White Paper
8/15/2018

Small Business Guide to Cyber Security

According to a government study about IT security in businesses, almost two thirds of small businesses experienced a cyber security breach in 2015, with costs surpassing $150,000 in the worst cases. Nonetheless, no modern business can hope to survive without taking advantage of the benefits afforded by technology.

A severe cyber attack can bring any business to its knees, particularly businesses that are heavily reliant on digital marketing and other IT resources. There's no doubt that cyber security has become a major concern among both consumers and businesses of all sizes. The threats are great, and they are becoming increasingly smarter and diversified. As such, your entire team needs to be made aware of the various threats to the business, its employees and its customers.

Why Hackers Target Small Businesses

Although you usually only hear about cases involving big international companies in the headlines, hackers frequently target small businesses for a number of reasons. Contrary to popular belief, small businesses are actually among the most popular targets for cybercriminals. As far as those with nefarious intentions are concerned, a small company likely is less likely to have invested in the latest and most expensive security measures unlike a larger enterprise. At the same time, any business is likely to have more valuable digital assets than the average consumer, making the small business somewhat of a sweet spot for hacking opportunities.

It is also important to remember that a hacker might not target a specific small business, but rather a whole group of businesses in a broader initial attack while trying to find the most vulnerable targets. Hackers typically use a variety of malicious to carry out these wide-reaching attacks, and if your business is among them, you'll be left open to far more severe consequences.

While large enterprises usually invest enormous amounts of money and human resources in guarding against the myriad of potential security threats, small businesses often have comparatively weak online security. A lack of suitable encryption technology, for example, can lead to vast amounts of sensitive data falling into the wrong hands.

Depending on your target market, your business may be an even more enticing target than most. For example, if you're a business-to-business industry or one that sells luxury and expensive goods to consumers, you'll likely be dealing with far larger transactions than a typical high-street venue. Hackers target such businesses in the hope of intercepting the personal and financial information of your customers, the results being vast financial loss as well as many extremely angry customers.

Understanding the Threats
The vast majority of cyber attacks share the same goal of stealing and exploiting sensitive information. In less severe cases, hackers may gather information for unscrupulous advertising and spamming purposes, while more severe attacks involve stealing financial information. A less common goal is simply to disrupt business operations for the purpose of making a statement. For example, a disgruntled former employee or customer might be out to wreak havoc for a business for no other reason than their own satisfaction. Nonetheless, the goal of a cyber attack is rather irrelevant, since any attack presents the potential of disastrous consequences for your business.

When people think about cyber security, they usually think of malicious software and the antivirus programs designed to guard against it. In reality, the issue is far more complex, and choosing the right security solutions is only a part of the battle. Small businesses also need to educate their employees on the various threats, since there's no substitute for common sense and getting into a few good security practices rather than relying solely on the latest and greatest IT security solutions. Cyber attacks come in many different forms:

Malicious Software
Malicious software, commonly referred to as malware, acts as a tool to aid a hacker in the vast majority of cases. Less serious forms of malware include adware and spyware designed to collect personal information for the purposes of advertising, while the most dangerous types are designed to steal more sensitive information, such as a bank account or credit card details. Hackers may also use rootkits designed to access your business's IT resources remotely for the purposes of spreading other forms of malware. Another common type is the computer worm, which works by exploiting vulnerabilities in the operating system and other software to slow down your network and consume bandwidth. Among the most dangerous of all malware are Trojan horses and keyloggers, since they afford attackers full access to your computer systems, even to the extent of recording every single keystroke to record passwords and payment information.

Advanced Persistent Threats
APTs are highly sophisticated cyber attacks carried out over several stages to break into a remote network while avoiding detection to gather personal or financial information over an extended period. The first stage of such attacks involves reconnaissance, whereby a hacker will typically target a broad range of small businesses to find the most vulnerable ones. The hacker will then exploit the vulnerability by delivering malware to the remote system while candidly capturing information. APTs can go on for weeks or even months while hackers lay low to avoid detection while coming up with a sophisticated plan of attack that only comes to light once it is much too late.

