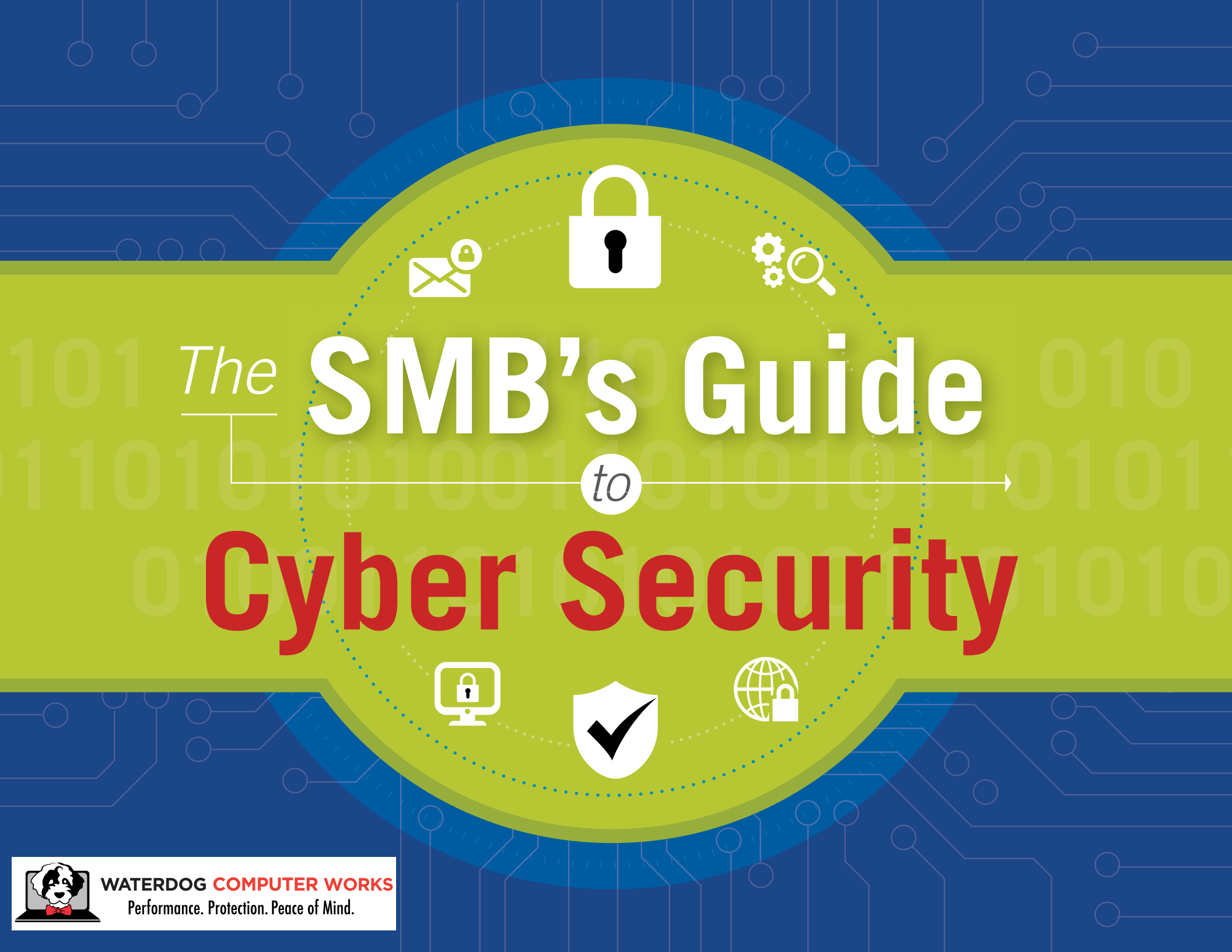


WATERDOG COMPUTER WORKS
Performance. Protection. Peace of Mind.

CONTENTS

Introduction

With massive data breaches making headlines on a regular basis, it's hard to ignore the fact that data security is becoming increasingly important. Unfortunately, there are still far too many SMBs that don't understand just how serious the threat is—and that can be dangerous.

