AnchorFree

Hotspot Shield: *Security. Privacy. Access.*

How to Protect Your Business from Cyber Attacks

As a small business owner, you might not worry about cyber-attacks as much as larger corporations do. However, you would be making a grave mistake if you are not taking proper measures to protect your business against cyber-attacks.

Criminals are increasingly targeting smaller businesses since most small businesses are easier targets. In their latest annual Internet Security Threat Report, Symantec found that 31% of all targeted attacks are aimed at businesses with less than 250 employees.
Such attacks can be incredibly costly for small businesses in terms of the financial loss, loss of valuable data, disruption of services, damage to reputation, and time involved to resolve issues related to a security breach incident.

According to a 2013 Small Business Technology Survey that polled 845 small business owners across industries in the U.S., “The average cost associated with the cyber-attack, among those targeted, was $8,699.48.”

In addition, nearly half of all small business owners surveyed claimed to have at one time been the victim of a cyber-attack.

Types of Information and Data that Cybercriminals Target

Whether your business is a restaurant, retail shop, e-commerce site, or an engineering service firm, your business is a potential target for data theft if your business contains or processes the following types of information:

- Intellectual Property (trade secrets & sensitive company information)
- Your customers’ names and information (name, address, age, credit card numbers, SSNs, etc.)
- Credit card or financial information
- Medical records
- Email and social media account details

- Merger and Acquisition data

All of the above data is valuable to cybercriminals. According to the report by Verizon, the vast majority of cyber-attacks are financially motivated.

Cybercriminals may steal your banking credentials to steal your money. They may sell your sensitive information or trade secrets to others.

A security breach incident can also quickly wipe out your customers’ confidence. Thus, it’s paramount that you have the security measures in place to protect the above sensitive information and data.

Methods Used By Cybercriminals to Attack Your Business

The methods used by cybercriminals to infiltrate your data systems are numerous and becoming increasingly more sophisticated.

Hacking and malware are the preferred methods used by criminals. The table below provides a summary of the most commonly used tools by hackers:

Other methods may include:

- **Social engineering** – Social engineering is the use of psychological techniques to manipulate people into revealing confidential data or personal information.

  Cybercriminals using social engineering might email you, friend with you on Facebook and chat with you, or call you pretending to be your bank. Social engineering is one of the most difficult risks to defend against.

- **Phishing Emails** – Sending phishing emails is one of the most common methods used by cybercriminals. The emails are usually sent to a large numbers of recipients.

  The email address may appear to come from someone you know or from a well-known and trusted organization (i.e. your bank, your ISP) or website. The message usually contains a link to a fake web page that asks you to verify your information or provide your personal information, including credit card numbers, social security numbers, passwords, and banking information.

  The link could also contain a keylogger malware, which would enable the criminal to record keystrokes. So when you log in to your banking site or other sites to conduct your business, your usernames, passwords, as well as answers to your secret security questions will be recorded by the criminal.

- **Fake Antivirus programs** – Fake antivirus programs are a form of malware. It appears on your computer screen as a pop-up, with a warning that your computer is infested with lots of viruses. If you click on it, it may load malware onto your computer.

Actors behind Data Theft

According to the Verizon's 2013 Data Breach Investigations Report, external actors account for 92% of the data breaches and insiders are responsible for 14% of the cases.

Besides the hackers and cybercriminals, other actors such as disgruntled employees, business partners, or competitors may also steal your data and confidential information.

How to Protect Your Business

It is a fact that highly skilled and motivated criminals can find ways to crack through your defense. But you can still make your business less vulnerable and less appealing to the attackers by implementing layers and layers of security measures.

Many times, cybercriminals would rather go for the low hanging fruits, which are the businesses that have weak defenses.

According to the Verizon report, "75% of the attacks were opportunistic" and "78% of the intrusions took little or no specialist skills or resources."

In this guide, we will discuss the security measures you can implement to protect your business' data and information. By implementing a layered security strategy, you will make your business a lot more difficult for cybercriminals to steal your information.

1) Conduct a Security Risk Assessment

Doing a risk assessment is an important 1st step toward protecting your business. The following should be assessed:

- What data and information do you store, process, or transfer? Which of those data are confidential and must be protected?
- Where do you store those data?
- Who has access to those data?

- What security measures (hardware & software) and controls have been put in place to protect your data and prevent a cyber-attack?
- What security protocols are currently in place to deal with lost or stolen data?
- What if an employee leaves your company?

Once you have completed the risk assessment exercise and have identified the risks and vulnerabilities, the next steps are to implement the necessary security measures to minimize or eliminate those risks and vulnerabilities.

2) Keep Computers Up To Date

One of the easiest strategies you can implement in order to prevent cybercriminals from hacking into your systems and stealing sensitive information is to simply make sure your company's computers are up to date.

This means paying attention to notifications about security updates and patches to your operating systems, firewalls, web browsers, application software, and other third-party plugins. As soon as you see the notifications appear, you should promptly make the updates.

When you ignore these notifications and postpone following through with security updates, you're willingly leaving cracks in your security defense system.

3) Secure your Wireless Router

Wireless routers shipped from the same manufacturer share the same default credentials. Additionally, they are incredibly easy to crack. If you haven't already done so, you should change the default password now. Refer to a later section to learn how to create a strong and secure password.

In addition to changing the default password, you should enable WPA2 encryption to secure and encrypt your wireless connection. Do not use WEP encryption or even WPA (without the 2) as they have been shown to be easily crackable.

4) Protect Your Network with a Software or Hardware Firewall

A firewall prevents unauthorized access to an individual computer or network of computers. They are used mostly as a first line of defense to protect your device or network from online threats such as hackers, viruses, Trojans, and worms.