DDoS
Hackers don't always carry out attacks for fraudulent reasons. Instead, their goal might be to disrupt your business operations for the purposes of revenge, blackmail or even activism by preventing access to certain services. A distributed denial of service (DDoS) attack is the most common method used to achieve these goals, and they're constantly becoming more powerful and more sophisticated. For example, major video game developer Blizzard Entertainment experienced a major DDoS attack during the launch of its much-anticipated Warlords of Draenor

title in November, 2014, causing connection issues for millions of players over the course of a week. In its simplest form, a DDoS attack works by overloading a remote server with more queries that it can handle, causing it to crash and the services relying on it to become unavailable to users.

Phishing

Phishing is one of the most dangerous of all cyber security threats, and it's constantly on the rise. Phishing relies on collecting sensitive information, such as passwords or payment details, by duping the user into voluntarily giving them away. Common phishing scams come in the form of things like legitimate websites or emails, and they're constantly getting more sophisticated. For example, an email might look like it's from a genuine source, perhaps even a business that you're a customer of, only to ask you for your personal or financial information and use it for nefarious purposes. In other cases, a phishing scam, masquerading as an email or website from a known and respected organization, may exist to dupe users into downloading malicious software. Although the vast majority of phishing scams are quite obvious, others are cleverer and more effective.

Customer scams using social media have also become a major concern in recent years. Social media has become an essential marketing tool for businesses of all sizes, but it's also particularly vulnerable to scammers. For example, information thieves might attempt to gather sensitive data by posing online as customer support representatives of your company in a similar manner to other phishing scams.

Employee Negligence

Sometimes, the biggest threats to your business come from within. While your employees are obviously an essential asset to your business, they can also be its weakest link. Employees who are not adequately trained concerning cyber security threats and how to deal with them are far more likely to download potentially malicious attachments and other software or leave the computer vulnerable to an inside job. For example, many employees leave their computers unattended, potentially allowing anyone else in the area to get unauthorized access without even having to make an effort. In other cases, employees working from home or on the move may connect to unsecured wireless hotspots where snoopers may be able to collect the unencrypted data being sent between their computer and the local router.

Common cyber security Mistakes

While larger companies are more likely to have the financial resources and expertise to overcome security breaches quickly and efficiently, small businesses must prioritize the defence of their systems in order to minimize the risks. Simply having fewer resources at your disposal is no excuse for neglecting cyber security, and you'll need to educate yourself and your team appropriately and avoid some of the common mistakes that can leave your business open to an attack. Following are some of the most common mistakes to avoid:

- **Thinking You're Protected**
  Small businesses often make the grave mistake of assuming that their insurance policies will bail them out in the event of a severe security attack. While your insurance company might pay out for any physical damages or immediate losses, you probably won't be

covered for any longer-term repercussions. For example, if your business falls victim to a cyber attack that claims the personal or financial information of your customers, you will need to be transparent about it to have any hope of recovering your reputation. Nonetheless, many customers will never trust you again, no matter what you do, and your business will inevitably suffer as a result.

- **Not Having a Contingency Plan**
  No matter how well-protected your business might be, you must always plan for the worst. According to a survey conducted in 2015, around 80% of small businesses had no response plan in place, in spite of the fact that most of them had already suffered a security breach. A cyber security plan should take into account three key areas: prevention, resolution and restitution.

- **Not Educating Your Staff**
  Even if you've invested in the most powerful cyber security tools available, there is no substitute for staff awareness. Every business, no matter how small, should have an IT security policy in place that outlines the best practices to adopt as well as the common mistakes to avoid. The growth in popularity of mobile devices and bring-your-own-device (BYOD) policies makes it doubly important to spell out your security policies and make certain that everyone follows them. Likewise, you should monitor your team to a degree, even in the case of a small and close-knit business community where you might assume that none of your employees would ever dream of deliberately causing a security breach.