Growing threat to SMBs

Recent research demonstrates that the growing cybersecurity threat isn't a trend that only affects big, national companies. It's just as serious—if not more serious—for small businesses to be prepared because data breaches and cyber attacks are very real possibilities for them. According to Ponemon Institue's 2017 State of Cybersecurity, cyber attacks affected 61 percent of SMBs in the past 12 months,[1] and the number of data breaches reported each year continues to climb. If that's not alarming enough, these companies on average lost more than 9,350 individual records as the result of a breach.[1]

Educate yourself and your employees

Knowing what you're up against is half the battle. As the owner of a small- to medium-sized business, you need to learn about current cyber threats and what you can do to protect your organization. Then, share that information with your employees so they understand why cyber security is important and how they can contribute to keeping the company safe.

Security is all about protecting data and preventing data loss. That used to mean protecting your data from fire, floods, and user error. Now cyber security is an even bigger threat than those more traditional dangers, and you need to make sure you're prepared. After all, the survival of your company could depend on it.

Cybersecurity Tip:
Use good judgement to protect yourself from social engineering and phishing attacks. Don't open emails from untrusted sources, and if you see an email that looks like it's from a contact but seems suspicious, give them a call rather than responding via email.

Common cybersecurity mistakes

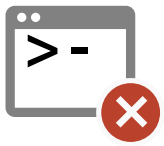
Bad habits are hard to break, and that's especially true when it comes to small businesses and cyber security. After all, it's easy to think "that will never happen to me," and let things slide that end up creating real security concerns.

Here are a few common errors you should try to avoid:

1. The Post-It full of passwords

Take a walk around the office. Most likely, you'll find at least a few desks with Post-It notes full of passwords stuck to the bottom of a computer monitor. Yes, it's convenient, but it also provides easy access to sensitive information to people who shouldn't have it—like disgruntled employees or a thief during a break-in.

The Fix: Explain to your employees why this is a bad idea, and give them some ideas on how manage passwords safely.



2. Out-dated operating systems

Technology is an important part of every small business, but it's often not a priority. That's how things like updating operating systems slip through the cracks or get ignored until they become a serious security threat. For example, do you still have systems running on Windows XP or Windows Server 2003? If you do, that creates a serious security vulnerability.

The Fix: If you're running outdated operating systems, it's time to transition to something more secure. A managed service provider will be able to help you execute a migration like this, and you can also have them take care of updates and patches going forward so you can make sure it gets done.

3. Security software that never gets updated

Do you think your business is secure because you invested in a firewall or installed antivirus software on your machines? That's a great start, but if you didn't take the next step and pay for subscriptions or updates to go with it, you aren't nearly as secure as you think.

The Fix: Find out if you have the subscriptions and updates you need to keep your firewall and antivirus software as secure as possible. If you don't, then you need to get those in place as soon as possible. It's also a good idea to reach out to a managed service provider who can oversee these types of updates for you going forward.

4. Old employees still have access

Lax password policies and passwords that don't expire create another security concern for SMBs. If you don't set passwords to expire regularly, there's a good chance a number of former employees still have access to your system. That doesn't necessarily mean any of them will do something malicious, but why take the risk?

The Fix: Set up a solid password policy, and have passwords expire every 90 days. Yes, employees might think it's a hassle at first, but the improved security will be worth it. While you're at it, teach your employees the best practices for choosing a strong password that's easy to remember but hard to guess.

Password Pitfalls

Using strong passwords is one of the easiest things you can do to help keep your data secure. While choosing an obvious phrase makes it easy to remember, it also makes it easier to guess. And there's nothing easy about regaining control over compromised data.

