At risk?: Equifax hack has businesses uneasy about security

September 27 2017, by Joyce M. Rosenberg

Towne & Country Building Inspection owner Scot McLean looks at his calendar outside his Fox Point, Wis., home Wednesday, Sept. 27, 2017. Towne & Country downloaded several apps to enhance the Google calendar the company uses for customer appointments. In July, McLean noticed some glitches with his Google calendar. McLean's staffer in charge of technology determined that the apps were vulnerable to hacking, and someone was able to log in and erase the appointments. (AP Photo/Morry Gash)

The Equifax breach is reminding small business owners that they may be

vulnerable to cybercriminals.

Companies that provide security and other technology services to small businesses say they've had an increase in calls from customers since Equifax revealed that the personal information of 143 million Americans had been exposed. The hack galvanized some owners into dealing with long-delayed issues.

"A customer called me today wanting to replace their one remaining XP computer," says Bob Herman, owner of IT Tropolis, a tech service company in Fountain Valley, California. Microsoft stopped providing security updates for XP models three and a half years ago.

Small businesses often lag behind big companies in data security, not believing they might be targets. But 61 percent of the victims of breaches in 2016 were businesses with fewer than 1,000 employees, according to a Verizon survey. And experts say small companies are being targeted more because they don't have the sophisticated defenses that big corporations do.

Still, Equifax says its systems were breached after it failed to correctly install a software patch designed to eliminate a vulnerability. Applying patches as soon as they're available and watching for new ones are critical for a company to protect itself, experts say.

But many small business owners, sidetracked by other issues, don't pay enough attention, says Diana Burley, a George Washington University professor whose expertise is internet security. Many don't have staffers or vendors to monitor technology, and no plan to improve their security.

"When you're in a crisis situation is not the time to develop a plan," Burley says.

Small businesses can be harmed by cybercriminals in a variety of ways. Here are some companies' experiences:

FAULTY APPS

Towne & Country Building Inspection downloaded several apps to enhance the Google calendar the company uses for customer appointments. In July, owner Scot McLean noticed some glitches—an appointment might disappear, or show up on another day. The problems persisted for about a week, stopped and started again. Then suddenly, four weeks of appointments vanished.

McLean's staffer in charge of technology determined that the apps were vulnerable to hacking, and someone was able to log in and erase the appointments.

"The hack cost us thousands of dollars in lost revenue," McLean says. Towne & Country was able to recreate part of the calendar, but most of the appointments were lost. Some frustrated customers didn't rebook, turning instead to other inspection services.

The Bayside, Wisconsin company eliminated all apps as well as plugins that added features. It changed its passwords and set up two-step verification, which requires a password and a single-use numerical code to log in.

A WRONG CLICK

Reuben Kats clicked on an attachment in an email nearly a year ago and soon found all the files of his website design business were encrypted and unable to be used. Grabresults.com was the victim of ransomware, or malicious software that hackers plant, hoping to extort money by holding a user's files hostage until they're paid a ransom.

Kats avoided paying because the Los Angeles-based company's files were backed up on a secure online service. Although infected computers can be fixed by returning them to factory condition, erasing all contaminated files, he chose to buy a new one.

Kats realizes the culprit email had a phony address. Now he checks before he clicks.

"I make sure all emails are sent from the actual company domain name," Kats says.

OVERWHELMED BY MALWARE

Hackers got into the website of Hyannis Whale Watcher Cruises in March 2016, just a month before the company's seasonal boat trips were scheduled to start.

When website manager Melissa Marchand called the company that hosts the website, she learned there were 100,000 pages of pornography on the site. This was a crisis: 90 percent of the Barnstable, Massachusetts, company's tickets are sold online.

Marchand contacted a computer security company that began removing malware from the website, a process that took two days. By the third day, the cruise company was selling tickets again. Marchand estimates it took six weeks for the number of visitors to the site to return to normal.

"Fortunately, it was very early in the season. If this had happened in July, it would have been hundreds of thousands of dollars in revenue lost," she says. The security firm now monitors the site, watching for signs of another attack.

HACKING FALLOUT

Small businesses can become victims after hackers invade larger retailers like Target or Staples and steal credit card data, or if information is stolen in other ways. A customer brought a laptop to New York Computer Help in Manhattan for a screen repair and paid with a credit card, signing on an electronic signature pad. That night, owner Joe Silverman got a text from someone else asking why his card had been charged. The card was counterfeit, and Silverman was out $650.

"His credit card, although still in his own wallet, was somehow ripped off by this fake customer," Silverman says.

Silverman says he's careful with emails that likely have phishing links or that ask if he'll do cash transactions, a hallmark of fraudsters. His website has safeguards against credit card crime. After this incident—not the first time he's been a fraud victim—Silverman and his staff are monitoring transactions closely, including sending test charges to card issuers to be sure a card is legitimate.

INSIDE JOB

Managers at Boomsourcing got a notification via one of its software programs in May that someone was trying to access its data without authorization. None of the business software company's information was stolen, but "it woke us up to the vulnerabilities that a small business has," manager David Hyde says.

The Lehi, Utah-based company conducted what Hyde calls "our own NCIS work" using social media to figure out an employee was responsible, trying to use the information to do his own deals. Boomsourcing now uses software that tracks the movements of everyone using its systems.

"If they were to download something they weren't supposed to, we would

know," Hyde says.