly targets for attackers, according to insurer Hiscox, which commissioned a survey of 5,400 companies and organizations of all sizes about cybersecurity in late 2018. Forty-seven percent of small businesses, those with under 50 employees, reported at least one or more cyberattacks, up from 33% in a survey a year earlier. Among mid-sized companies, those with between 50 and 249 staffers, 63% reported they'd been hit by a cyberattack, up from 36%.

Many small businesses have taken steps to make their data more secure, according to a survey of 1,504 owners Bank of America released during the spring. But when asked about the steps owners took, many hadn't taken care of some key fundamentals. Of the 80% of small businesses that had made adopted cybersecurity measures, only 47% installed security patches and updates and 44% secured their customers' information. That meant a lot of systems weren't protected.

"The bad guys know the small guys aren't spending money on it," Goepel says.