Here are a few key tips on what to avoid when choosing a password:

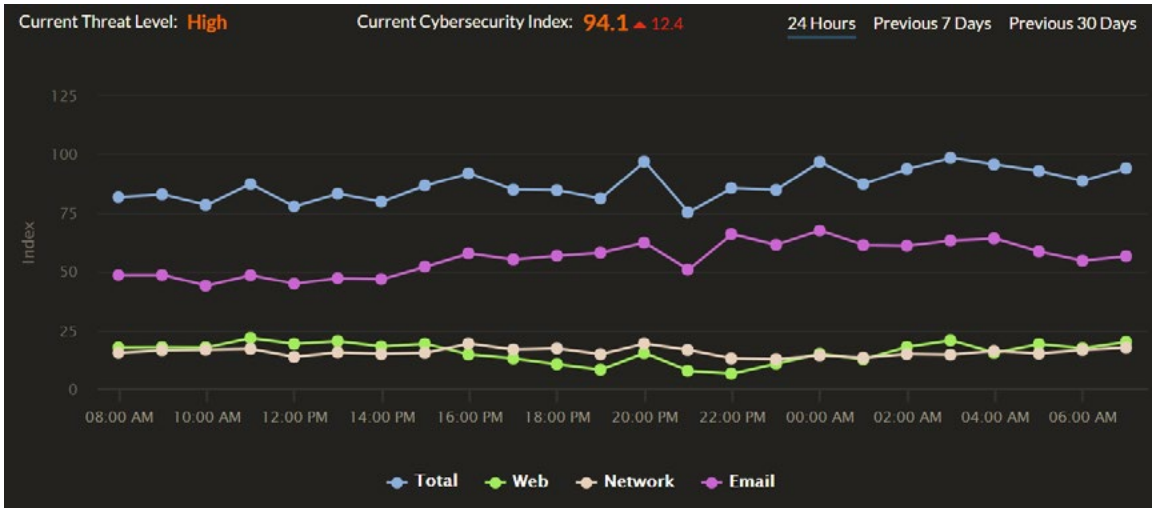
- Avoid a sequence such as "qwertyuiop," which is the top row of letters on a standard keyboard, or "1qaz2wsx," which comprises the first two 'columns' of numbers and letters on a keyboard.
- Don't use a favorite sport or sports team as your password.
- Don't use your birthday or especially just your birth year. You should also avoid passwords that are just numbers.
- Avoid using first names as passwords. Names of friends and family are particularly vulnerable.
- Stay away from swear words and phrases, hobbies, famous athletes, car brands, and film names, which are all widely used passwords as well.
- Avoid password reuse. If a hacker gains accesses to one of your accounts and all (or most) of them use the same password, you're in trouble.

What Is Malware?

The term malware translates quite literally to "malicious software." It's an all-encompassing term that includes viruses, ransomware, worms, spyware, adware, and generally any software that is used to obtain sensitive information without a user's consent. Malware disrupts computer systems in a variety of ways, such as by restricting access, encrypting files, corrupting data, stealing personal information, or slowing the system down.

Malware can enter a system through downloads, email attachments, advertisements, or any type of hole in the security of the system. After an infection occurs, a system shows signs of the attack and is recovered in different ways, depending on the type of infection. For example, ransomware will display a message demanding a sum of money, and spyware will live in your files, possibly without ever being noticed.

Also, be aware of any present threats. A great resource for this is the Barracuda Security Threat Index which shows alerts and vulnerabilities in real time.



Cybersecurity Tip:

Travelers should take extra precautions to guard against cyber threats and protect devices they take on the road. This includes backing up all files, removing sensitive documents and information from their devices, ensuring passwords are in use and that antivirus software is updated.

Types of Malware You Need to Know About

Adware - A type of malware that displays advertisements on your computer and collects data about your browsing habits without your consent

Keylogger - Malicious software that tracks the keystrokes on a computer and transmits the data to another location so it can be used to detect usernames and passwords that are typed on a computer

Ransomware - Software that locks a computer and retains control until the user pay a certain amount of money

Rootkit - A type of software designed to open a backdoor into areas of operating system that are not supposed to be available and to mask its presence while doing so. It is used to deploy other types of malware.

Spyware – Software designed to steal user data—such as website logins and passwords or proprietary information and trade secrets—off machines it has infected

Trojan – Malicious software that seems legitimate but contains other software that attacks the system in some way after tricking a user into activating it.

