CYBERCRIME

How to Prevent Attacks on Your System

By Kerri Fivecoat-Campbell

As a business owner, you have a lot to worry about when it comes to the possibility of crime darkening your doorstep, but one thing many managers do not pay enough attention to is cybercrime—which could disable your entire business and put you at risk for liability.

In a previous issue, we discussed what cybercrime is and why you should be mindful of it; in this article, we aim to help you take steps to prevent it.

"Anyone connected to the Internet will face this common threat," says Bob Bunge, associate professor at DeVry University in Federal Way, Washington.

The risk is very real, but how high your particular risk may be is hard to quantify. Chris Travis, shareholder with Gill Ragon Owen, PA, a law firm in Little Rock, Arkansas, says that in researching cybercrime dealing with self-storage businesses, he has only found three cases since 2007.

One of the cases dealt with the reconstruction of shredded documents that had been discarded in the trash. The papers contained customers' social security and driver's license numbers, as well as banking information. The papers were used to commit identity theft online.

In another case, someone stole customers' files, including lease documents. This case also resulted in self-storage customers being the victims of identity theft.

In the third case, thieves were able to gain access to customers' online records through the self-storage facility.

While the first two cases were in fact cybercrimes (because the thieves stole paper files from the self-storage facilities and used the Internet to steal the customer's identities), the third case is the type of cybercrime that businesses will have to become vigilant against. As businesses rely more heavily on online transactions, owners and managers will have to increase their awareness of how thieves and hackers break into systems.

THE FIVE GENERATIONS OF CYBERCRIME

In order to understand the threats that face business owners and managers today, we should take a look at how they've evolved, says Stu Sjouwerman, CEO of KnowBe4, a cyber-security awareness training company in Tampa Bay, Florida. Sjouwerman explains the five generations of cybercrime:

1. Tech-savvy teenagers spread computer viruses because they could, and because they wanted to show their friends they could. It was mostly annoying and relatively harmless.

2. More malicious viruses like Sasser and NetSky

started causing multimillion-dollar losses to businesses, but were still created, in large part, by teenagers to gain notoriety.

3. Then the true cybercriminals entered the picture. Their goal: to get their hands on easy money through spam, attack websites, and identity theft. The malware used was more advanced, but was still easy to find and easy to disinfect.

4. Coming from mostly Eastern European countries, the next generation of malware bore the mark of the professional. These pros sought larger targets from which more money could be stolen.

5. Cybercrime now specializes in different markets and comprises organized criminal segments that, taken all together, form the full criminal supply chain. Because of this complete supply chain, cybercrime develops far more swiftly than ever before. All the tools are for sale now, and relatively inexperienced criminals can get to work quickly.

Another thing that business managers must understand is the most common way that these cybercriminals will try to get into your computer and create havoc.

One of the most common ways that cybercriminals will hack into your system, says Bunge, is through phishing attacks.

Here's what happens: Cybercriminals will look for email addresses associated with your business address. For example, if your business address is J.Smith@BestSelfStorage.com, the cybercriminals will create an email address from the same business address and send you an email trying to convince you to open either an attachment or a web link. Once you fall for the scheme, you open your computer up to the attacker, revealing any and all information stored on the machine—including your customer's private information (which can be used to steal their identities), as well as your business's banking information.

"These people are sending these messages all day long simultaneously to different businesses," says Bunge. "It's akin in the real world to gangs running door to door trying to get in. If your computer has weaknesses, they will be able to exploit them."

Sjouwerman says the first line of defense in protecting your computer system from attacks is making sure your employees are trained in security awareness.

He offers this guide to preparing a security-awareness training initiative:

• Formulate, and make easily available, a written security policy. Each employee needs to read the document and sign it as an acknowledgment that they understand the policy and will apply it.

• Give all employees a mandatory online security-awareness course, with a clearly stated deadline for completion. It is highly recommended that you explain to them in some detail *why* this is necessary.

