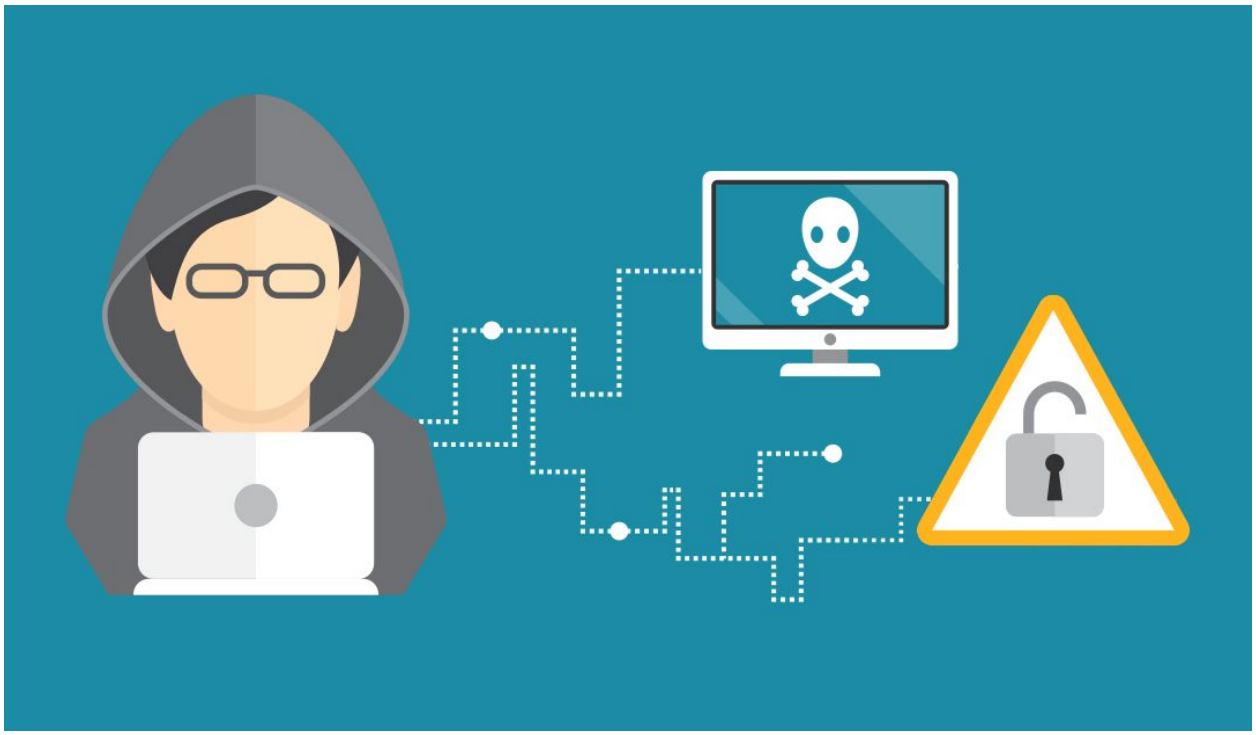
9 Ways to Protect Your Small Business From a Cyber Attack



Datacate, Inc
2999 Gold Canal Dr
Rancho Cordova, CA 95670
855.722.2656 | 916.526.0737
info@datatacate.net | www.datacate.net

Introduction

Your company may be small - perhaps even *very* small - but that doesn't mean that hackers and cyber-criminals are not interested in you. Unfortunately, small businesses are particularly susceptible to hacks and breaches, often because they think they are too insignificant to be targeted, and are unprepared as a result. Consider these actual cases:

- A bandit and his gang of cyber crooks compromised at least 53 small and medium-size businesses over a two-year period, stealing enough data to cause $3 million in damages to the companies, their employees and their customers.
- A company was hacked after its old laptops were stolen in an office break-in; about a month later, funds were siphoned out through fraudulent payroll accounts.
- An employer had the identities of almost all its employees stolen when the hacker gang cracked the company's network security.

By breaking into networks and encrypting businesses' data, some cyber criminals have held companies virtually hostage, demanding a ransom in exchange for the password. A handful of recent statistics highlight the extent of the problem facing small businesses:

- 58% of all cyber-attack victims are small businesses[1]
- Two out of three businesses suffered data loss due to inadequate security in 2018[2]
- Ransomware attacks costs businesses more than $75B per year[3]
- The average ransomware demand is $133,000[4]
- One in four small SMBs were forced to halt operations due to a cyberattack in 2017; over half of those never recovered[5]

1 - Verizon
2 - Quocirca
3 - Datto
4 - Sophos
5 - Malwarebytes

The good news is that small business can defend themselves with a handful of smart strategies. Here are a few ways that you can protect your business from a cyber attack:

1. Encrypt your data.

Whether it's bank routing digits, credit card accounts or employee social security numbers, this type of long-gestating information is what hackers use to steal money. When the data is at rest - which means it is not being actively used at the moment - it should be encrypted to help protect it from breach. Turning on full-disk encryption tools that come standard on most current operating systems is one easy way to do this. However, take note that this encryption applies only when users are logged out of the computer. That means hackers can still attack through viruses and malware while the system is running.

