# Vulnerable to attack: Businesses should boost cyber defenses

13 March 2019, by Joyce M. Rosenberg

Josh Lamont poses for a photo in Menlo Park, Calif., Wednesday, March 13, 2019. A cyberattack that leads to down time and lost data can be costly for small companies. Lamont, whose Social Security number was stolen five years ago when he became a joint depositor on his mother's account, has been taking steps to make his business more secure, among them obtaining an Employer Identification Number from the IRS to be used on business accounts instead of his Social Security numbers. (AP Photo/Jeff Chiu)

When cyberthieves attacked Empire Industries' computer network, technology manager Rich Shemanskis could see files in the process of being infected by malicious software.

"We were looking at the network, and I noticed it, and another guy noticed it. We're looking at the files and watching them change," Shemanskis recalls about the attack three years ago.

Shemanskis told staffers to quickly shut down their PCs, which helped limit the malware's spread, but the company did lose about a day's worth of work. The saving grace for the Manchester, Connecticut, manufacturer of building materials was it had backed up most of its files.

A cyberattack that leads to down time and lost data can be more costly for smaller companies than for larger businesses—an average of $763 per affected computer or other device versus $470, according to a 2018 study by the Poneman Institute, which researches data protection. Many small businesses don't have sophisticated systems to protect themselves from hackers, viruses, malware and what's called ransomware, which renders files inaccessible unless a computer user pays thieves to release them. And many owners aren't tech-savvy enough to anticipate potential problems or don't make use of technology staffers or outside help to strengthen their defenses.

After the attack, Empire reassessed its security. "We already had antivirus protection, but we upgraded everything—we added more layers of security," Shmanskis says.

Josh Lamont, right, laughs with his father Bob at their residence in Menlo Park, Calif., Wednesday, March 13, 2019. A cyberattack that leads to down time and lost data can be costly for small companies. Lamont, whose Social Security number was stolen five years ago when he became a joint depositor on his mother's account, has been taking steps to make his business more secure, among them obtaining an Employer Identification Number from the IRS to be used on business accounts

instead of his Social Security numbers. (AP Photo/Jeff Chiu)

Josh Lamont poses for a photo in Menlo Park, Calif., Wednesday, March 13, 2019. A cyberattack that leads to down time and lost data can be costly for small companies. Lamont, whose Social Security number was stolen five years ago when he became a joint depositor on his mother's account, has been taking steps to make his business more secure, among them obtaining an Employer Identification Number from the IRS to be used on business accounts instead of his Social Security numbers. (AP Photo/Jeff Chiu)

Empire's experience shows why it's critical for small businesses to keep strong defenses against cybercriminals.

"The nature of the threat continues to evolve," says Diana Burley, a professor at George Washington University's Graduate School of Education and Human Development whose expertise includes cybersecurity. Cyberthieves use increasingly advanced technology and develop attack methods that are harder to detect and foil, she says.

A company's computers can be invaded indirectly—a supplier or customer could be attacked and the virus or malware is passed along if computer systems are linked. That's how cyberthieves hacked into the computers of discount retailer Target in 2013—they broke in after first invading the system of one of Target's vendors. Target had to settle legal claims for having not protected customers' information that was stolen.

Smaller businesses are likely to be even more vulnerable, Burley says, adding that "it is the responsibility of the business to be aware that those things can happen."

Sometimes the invasion is more low-tech. Jay Marose, who has a Los Angeles-based publicity business, allowed a longtime friend who was also a client to use his password to access his website-building account. The friend logged into the account after their work relationship ended, took files that didn't belong to him and reversed his payment to Marose. The incident cost the publicist $10,000 and two clients.

Marose realizes that giving the password to someone else was a mistake. But the theft was made easier by the website company's weak security—it didn't use two-factor authentication, which requires a temporary passcode in addition to a password. Moreover, the theft happened during a hurricane and the company was shut down for 10 days; Marose couldn't get any help.

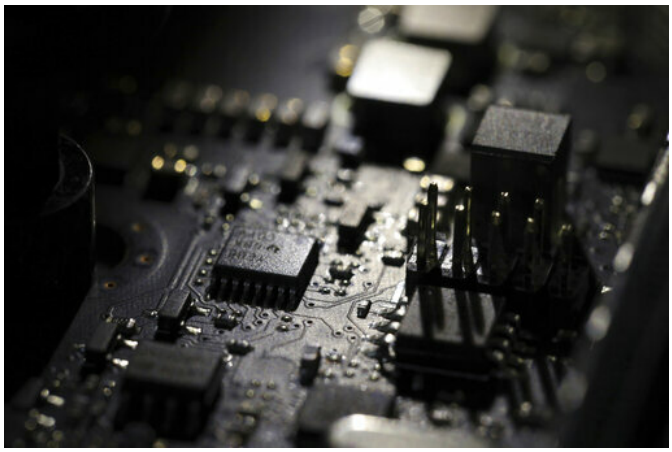
Marose now guards his information closely. "It changed the way I do business going forward," Marose says.

The attack on Amanda Naor's website showed her why it's critical to back up content and data. Naor, who has a photography business in Los Angeles, tried to log into her site early last year but her password was rejected. Technicians at the company that hosted her site found that someone had hacked in and changed the password. Naor created a new password, but a week later was again locked out and her website was completely disorganized—pictures and text were jumbled

haphazardly. She had no backup.

A website security company Naor hired found malware on her site and was able to restore her content. Technicians said she was targeted because cyberthieves develop their skills by practicing on small websites.

"Essentially, I was a playground for a hacker," says Naor. She now has a backup and an ongoing relationship with the security company.



This Feb 23, 2019, photo shows the inside of a computer in Jersey City, N.J. A cyberattack that leads to down time and lost data can be more costly for smaller companies than for larger businesses, an average of $763 per affected computer or other device versus $470, according to a 2018 study by the Poneman Institute, which researches data protection. (AP Photo/Jenny Kane)

When hackers get hold of a small business owner's personal information, the company can suffer. Josh Lamont's Social Security number was stolen five years ago when he became a joint depositor on his mother's account; unbeknownst to the family, her identity had been stolen and the thieves had access to all the information on her accounts. Lamont discovered his accounts had been hacked when a $13,000 charge to an adult website appeared on his credit card. His bank froze his accounts, including those used in his consulting business, while it investigated what had happened.

"I didn't have access to a single account for a good three or more weeks," says Lamont, whose business, JRL Strategies, is based in Menlo Park, California. Moreover, he had to help with the investigation; that cut into his work time.

Lamont has been taking steps to make his business more secure, among them obtaining an Employer Identification Number from the IRS to be used on business accounts instead of his Social Security numbers.

As can often happen when an identity is stolen, thieves struck again 15 months later. This time Lamont got a provisional line of credit.

Last month, Lamont got an email warning that his files would be attacked by ransomware; it turned out to be a hoax.

But, "even as a hoax, it caused missed meetings and a rescheduled pitch to a new client," Lamont says.