No Business Too Small to Be Hacked

By CONSTANCE GUSTKEJAN. 13, 2016

Continue reading the main storyShare This Page

- Share
- Tweet
- Email
- More
- Save

Photo

Paul Eichen at Rokenbok Education in Solana Beach, Calif. Last year, online attackers encrypted its database, making the data unusable. CreditTara Pixley for The New York Times

Just as the holiday shopping season neared, a toy company, Rokenbok Education, was navigating a nightmare situation: Its database files had been infected by malware.

Online criminals had encrypted company files, making them unusable, and were demanding a hefty ransom to unlock the data. Rokenbok, a California-based company that uses building blocks and even robotics to teach children how to think like engineers, lost thousands of dollars in sales in two days.

Rokenbok's founder and executive director, Paul Eichen, was already struggling to adapt his seven-employee company to a fast-changing toy world. Even worse, the malware attack was not Rokenbok's first. The company had been hit earlier with a denial of service attack that shut down the company's website.

"I sweated that one," Mr. Eichen said. "Customers' first impressions are critical."

Focusing on revenue over protection is far from unusual for small companies like Rokenbok. But it is an increasingly dangerous path, experts say. Limited security budgets, outdated security and lax employees can leave holes that are easily exploited by ever-more-sophisticated digital criminals.

The threat to small businesses is growing, some experts say. Sixty percent of all online attacks in 2014 targeted small and midsize businesses, according to Timothy C. Francis, enterprise leader of cyberinsurance at Travelers.

"Smaller companies are easier to hack," said Clay Calvert, director of security at MetroStar Systems, a Virginia-based firm. "They don't have the resources to set up protective barriers." Big companies, which have the financial resources to upgrade their security, have become less vulnerable.

These days, businesses like Rokenbok are especially susceptible to a type of malware called ransomware, which holds data hostage in return for money. Data is slowly encrypted by criminals until the entire system is locked up. The process can take up to 42 days, Mr. Calvert said.

Rokenbok's ransomware attack made its database files unusable. But rather than pay the ransom, the company reconstructed its key systems, a process that took four days.

Although figures are hard to come by, experts say these kinds of attacks can be so damaging to revenue and customer expectations that many small businesses are forced to close after an episode like the one Rokenbok experienced.

And increasingly, as in Rokenbok's case, criminals are going after cash through attacks using ransomware rather than through attacks on credit card data.

"Credit card numbers are harder to monetize," said Christopher Young, general manager of the Intel Security Group at Intel Corporation. "You have

to get the numbers and sell them to someone else before you make money." Ransomware, he said, is high volume and requires no middleman. Hackers gain entry when employees click on malicious links in emails or download infected material.

Phishing attacks, which use malicious emails to steal data, are also on the rise, security experts added.

Given the increase in such attacks, being unprepared is like playing security roulette, said Robert Siciliano, chief executive of IdTheftSecurity.com.

"If you're not deploying some level of security, you'll go under," he added. "You have to make time for quality control. The worst thing you can do is nothing."

Mr. Siciliano recommends a security audit as a first step. The audit should take note of potential areas of risk, like customer data or employee access. "How secure — or not — is your system?" he said.

Strengthening security can be inexpensive and simple — something small businesses can do on their own, experts say. It can include updating antivirus software, adding firewalls and strengthening passwords. Or it can mean putting data in the cloud rather than on company servers, which may be more vulnerable. But often, given lean staffing, it makes more sense and can cost less in the long run to hire a firm that specializes in digital security.

Steven Annese, owner of the lighting and home décor company EliteFixtures, knew he needed tighter security as his business soared. So he outsourced security to a web performance and security firm, CloudFlare.

Mr. Annese uses a checklist to make sure security updates are installed. And he logs onto CloudFlare every day to see what threats have been blocked and to review site analytics.

"So far, we've never been hacked," Mr. Annese said. "Security issues don't keep me up at night."

Among the simpler precautions small businesses and consumers alike can take is to create strong passwords. That has long been the advice of security experts but many say it is stunning how many people and small businesses fail to heed the advice.

Hackers use big-data analytics to help crack passwords, said Mr. Calvert at MetroStar Systems. "They have databases of passwords," he said, "and they analyze how we come up with them."

He recommends using passwords that are 20 characters or longer and that contain a mix of characters. The longer the password, the harder it is to crack.

Password managers, which use software to encrypt passwords, are another option, he added.

The 5050 Skatepark, an 8,000-square-foot indoor park on Staten Island for skateboards, BMX bikes and scooters, rejiggered its passwords after being hit with a denial of service attack last fall that made its website unavailable. The skatepark, which generated $100,000 in revenue in 2014, attracts skateboarders from all over the world, said one of its founders, Edward Pollio. Having the website closed down was a blow to revenue, he said.

“The attack caused havoc,” said Mr. Pollio, who still has a day job as a carpenter. “People were asking if we were still in business. Not having a website is like being closed.”

Now, 5050 Skatepark is more strict about its passwords; it follows longstanding recommendations to use different ones for different accounts, like on Instagram and Twitter. And Mr. Pollio, who helped start the business with $50,000 of his own savings, monitors the site every day.

Employee training is also inexpensive, but important. Since most hacking episodes occur when employees click on malicious links or websites, education is the best defense, many security experts said.

Daniel Peebles, information technology manager at Andretti Autosport, the auto racing group based in Indianapolis, tackles education head on. Besides explaining malware and phishing through PowerPoint presentations, he sends emails to employees about the latest threats.

“You must definitely have a will to learn,” said Mr. Peebles, who served in the Army. “Attackers are always finding new methods. So you’ve got to keep up with the pace.”

Tom Gorup, security operations leader at Rook Security in Indianapolis, advised preaching security to employees from the beginning. He advocates offering monetary rewards for identifying security problems. “Become a guerrilla work force,” added Mr. Gorup, who also served in the Army.

Online security tutorials are helpful and free. They can be found on government sites like that of the Small Business Administration, which also has webinars, and the site of the Defense Security Service, part of the Defense Department.

Once security is in place, experts advise hiring ethical hackers, who test a system by hacking into it to spot vulnerabilities. “And they’re less expensive than being hacked,” Mr. Siciliano said.

Fighting the good fight against online criminals should now be part of any company growth strategy, he said.

Mr. Francis at Travelers said, “Once data is compromised, the ball is rolling in terms of cost.” Banks generally are not obligated to repay money taken from an account. And legal bills aimed at recouping that money can quickly pile up.

Worse, the criminals are hard to track down. They typically operate from office complexes in Eastern Europe or Russia. “It’s their business to hack businesses,” Mr. Calvert said.

Rokenbok reported its malware attack to the local police, who said the F.B.I. was more suited to do the investigation. So far, no one has been arrested in connection with the attack.