• Make this course part of the onboarding process for each new employee.

• Keep all employees on their toes, with security top of mind, via continued testing. Sending a simulated phishing attack once a week is extremely effective to keep employees alert.

• Never publicly identify an employee who fails to respond appropriately to a simulated attack. As a manager, you should address this problem privately with that person. Give a quarterly prize to the three employees with the lowest fail rate.

These procedures are the first line of defense, says Sjouwerman. Once you've created the security-awareness training, you can take measured steps at the system level to help minimize your risk of being on the receiving end of an attack.

The second line of defense is to make sure that you have the best antivirus and firewall protection you can afford. Bunge also suggests having a good working relationship with a local computer guy. "I don't trust a lot of

Legal Advice on Cybercrime

Chris Travis offers these tips for ensuring that you are protected legally from cyber-attacks:

Review your vendor contracts on your software to make sure they have proper encryption security for your business. Also, review the contract to clarify who is liable if there is a breach.

Review your general business-liability policy and make sure it covers you in the event of a cybercrime attack on your business. Many policies do not automatically cover this, says Travis, but many now have cybercrime liability riders or separate policies.

"It's definitely worth it to be aware of the risk and consider your business model and mitigate or insure against the risk," says Travis. "The bad option is to ignore the risk of cybercrime and have it happen to you."

online security products," says Bunge. "Many of them are fraudulent."

Having a good relationship with someone local also means you may not have to wait if you have a problem. If you've ever spent time on the phone with an IT "specialist" in a foreign country when you dial a toll-free number, you know how maddening and time-consuming it can be.

Sjouwerman says part three of your defense is making sure you have protection on your internal network. "There are various software tools that scan the network for attackers, traffic that should not be there, and [offer] many other ways to detect attacks," he says.

Part four is protecting your individual computers. You might do this in a variety of ways.

Bunge suggests that the first and most reliable step in computer protection is making sure you have a separate computer that stores your highly confidential banking and customer information, as well as a separate computer from which you receive and send emails.

"Don't do your personal or business email, or engage in social networking such as Facebook and Twitter, from the same machine on which you do online banking or keep important records," says Bunge. "Keep a degree of separation between your financials and your public and personal communications." If you're not doing email or social networking from the computer on which you do online banking or other business, cybercriminals will have less chance to invade your computer.

Bunge also suggests that you keep your computers up to date. "Business owners and managers like to keep their systems for as long as possible to get as much use from them as they can," says Bunge. "The major threats are known to target older operating systems and browsers."

At the very least, you should make sure that you update your computer regularly with recommended patches and updates from Microsoft or Apple.

It's also very important to make sure your passwords are not vulnerable. Sjouwerman offers these suggestions for protecting your passwords:

- Do not give your passwords to anyone, including tech support, who will almost never need your password to help.
- Don't use simple dictionary words, pets' names, or people's names for passwords. Avoid easy-to-guess numbers.
- Use passwords that are at least 20 characters long. And do not write them down where they can be easily found.
- Create a "pass phrase" instead of just one word.
- Use a different password for each website.
- Change your passwords for sensitive websites (such as your online banking) every 60 to 90 days. Do not use easy-to-guess patterns when you change them.
- If you think someone may have learned your password, change it immediately. Then check the websites where you use that password for any signs of misuse—starting with your online banking site.
- Sometimes websites ask you to enter the answer for a "security question" you can use if you forget your password. Make your answer to the security question just as hard to guess as your password.
- If your bank or webmail offers you extra security features, use them.
- Consider using a password manager such as KeePass or Password Safe. Password managers make your Internet use a lot safer and easier.

By following these suggestions from the experts, you will have already decreased the possibility that your business will become the victim of cybercrime. **N**

Kerri Fivecoat-Campbell is an independent journalist who writes regularly on issues surrounding the environment. She is a member of the Society of Environmental Journalists and writes from her home in the Ozark Mountains.