Cyber Security Recommendations for Small Business

Mike Kokal
Heyl Royster

CYBER-CRIME IS THE FASTEST GROWING CRIMINAL ENTERPRISE ON THE PLANET. Last year, over two billion records were lost or stolen, amounting to a global cost of over $500 billion. That number is expected to quadruple in the next three years. The ultra-sophisticated criminal enterprises and state actors behind these crimes have been reaping profits in excess of the global drug trade. Surprisingly, small businesses with less than 200 employees have been the hardest hit.

According to a report by Keeper Security, 50 percent of small businesses have been breached in the past 12 months. Small businesses make appealing targets to hackers because hackers believe they are less careful about security. Here are 10 recommendations your small business can take to respond to the threat:

1. **Get insurance.** Consider obtaining cyber security insurance. No defense against hackers is foolproof, and if your business is breached, cyber insurance may assist in recovering your losses. (Your general liability policy may not assist you in the event of a cyberattack.) Further, cyber insurance may assist you in notifying your customers in the result of a breach, which is required under many privacy statutes.
2. **Focus on passwords.** Perhaps the easiest precaution you and your employees can take is to pay attention to your passwords. Change them regularly, don't use the same password for multiple accounts, and consider using a secure, offline password manager to keep track of your passwords. Darrell Fortae, cyber security instructor at Lincoln Land Capital City Training Center in Springfield, recommends passwords that are at least 10 characters in length, and for important work and financial information, as many as 16 characters. In addition, consider selecting a password that cannot be found in a dictionary. Use phrases instead of words, and include special characters in the middle of the words. For example, the password "friedgreentomatoes" is not in a dictionary; but "fried77gre@en5tomatoes" or "fri!ed24green7tomatoes" would be even harder for a hacker to decode.
3. **Limit access to information, and limit authority to install software.** Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems they need for their jobs, and should not be able to install any software without permission.
4. **Provide firewall security for your Internet connection.** A firewall is a set of programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled, or install free firewall software available online. If employees work from home, ensure their home system(s) are protected by a firewall.
5. **Keep your software up to date.** Make sure every computer on your network uses the latest versions of all software and security patches/system upgrades. Hackers are continually finding software vulnerabilities, especially those based on Windows. They may discover a so-called "zero-day" exploit, which is not publicly reported or announced before becoming active, leaving software vendors with "zero days" in which to create patches or advise workarounds to mitigate the impact of the exploit. Keeping all security patches and systems up to date, though not perfect, provides a defense to the "zero-day" exploit.
6. **Train employees to recognize malware.** An untrained employee can thwart even the best computer defenses. Your business may use the most effective firewall on the market, but if employees are not trained to recognize a potential spear-phishing attack or malware, your network can still be breached. A phishing attack involves a malicious email sent to any random email account. *Spear-phishing* is more sophisticated, because these emails appear to originate from someone the recipient knows, and may include a subject line or content tailored to the victim's known interests or industry. If the user clicks on a malicious attachment or link, it may allow hackers to access your computer. Fortae recommends training your employees with mock-simulated spear-phishing attacks to help them recognize suspicious emails. Outside vendors can also provide training and software that simulates phishing attacks, which can be helpful for individuals

who might otherwise fail to recognize the mock attack.

7. **Train employees not to use public Wi-Fi.** Public Wi-Fi networks are inherently vulnerable to hackers. Anyone with a cheap wireless router or a device called a "Wi-Fi pineapple" can set one up. Hackers sometimes use this tactic to ensnare careless users and trick them into thinking they're connecting to legitimate access points. To further conceal their ruse, hackers may impersonate the names of known networks, such as those belonging to your local Starbucks or McDonalds. This type of attack is called the "evil twin." If an employee logs into the "fake" Wi-Fi server, it may allow hackers to mount what is called a "man-in-the-middle" attack, which allows them to inspect the data flow between the victim and any resources they are accessing on the web or any computer with which they are networked. Also, keep in mind that server administrators can capture unencrypted data being sent, even on legitimate Wi-Fi networks.
8. **Train employees not to use USB devices from unknown sources.** While USB flash drives are extremely useful for transferring data, they come with substantial security risks if they come from unknown sources. Employees using USB drives at home and plugging them back into the network at work is also a security concern. USB devices can contain infected files that execute and spread malware when opened. For example, the Stuxnet worm that affected Iranian nuclear facilities was allegedly deployed on a USB device. They can also be booby-trapped to emulate a keyboard and take over a Windows-based computer by sending keystrokes as soon as they are plugged in.
9. **Back up critical data.** Ransomware has received a lot of publicity lately. This form of malware is based on encryption software that seeks payment (a ransom) to undo the damage. When the network is affected, the malware typically encrypts all data files, rendering them useless until the ransom is paid. Backing up your critical data remains the best recovery option in surviving a ransomware attack. Backups are best protected when maintained offline from the production environment, as the ransomware can corrupt backup copies.
10. **Recognize that every industry is different.** In Illinois, the Personal Information Protection Act (effective January 1, 2017) requires companies that deal with records containing personal information of Illinois residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." The Act does not, however, specify what constitutes "reasonable security measures." If you conduct business in a regulated industry—such as the healthcare, governmental or financial services sectors—you are likely subject to additional, heightened data-privacy standards from a number of statutes and regulations not mentioned above.

It is critical to determine where your company is vulnerable, and to reasonably address those risks. A qualified law firm can help a small business understand where it may have exposure and help coordinate the above steps into a cohesive loss-prevention strategy reflected in your business policies and procedures. A comprehensive data-security strategy can help protect your business before, during and after a cyber breach. iBi

Mike Kokal is a partner with the law firm of Heyl Royster, a certified privacy information professional (CIPP/US) and a licensed intellectual property attorney. For more information, visit heylroyster.com.