Virus – A type of malware that attaches itself to an application and then spreads to other programs and computers on the same network through an infected host file, causing a variety of damage when the application is run.

Worm – Software that infects a computer and then replicates itself from system to system on its own without the help of a host file.

Malware's Most Wanted

Cerber - Identified in March 2016, Cerber is spread by phishing emails with malicious files attached, and it is activated by enabling macros.

CryptoLocker - Ransomware that encrypts a victim's files and demands payment before restoring access. It was identified in September 2013 and quickly infected hundreds of thousands of computers and grossed millions of dollars in ransom.

CryptoWall – Malicious software that made its entrance to the ransomware scene in June 2014, taking over were CryptoLocker left off.

TeslaCrypt – Identified in early 2015, TeslaCrypt is a type of ransomware that only infects certain file types, and it is also the first ransomware to explicitly go after game saves, such as those from popular franchises like Minecraft.

WannaCry - Discovered in May 2017, this ransomware cryptoworm spread through EternalBlue, a vulnerability found in older, unpatched Windows systems.

Zeus/Zbot – A Trojan that steals banking information and other personal details from infected computers. It was initially detected in 2007 and has since infected millions of devices. The source code was made public, which led to a number of new malware variants.

Rombertik - A type of spyware that captures anything transmitted or typed in plaintext on an infected system. It also has a fail-safe that can destroy the system by overwriting important boot information and the hard drive partition if the malware code is tampered with, making it difficult at best to recover any data.

This list only scratches the surface because new malware threats are being detected almost every day. So, it's imperative for organizations to be aware of these malware threats and back up their business critical data offsite. Those who don't risk their livelihood because in the wake of a cyber attack or other data loss event, having their data backed up can be essential to a business' survival.

What you need to teach employees about ransomware

Ransomware is now considered a fact of life in today's cybersecurity landscape, but that doesn't mean SMBs are protecting themselves from a potential ransomware attack or even know it's a possibility. Often, users recognize a ransomware threat after it's too late. In February 2018, according to Osterman Research and Barracuda there was one phishing attempt in every 3,331 emails and one piece of malware for every 645 emails.[2]

And falling for one of these emails can be costly. According to the Ponemon Institute, the average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053 in the past 12 months, and the average cost due to disruption of normal operations increased from $955,429 to $1,207,965. [1]

SMBs need to start protecting themselves from the growing threat of ransomware. Educating your customers about the threat of ransomware and sharing these important tips is an important first step.

1. Put technical safeguards in place

As a best practice, have an intrusion-prevention system and security software running on your computers. This should include antivirus software, firewalls, and spam filters. Then, make sure all security patches are up to date, and deploy new patches on a regular basis.

It's also critical to have a backup solution in place and frequently test the backups running on your systems to make sure they're working properly. If you're hit with ransomware, you'll want to restore operations as quickly as possible, and having a recent backup to recover from will save you both time and money.

2. Train employees

Even with technical safeguards in place, it's employees who ultimately risk exposing a business to ransomware. User error, such as clicking on an infected online advertisement, pop-up window, or attachment in a spam email, is often to blame for inviting ransomware into a computer. So, users are the most important line of defense.

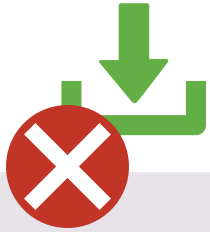
Talk with your employees about ransomware, educating them on what it is and how they can help defend the business. Try getting the whole staff together for a training session and bring lunch to make it a Lunch and Learn event.

As a best practice, you should require all new employees to complete the training and offer it on an ongoing basis to avoid information being missed. If you don't have the resources to put this type of training together, talk to your IT service provider. They should be able to run a program like this for you or provide other educational materials.

3. Provide examples to end users

The most effective way to educate your employees on ransomware is to show them examples of what it looks like so they'll know the warning signs and be able to identify a suspicious message or attachment before they click on anything. For example, you can share Barracuda MSP's Ultimate Phishing Quiz, which includes examples of infected and legitimate emails and provides explanation of how to tell the difference.

