CYBERSECURITY

A Short Business Guide

BUSINESS
NEWS DAILY
Small Business Solutions & Inspiration

Cybersecurity

Credit: wk1003mike/Shutterstock

The news often reports on incidents involving large corporations facing massive data breaches where the personal information of millions of consumers was potentially leaked. However, we don't often hear reports about the hacking of small businesses, mainly because these types of attacks aren't public knowledge.

Many entrepreneurs don't realize that small businesses are just as at risk for cyberattacks as larger companies, but they are. According to a report by Verizon, 61 percent of data breach victims were small businesses.

Here's an overview of everything you need to know to protect your business.

In this article…

Why do hackers target small businesses?

While breaches at big corporations, such as Target and Home Depot, make the headlines, small businesses are still very much targets for hackers. Stephen Cobb, a senior security researcher at antivirus software company ESET, said that small businesses fall into hackers' cybersecurity sweet spot: They have more digital assets to target than an individual consumer has but less security than a larger enterprise.

The other reason small businesses are appealing targets is that hackers know these companies are less careful about security. According to Towergate Insurance, small businesses often underestimate their risk level, with 82 percent of small business owners saying they're not targets for attacks, because they don't have anything worth stealing. However, there are several reasons why small businesses are a prime target for cyberattackers.

Ultimately, it's because they're easy to attack due to this complacent attitude and a lack of investment into cybersecurity measures. Since security breaches can be devastating to a small business, many SMB owners are more likely to pay a ransom to get their data back. And finally, small businesses are often the key for attackers to gain access to larger businesses that the SMBs work with.

Types of cyberattacks

In almost every case, the end goal of a cyberattack is to steal and exploit sensitive data, whether it's customer credit card information or a person's credentials, which is then used to manipulate the individual's identity online.

This is by no means an exhaustive list of potential cyberthreats, especially as hackers' techniques evolve, but businesses should at least be aware of the most common types of attacks.

Phishing: Perhaps the most commonly deployed form of cybertheft, phishing involves collecting sensitive information like login credentials and credit card information through a legitimate-looking (but ultimately fraudulent) website, often sent to unsuspecting individuals in an email. Spear phishing, an advanced form of this type of attack, requires in-depth knowledge of specific individuals and social engineering to gain their trust and infiltrate the network.

Inside attack: This is when someone with administrative privileges, usually from within the organization, purposely misuses his or her credentials to gain access to confidential company information. Former employees, in particular, present a threat if they left the company on bad terms. Your business should have a protocol in place to revoke all access to company data immediately when an employee is terminated.

Password attacks: There are three main types of password attacks: a brute-force attack, which involves guessing at passwords until the hacker gets in; a dictionary attack, which uses a program to try different combinations of dictionary words; and keylogging, which tracks a user's keystrokes, including login IDs and passwords.

APT: Advanced persistent threats, or APTs, are long-term targeted attacks in which hackers break into a network in multiple phases to avoid detection. Once an attacker gains access to the target network, they work to remain undetected while establishing their foothold on the system. If a breach is detected and repaired, the attackers have already secured other routes into the system so they can continue to plunder data.

DoS: An acronym for distributed denial of service, DDoS attacks occur when a server is intentionally overloaded with requests until it shuts down the target's website or network system.

Malware: This umbrella term is short for "malicious software" and covers any program introduced into the target's computer with the intent to cause damage or gain unauthorized access. Types of malware include viruses, worms, Trojans, ransomware and spyware. Knowing this is important for choosing what type of cybersecurity software you need.

Ransomware: Ransomware is a type of malware that infects your machine and, as the name suggests, demands a ransom. Typically, ransomware either locks you out of your computer and demands money in exchange for access or it threatens to publish private information if you don't pay a specified amount. Ransomware is one of the fastest-growing types of security breaches.

Security solutions and what to look for

There are a few different basic types of security software on the market, offering varying levels of protection. **Antivirus** software is the most common and will defend against most types of malware. For a side-by-side comparison of the best

antivirus software programs for small businesses, visit the site business.com or www.toptenreviews.com.

