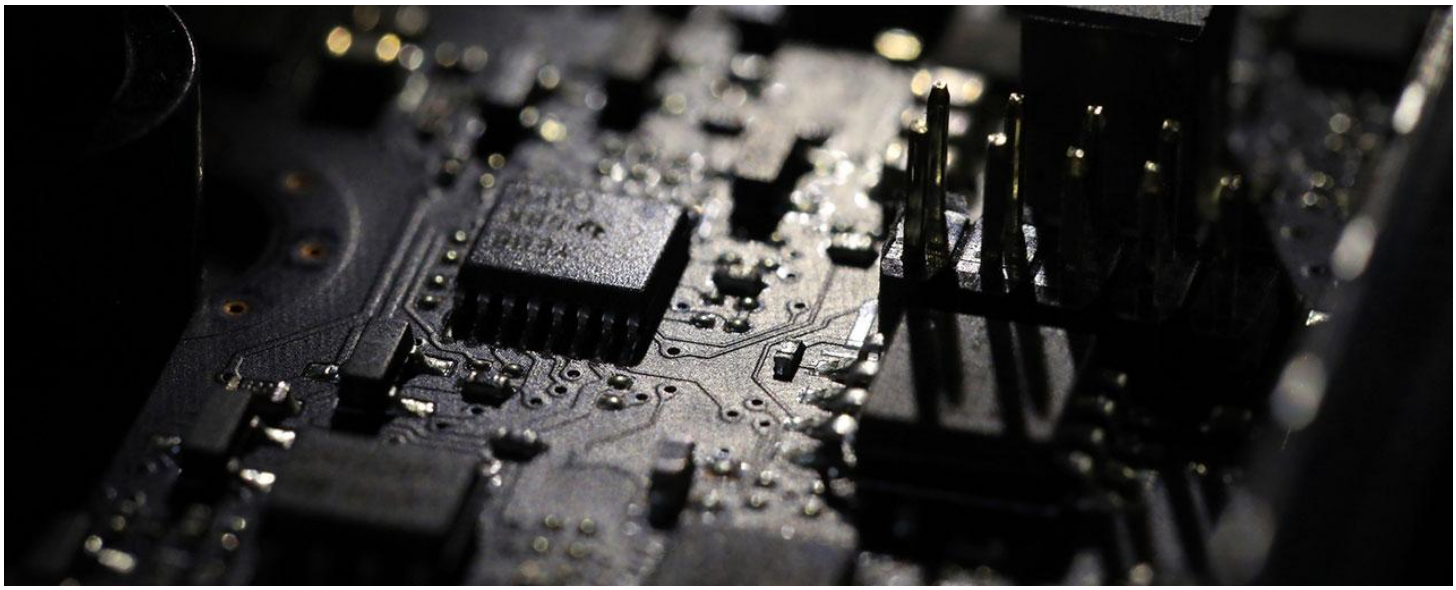

MARCH 14, 2019

BY: Joyce M. Rosenberg

Small businesses can be more vulnerable to cyberattacks than larger companies because they often don't have sophisticated and comprehensive systems to protect themselves from hackers, viruses, malware and what's called ransomware. And owners who are focused on customers and employees may not ensure that their defenses are up to date.

But there are things small businesses can do to improve cybersecurity. Here are six:

— Don't do it alone. Small companies, if they can't afford their own in-house technology experts, should hire consultants who specialize in helping small businesses build and maintain their defenses.

— Think beyond your system. Companies can be attacked through other businesses or computer users including vendors and online storage services. Small business owners should ask anyone who links into their computers about the steps they take to protect everyone's data. "It's not OK to just contract with a firm. It's also doing due diligence," says Diana Burley, a professor at George Washington University's Graduate School of Education and Human Development, whose expertise includes cybersecurity.

— Back up everything. When Marcos Francos' company, Atlanta-based Mighty Clean Home, was attacked by ransomware, his files were rendered inaccessible. But because he had backed up all of his data, he didn't have to pay the ransom demanded by cyberthieves to unlock the files, and he was able to restore his system.

The best way to back up files is on an off-site system that continually creates new versions of all of a company's data.

— Stay current. Software and hardware manufacturers routinely issue updates and what are called patches to improve security. Every device at a small business needs to have all updates and patches downloaded and installed.

— Get an EIN. Owners need to guard against a stolen identity from affecting their business accounts. So instead of using a Social Security number for business, they should have an Employer Identification Number. It's easy to obtain one from the IRS website, www.irs.gov.

— Beware of phishing scams. These are invasions that are often delivered by email with links or attachments. Owners and all employees need to be aware that cyberthieves are sending emails that look legitimate; when the links or attachments are clicked on, destructive malware enters the computer or network. Barry Kelly, CEO of technology consultant Kelser Corp., has training emails sent internally to staffers to help them sharpen their ability to detect phishing emails. That includes Kelly himself.