Once ransomware has infected a computer, a message is displayed on the screen letting the user know their machine has been compromised. Examples of these messages can be found here. It's helpful to share this type of information with employees as well so that, even if it's too late, they'll know to alert management and ask for help.



Cybersecurity Tip:
Take preventative measures to protect yourself from attacks. De-activate auto-downloads for attachments, and save and scan attachments before opening them.

How to create a security policy for your SMB

Many successful SMBs have developed formal, documented IT security policies to govern operations both in their offices and in the field. These policies educate employees and guide behavior, in addition to protecting the business and adhering to compliance regulation. Equally important, successful SMBs conduct regular reviews of these policies and revise them as necessary to adjust to changes in their environments and business practices.

If you don't have a security policy in place, follow these best practices for developing one with the help of your IT service provider.

1. Identify roles and responsibilities

First, figure out who currently has access to critical data, infrastructure, and applications. Note your findings and then assess whether or not each person needs the access they've been granted. Then, you can begin to limit or reinstate permission to access sensitive information and assets. For example, system administrators should have access to things that contractors should not. You want to make sure there will be no uncertainty about who has access to what.

2. Define data retention parameters

You'll also need to implement a document retention policy. These types of policies are especially important in certain regulated industries that require specific retention parameters. Defining a data retention policy is critical because there's an increased risk of data being stolen or compromised when it's kept beyond those defined dates.

3. Verify robust encryption technology is being utilized

Setting standards for encoding your information is another important part of a security policy. Implement military-grade 256-AES (Advanced Encryption Standard) encryption technology to secure data stored in the cloud, and use SSL (Secure Sockets Layer) encryption technology for data in transit. To make your security policy even stronger, ask your IT service provider to look for a data protection solution that uses private key encryption (PKE) technology.

4. Adhere to compliance regulations

When developing a security policy, be sure to meet to your industry's compliance regulations. Certain industries are more regulated than others, but you should always stay informed about any pertinent regulations and make sure your security policy addresses all issues necessary to help your SMB stay compliant. HIPAA, for example, requires all covered entities to encrypt all their storage technologies for data at rest. An IT service provider can help you determine what you're liable for and make sure you comply with all requirements.

Cybersecurity Tip:

Always share a potential error ASAP! If you accidentally clicking on a suspicious link or opening a suspicious email, tell your service provider right away. The sooner the right people know, the sooner you can get it fixed — hopefully without suffering a breach.

Conclusion

With cybercrime becoming an increasingly serious threat, **it's not a question of if businesses need security; it's a question of what level of security you need**. Keeping this in mind, you should reach out to your IT service provider about data security to make sure your business is properly protected.

It's also important to start educating your employees as soon as possible because new cyber threats emerge every day. Be proactive and s**tart talking about cybersecurity now** instead of waiting until after your company experiences a data breach or malware infection. Don't wait until it's too late.

Cybersecurity Tip:

The FCC recommends making workplace Wi-Fi networks secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID).

Contact Waterdog Computer Works to learn more about cyber security and to get help making sure your business is properly protected.

SOURCES

1. 1. "2017 State of Cybersecurity in Small & Medium-Sized Businesses," Ponemon, Sept. 2017.
2. "Best Practices for Protecting Against Phishing, Ransomware, and Email Fraud," Osterman Research on behalf of Barracuda Networks, April, 2018.

WATERDOG COMPUTER WORKS

Performance. Protection. Peace of Mind.

About Waterdog Computer Works:

Waterdog Computer Works is a trusted provider of Business IT services, Network Compliance and Cybersecurity solutions in the Main Line Philadelphia area. For over 18 years, we have been "in the trenches" gaining real-life experience, continuously training our employees about the latest trends in Cybersecurity and developing valuable vendor partnerships. As a result, we have the tools to recommend comprehensive solutions with the best product offerings to keep your business protected and running at peak performance.

Waterdog Computer Works

121 N. Wayne Avenue, Suite 201

Wayne, PA 19087

484.580.8568 | sales@waterdogcomputerworks.com | www.waterdogcomputerworks.com