Every time you are connected to the Internet, your computer is exposed to all sorts of dangerous programs and malicious people that want to infiltrate your computer to steal your personal information, send spam emails to your inboxes, or use your computer to launch attacks on other computers.

A good firewall system blocks attackers from trying to infiltrate your system and prevents your data and information from flowing out to attackers.

A firewall can be implemented using either software or a separate physical device (usually for large networks) or a combination of both.

- Hardware firewalls are built into the routers. They are designed to protect all the devices connected to a network. It is recommended that you get someone who is familiar with configuring hardware firewalls to correctly configure the hardware firewalls for you.
- Software firewalls are included in Microsoft operating systems such as Windows XP, Vista, 7, and 8 and it is turned on by default. Window's firewalls generally provide less protective features than those purchased from antivirus vendors. One notable feature missing from Windows has been two-way controls to restrict what travels out from your device as well as what comes in.

Firewalls made by internet security companies can provide two-way protection and may also block malware and other malicious programs.

5) Keep Your Antivirus and Anti-Malware Programs Up to Date

Antivirus and anti-malware programs are used to prevent, detect, and remove malware from computers. Hackers and criminals are constantly developing and releasing new viruses and malware.

In order to prevent computer viruses, Trojan horses, worms, keyloggers, and other forms of malware from attacking your computer, it's essential that you keep your antivirus and anti-malware programs up to date with the latest definitions.

According to reports, Google flags somewhere around 10,000 sites each day that it deems unsafe for users to visit. Without the constant use of antivirus software, your machines are vulnerable to dangerous malware and cybercriminals looking for opportunities to hack into unprotected computers.

6) Use Strong Passwords For Everything

According to the Verizon's 2013 Data Breach Investigations Report, "authentication-based attacks (guessing, cracking, or reusing valid credentials) factored into about four of every five breaches involving hacking in our 2012 dataset."

Security experts estimate that if the password you use can be found in a dictionary (like the word "password" for example), it can be hacked in roughly thirty seconds. In an article titled, "*How to Devise Passwords That Drive Hackers Away*," author Nicole Perlroth writes, "A password should ideally be 14 characters or more in length if you want to make it uncrackable by an attacker in less than 24 hours."

Additionally, the password should use a combination of upper and lower case letters, numbers, and symbols.

Because longer passwords tend to be harder to remember, consider a passphrase, such as a favorite movie quote, song lyric, or poem, and string together only the first one or two letters of each word in the sentence.

It’s also important that you use different passwords for every site or account you have (Facebook, PayPal, email, etc.). If you have to keep an account of your passwords, don’t store them in places that could easily be found (like your email inbox, on your desktop, or on a sticky note).

If you want to use a tool to help you manage all your passwords, you can try LastPass or 1Password. By using these tools, you only have to remember one secure password, which you use to unlock the tool.

7) Manage Your Data on the Cloud

If you are storing your company’s sensitive data and information on the cloud, you should know what data is stored in the cloud, how your data is managed, and what security measures are in place by your cloud provider to protect your data.

8) Hire a Security Consultant and Have Them Perform an Audit

Hiring a security consultant to find security flaws in your systems might sound expensive, but it’s a valuable service that can save you a lot of headaches and money down the road. It is for this reason that companies like Facebook have developed programs that reward security researchers and other “white hat hackers” for finding and informing them about potential security risks.

With over 1.11 billion people using the social networking site each month, the company takes great measures to protect a huge amount of private data and information. As a small business owner, it’s important that you make similar investments in order to prevent costly cyber-attacks.

9) Train Your Staff on Basic Security Principles

According to the website CyberFactors.com, in-house employees are responsible for 40 percent of small business breaches. If you have employees, you need to spend time training and educating them on basic security principles and how they can help prevent cyber-attacks.

George Westerman, a research analyst in the MIT Sloan School of Management's Center for Digital Business, recommends the following:

- Train your employees on IT risk – Hire security consultants to educate your employees them on the different methods and schemes used by hackers, make them aware of social engineering schemes, phishing emails, and teach them how to protect their personally identifiable information.

- Create clear and simple company policies and guidelines regarding technology, password, and email security – Make sure your have clear policies regarding the use of personal devices and USB drives, download/installing software to company's devices, using social media sites and IM/chatting programs, password creation, email security, and how to protect company's data and information.

  Downloading/installing unauthorized software from unknown sources and connecting infected personal devices to company's network could introduce destructive malware into your company's network.

- Put somebody in charge of security.

For more details on each recommendation listed above, click here.

10) Use a VPN Service When Accessing the Internet at Public Networks

Your laptop and mobile device probably contain some confidential information and data that you wouldn't want stolen. But if you happen to access the Internet at places with weak wireless security (Public WiFi networks at coffee shops, hotels, and airports are inherently unsecured), you are vulnerable to attacks from hackers.

Without strong security measures in place, a hacker can easily get access to the data and information on your computer using various methods. The best way to protect the data and information going in and out of your device when accessing the Internet via WiFi is to use a VPN service.

A VPN service encrypts all your internet communications, thereby preventing anyone from tracking your internet activities and stealing personal and sensitive information going in and out of your device.

What to Do Next?

By following the tips presented in this guide and implementing a layered security approach, you will greatly enhance your business' ability to protect your data and information.

Below are some additional resources to provide you with more information:

- Verizon 2013 Data Breach Investigations Report
- Security: Malware, Hacking Remain Preferred Methods of Cyber
- 5 Ways For SMBs To Boost Security But Not Costs
- A Short Primer for Developing Security Policies