INSIGHTS

Cyber made simple.

one brightly cyber

SMB CYBER MYTHS

BY JAY BORDEN

There are some myths about Small and Medium businesses, SMBs, and cybersecurity. These myths are just that, myths, and can be very dangerous to any SMB that believes them.

Two facts before we begin. According to the IBM Cost of a Data Breach Report, in 2023 that cost rose again and is now $4.45 million. The cost does vary by industry and company size, but it can easily be more than an SMB can afford. Research found that 60% of SMBs sustaining a cyberattack go out of business within 6 months. That should certainly motivate you to take cybersecurity more seriously.

So, let's look at the myths.

Myth - Cyberattackers only go after large businesses. A survey found the 69% of SMBs reported having at least one cyberattack last year.

Cyber incidents can be damaging or even fatal to an SMB because they don't have the resources for a large cybersecurity team or in many cases any team at all. They also are often unaware of their risks.

Myth - SMBs aren't big enough targets for ransomware, an attack that encrypts all your information effectively closing your business. SMBs most certainly are big enough. Ransomware attackers view SMBs as easy targets because of their lack of knowledge and preparedness.

When struck by ransomware, there are two courses of action. First is to restore all the devices from a backup. But this requires a current and complete backup, something not all SMBs have, and that the backup was offline and not encrypted by the ransomware. But even if you meet both of these requirements it still takes days or weeks to restore all your systems. Your information will be unavailable during that time. Without access to your information, can your business operate?

onebrightlycyber.com
(888) 773-1920

SMB CYBER MYTHS

CONTINUED

The other course is to pay the ransom. However, in many cases the decryption key does not decrypt all your information. In some cases, it doesn't work at all. Even if the key works decryption is not instantaneous and takes time. Time you are still not operating.

One more point about ransomware. Before the ransomware is activated, the attackers steal sensitive information about your customers. This is their leverage. Fail to pay and they make the information public. What will your customers think of your company then? Even if you pay the ransom and the cybercriminals say they will destroy the stolen information, they are not the most trustworthy group of people.

Research shows that a successful ransomware attack often leads to another ransomware attack because the attackers know you will pay, already stole your information, and know your weaknesses.

Myth - Cybersecurity risks can be solved by technology. If that were true, then you wouldn't read about new breaches all the time. Tools are necessary but will not stop many types of attacks. People are the main cause of cyber breaches and phishing is often what catches them. Research puts people as the cause of anywhere from 80% to as much as 95% of the breaches and tools rarely catch these.

Myth - Using cloud services removes cyber risks from your company. Not true. There is a legal and regulatory principle that says you can outsource a function; you cannot outsource responsibility. That means that using cloud services does not relieve you of the burden of responsibility. Cloud services do offer benefits. But they also add complexity over who is responsible for what and that has created additional cyber risks and weaknesses. The cloud service vendors themselves have been hacked.

Myth – Following cyber security practices gets in the way of business. Children are taught the value of good hygiene for staying healthy. The same is true for cyber hygiene and keeping your business healthy.

What constitutes poor cyber hygiene? Weak or reused passwords are a major factor. Cybercriminals can crack weak passwords in seconds. Substituting a $ for an S, putting a capital letter in an unusual place, or adding a number or special character doesn't make a password strong.

SMB CYBER MYTHS

CONTINUED

Once cybercriminals get one of your passwords they will try it, and variations of it, on multiple websites.

What to do?
Know what good cyber hygiene is, and how to do it properly.

The importance of cybersecurity needs to start at the top. Not just words but actions. If employees see that you take cybersecurity seriously they will be more apt to.

Keep all software up to date. Patches and updates may add new features, but they also fix cyber holes.

Go beyond tools. Tools may find a risk, but they rarely tell you what to do. They also don't teach users about phishing and other attack methods. They certainly don't help after a breach.

Lastly, do not forget about cyber insurance. Cyber insurance is like fire insurance on your home or collision on your car. You hope to never need it, but when you do, you are happy it is there.

One Brightly Cyber assesses your risks and provides guidance and education based upon the results of the assessment and your industry. We also provide a simple path to cyber insurance.

In the event of a breach our team of US based cyber advocates are with you the whole way. We have over 20 years of experience helping people and companies like yours recover. We can even help with insurance and regulatory filings.

Neglecting any part of cyber protection may cost you your business.

We make cyber simple.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.