- **Not Keeping Your Systems Up-to-Date**
  Small businesses, with their relatively limited financial resources, often end up using deprecated hardware and software, potentially leaving themselves open to a wider range of cyber attacks. In the constant battle between software developers and cybercriminals, both parties are always finding new weapons to keep up the equilibrium. As such, Microsoft and other major IT firms regularly release updates or even entirely new editions of their products to overcome security flaws. Older operating systems, such as Windows XP, for example, are no longer supported, allowing hackers to take advantage of major security holes. Nonetheless, zero-day threats are also a major issue that developers need to stay on top of to block any potential security threats as soon as they arise. All businesses should keep their software systems updated, even if it does mean spending a significant portion of their budgets.

- **Not Investing in Security Software**
  By far the biggest mistake is not having any cyber security solutions in place at all. Any modern company, particularly one that carries out much of its business online, must invest in robust security solutions. While the basic built-in security systems, such as Microsoft's Windows Defender might offer adequate protection for consumers, they still leave a lot to be desired for major targets such as small businesses. The most important systems to protect are point-of-sale systems, since they are inherently more open to security threats, potentially allowing criminals full access to customer data. However,

your business should perform regular security testing and scanning of *all* of its systems, including databases, networks, applications and cloud services.

A 10-Step Plan for Securing Your Business

Your cyber security plan is central to safeguarding your business from the multitude of threats out there. To summarize what you've learned from the above, here are the 10 key steps to making your business safer for you, your employees and your customers:

1. Educate your employees by way of a staff training program that covers security policies concerning the acceptable use of your company's IT resources. Your main goal should be to raise awareness of the various types of threats and how to combat them.
2. Develop and maintain a policy for any employees who bring their own devices to work or conduct business operations using mobile devices (either their own or those of the business). In particular, ensure that proper monitoring and security controls are in place at all times.
3. Update and maintain your company's IT resources. If you're using any deprecated operating systems or other outdated software, you should prioritize their replacement. Alternatively, you may want to consider migrating to cloud-based services that are always kept current.
4. Install malware protection on all of your company computers and other devices. For best results, choose a security platform designed for business use that offers heuristic scanning and guards against zero-day threats. Maintain a schedule for regularly scanning all of your systems.
5. Improve the security of your network by filtering out unauthorized access attempts. You'll need to use a firewall to limit exposure of your IT resources to the wider world. All modern operating systems include a software-based firewall, although hardware alternatives provide greater protection.
6. Create and manage secure user accounts for all of your employees and the devices they use. For each account, manage access rights to ensure that people only have access to the system settings and data that they actually need to carry out their work.
7. Configure removable media controls to reduce the risk of malicious software getting onto your company's devices from USB flash drives and other removable disks and devices. Limit the types of removable media people are allowed to use, and make sure everything is scanned before use.
8. Establish a monitoring strategy whereby you keep a close eye on all activity across your network and connected devices. However, while you can use more exhaustive technologies, such as keyloggers, you need to find the right compromise between security and breaching your employees' privacy.
9. Invest in a suitable data backup solution to keep all important information securely stored in the event of a security breach or system failure that claims your data. Automated data synchronization services can make backup easier, and you may want to consider cloud storage solutions too.
10. Build an incident response and disaster recovery plan to minimize the impact of any cyber attacks that do manage to break through. For best results, you should have a dedicated member of staff with specialist training who can help restore your compromised systems.

While the above steps will help set you on the right track to building a secure information protection plan, you'll also need to consider it an ongoing regime. As such, you'll need to

regularly review your business's security practices and protocols and keep your team informed at all times.

Final Words

It's never too early to start implementing a cyber security routine, and while it might be a time-consuming and expensive activity, the consequences of suffering a cyber attack can cost your business dearly. You owe it to yourself, your employers and your customers to ensure that all personal, financial and any other sensitive information is kept safe at all times.