Firewalls, which can be implemented with hardware or software, provide an added layer of protection by preventing an unauthorized user from accessing a computer or network. Most modern operating systems such as Windows 10 come with a firewall program.

It is advisable that businesses invest in three key security solutions. The first is a **data backup solution** so that any information compromised or lost during a breach can easily be recovered from an alternate location. The second is **encryption software** to protect sensitive data, such as employee records, client/customer information and financial statements. The third solution is **two-step authentication** or **password-security software** for a business's internal programs to reduce the likelihood of password cracking.

Remember, there's no one-size-fits-all security solution, so Charles Henderson, global head of security threats and testing at IBM, advised running a risk assessment, preferably through an outside firm.

Cybersecurity insurance

One important solution that doesn't involve software and that many small businesses overlook is cybersecurity insurance. As mentioned above, your general liability policy will not help you recoup losses or legal fees associated with a data breach. A separate policy covering these types of damages can be hugely helpful in case of an attack.

According to a survey by insurance company Hiscox, only 21 percent of small businesses have some form of cyber insurance, with 52 percent indicating that they have no intention of acquiring any.

Tim Francis, enterprise cyber lead at Travelers, a provider of cyber insurance, said many small businesses assume cyber insurance policies are designed only for large companies, because those businesses are the most frequent targets of hackers. But many insurance carriers are beginning to offer tailor-made coverage for smaller companies to meet their budgets and risk-exposure levels, he said. **In Kenya** small companies can get **cyber insurance** from **AIG Insurance, Dawiti Insurance Agency, BRITAM** and **AON Kenya**.

Francis advised business owners to look for a combination of first– and third-party coverage. First-party liability coverage includes general costs incurred as a

result of a breach, such as legal expertise, public relations campaigns, customer notification and business interruption. Third-party coverage protects you if your company is at the center of a breach that exposed sensitive information. This type of protection covers legal defense costs if the affected parties sue your company.

“Coverage is more than words on a page,” Francis said. “Make sure your carrier is well regarded financially and has a good reputation in the industry. There’s tremendous variety in policies, [and] … you need an agent who understands the differences.”

Best practices for your business

Ready to protect your business and its data? These best practices will keep your company as safe as possible.

Keep your software up to date. As stated in this Tom’s Guide article, “an outdated computer is more prone to crashes, security holes and cyberattacks than one that’s been fully patched.” Hackers are constantly scanning for security vulnerabilities, Cobb said, and if you let these weaknesses go for too long, you’re greatly increasing your chances of being targeted.

Educate your employees. Make your employees aware of the ways cybercriminals can infiltrate your systems, teach them to recognize signs of a breach, and educate them on how to stay safe while using the company’s network.

Implement formal security policies. Putting in place and enforcing security policies is essential to locking down your system. Protecting the network should be on everyone’s mind since everyone who uses it can be a potential endpoint for attackers. Creating a culture of caution and preventive practices will bolster your protection. Regularly hold meetings and seminars on the best cybersecurity practices, such as using strong passwords, identifying and reporting suspicious emails, and clicking links or downloading attachments.

Many companies enforce password policies that require employees to follow strict standards for creating passwords, such as including numbers, both uppercase and lowercase characters and symbols, as well as never using the same or similar passwords for different applications

Practice your incident response plan. IBM’s Henderson recommended running a drill of your response plan (and refining, if necessary) so your staff can detect and contain the breach quickly should an incident occur.

Ultimately, the best thing you can do for your business is to have a security-first mentality, Henderson said. He reminded small businesses that they shouldn't assume they're exempt from falling victim to a breach because of their size.

About Us

Whether it's a food truck or a fashion line, a coffee shop or a consulting firm, Business News Daily's goal is to help entrepreneurs build the business of their dreams and to assist anyone working in a small business make smart decisions about products, services and ideas. Our reporting style is simple: We seek insights and advice from experts and then stick to the basics by bringing you concise, actionable information business owners can use to make the daily decisions required to start and grow their businesses.

Mission Statement

To provide the ideas, inspiration and solutions needed to help entrepreneurs and small business decision makers succeed.

To learn more visit our website and follow us on social!