2. Educate your employees.

If a computer on your network becomes compromised, whether the intrusion came from an internal fantasy-football email or through a nefarious Facebook app that an HR administrator clicked on during lunch, your entire operation is at risk. Cyberattacks are becoming more and more sophisticated and it's easy to be fooled by emails, links and attachments that look like everyday business requests but carry dangerous payloads.

The more your employees know about cyber attacks and how to protect your data, the better off you'll be. It may be as simple as reminding them not to open attachments from people they don't know or expect, posting procedures for encrypting personal or sensitive information so they don't forget, or requiring them to change their passwords regularly. Write out a formal company internet policy, setting acceptable and prohibited online activities for employees. For example, prohibit employees from opening email attachments or clicking on links that don't pertain to company business. Or limit personal e-mail access to personal smartphones via the employee's wireless connection, not the company Wi-Fi.

3. Make sure you've got the right partners and platforms.

Do you have a WAF (web application firewall) in place to protect your site? Is your ecommerce platform PCI-DSS (payment card industry data security standards) Level 1 compliant? That will protect you against digital data security breaches across your entire payment network, not just a single card. Does your hosting company have staff that are constantly patching security vulnerabilities, so nothing can attack your website? Is your data continuously protected with rollback capabilities?

4. Secure your hardware.

Data breaches can also be caused by physical property being stolen. If your servers, laptops, cell phones or other electronics are not secure and easy to steal, you are taking a big risk. Security cameras and alarms will help, but for thieves who are not scared off by alarms and motion detectors, physically locking down computers and servers will help even more.

Just looping a metal cable through the computer's Kensington lock port (the small metal loop found on most laptop and desktop devices) to secure it to a desk can tilt the odds in your favor. Removable and external storage devices that have a high “grab and go” factor should be avoided altogether, in favor of off-premises storage or devices that are secured by USB keys or being bolted to racks. Use of mobile device tracking and management software is crucial if your business runs on laptops, tablets and phones.

5. Backup your data

Backup your data several ways, and store the backups off-site in at least two places. Configure backups so that you can do file-level and database-level restores, as well as directories, full file systems and even bare-metal restores of full servers. Schedule regular automatic data backups to maintain the safety of your business information, targeting critical information that changes frequently with more frequent backups.

6. Lock down your network.

Many hacking victims are compromised via Wi-Fi networks, through a technique called "wardriving." In cars outfitted with high-powered antennas, hacker gangs drive around cities, scanning for unlocked or poorly protected networks. Once a vulnerable Wi-Fi hot spot is found, the crooks are as good as in the company's front door, scouring machines on the network for passwords and financial data.

The best defense against exploits like wardriving is to have no wireless network at all. But if your company must have a wireless network, disable the service set identifier (SSID) broadcasting function on the wireless router. This creates a cloaked or hidden network, invisible to casual Wi-Fi snoops and accessible only to users with the exact network name. Be sure you to use the WPA2 encryption standard (currently the latest and strongest standard as of this writing) to protect your Wi-Fi network from intrusion.

Wi-Fi aside, secure your network via a firewall at it’s edge to tightly control inbound access from the WAN (Internet). By minimizing what’s called the “attack surface” via

closing unused ports and blocking any traffic that is not known or authorized, you can minimize the risk of hackers forcing their way into your network via vulnerabilities and exploits.

7. Deploy malware and virus protection.

When wardrivers are successful in cracking a wireless network, they can log in and infect connected computers with malicious software or viruses. But this is just one method; spam emails and harmful websites successfully push malware and viruses to computers all the time. Malware can install code that runs in the background, capturing keystrokes and login information, and relaying it to the hackers. Malware's cousin Ransomware can encrypt all of your company's valuable data, rendering it useless to you, then hold it for ransom. The average ransom demand exceeds $130,000. Properly deployed anti-malware and anti-virus protection on all devices can help protect your company from being victimized.

8. Stay on top of patches and updates.

Frequent updates to operating systems, software, network devices and the like can feel like a pain, but those updates often contain important security patches that address vulnerabilities. Keeping programs and hardware up to date, from upgrading to newer routers and computers to immediately installing browser updates, blocks malicious code that thrives in older equipment and out-of-date software.

9. Hire security.

Though it may seem counterintuitive, small businesses can limit their exposure to cyber criminals by signing on with an Internet-based data-security vendor, especially as the quality of cloud-based business services evolves. Cloud-based providers can offload a lot of the burdens that a small business doesn't have the time or resources to deal with. Hire an outside expert to evaluate your risks and secure your systems and data. Enlisting an outside expert can improve your odds of deflecting an attack.

A solution that is growing in popularity involves moving responsibility for your technology infrastructure to a managed service provider (MSP) that will maintain and secure your company's systems remotely. The MSP will be responsible for backing up your files on its servers, updating firewalls, encrypting data and making sure everything's running smoothly.