Six Misconceptions that may invite a cyberattack on your **small business**

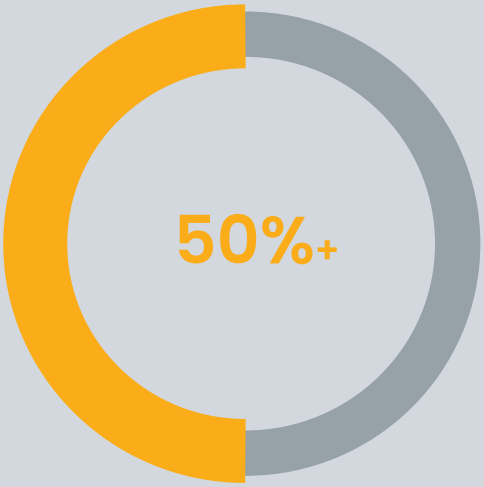
(Plus one thing you can do about it)

Introduction

Digital technology has been a boon for small businesses, in effect leveling the playing field between big and small businesses. Whether it's a sophisticated e-commerce website, automated marketing campaigns or advanced data analytics, small businesses have more tools than ever before within their reach. But in leveling the playing field, digital technology has also leveled the field of attack. Cybercrime affects big and small businesses alike, often with no regard for size, reputation or revenue. In fact, more than half of all small businesses have suffered a data breach within the last 12 months.[1]

The reality is that once you connect your business to the Internet, you open the door to cyberattacks, viruses and other problems. Importantly, small businesses are more vulnerable to cyberattacks. While big businesses face mostly heavy fines and move on after a data breach, **one in ten small businesses go out of business following a data breach, and one in four are forced to file for bankruptcy.[2]**

So what can your business do to protect itself? Understand what the signs of an imminent attack look like, from overconfidence in anti-virus software to ignorance of attacks that have already occurred. To help safeguard the future of your small business, here are six common misconceptions that could be helping cyberattackers steal your data.



More than half of small businesses have suffered attacks in the last 12 months[1]

Misconception #1

"I'd know if we were attacked."

We've all imagined what a cyberattack would look like: alarms beeping, anti-virus alerts flashing, employees frantically saving files before they're lost forever. But it turns out that scenario is largely the product of our imaginations. Most companies don't even know they've been attacked until months later. One study in 2018 found that the average time between infection and detection of a data breach was 196 days.[3] Not minutes, not hours, but days.

If that happens to big businesses with vast security systems and dozens of security professionals situated in a high-tech security operations center, what chance does your small business have of finding data threats? Actually, small businesses have a natural advantage because they have a smaller attack surface to guard. But they still need to be vigilant, which means investing in a 24/7 network monitoring system and 24/7 support from trained security professionals. This is an area where managed service providers (MSPs) can play a critical role, providing round-the-clock monitoring while you and your employees are sleeping. **If your business stores sensitive data—credit cards, social security numbers or other personally identifiable information—or conducts business transactions over the Internet, it's a target for a data breach.**

Misconception #2

"We need a solution that stops 100% of threats."

Blocking every brute-force attack or ferreting out every phishing email is a recipe for failure because of the sheer impossibility of stopping everything. In a world where each malware variation has an average life expectancy of less than one minute, businesses cannot count on the perfection of their anti-virus or firewall software for protection. Instead, the best approach to external threat protection is internal data protection: stopping valuable data from getting out, rather than stopping everything from getting in. This can be achieved through real-time blocking in combination with analytics, anomaly detection, identity and access management (IAM) and, increasingly, artificial intelligence (AI) tools. Using these technologies to provide inbound controls and content screening are essential to keeping threats at bay.

Misconception #3

“I trust my employees, it’s the people I don’t know I should be worried about.”

Remember those old horror movies where the caller would be traced inside the house? It turns out there’s something even scarier than that. Studies show that **one in three data breaches originate on the inside of the business.**[4] How can that be? Well, many of those attacks are the result of human error: clicking on a phishing email by mistake, accidentally sharing login credentials on an unsecure network, etc. Yet even so, the fact remains that small businesses have to be diligent about monitoring the activities of employees, partners and other “trusted” entities who may have access to sensitive business data.

Inside threat protection starts with strong security policies: managing data access privileges based on assigned roles and responsibilities, enforcing policies for how and where business data is stored (e.g., in the cloud, on personal devices), requiring partners to demonstrate their own security preparedness and so on. If outbound controls and data loss prevention activities can be automated – such as automatically updating access privileges when an employee’s job or job status changes – your business will have a better chance of eliminating insider threats.

Is your data secure?

1 Minute

Less then one minute is the average lifespan of a malware variation.

50 Percent

The percent cyber-attacks targeting mobile devices rose last year.

“1234”

The most common password along with “guest” chosen.

Misconception #4

"Cybercriminals are interested in hacking my network, not my smartphone."

As smartphones and tablets are being used more for business, cybercriminals are paying more attention to mobile devices. Last year, the number of cyberattacks targeting mobile devices rose 50 percent.[5] There are a number of security factors in play with mobile devices, including mobile endpoint security, Wi-Fi network security, virtual private network (VPN) tunneling, mobile/cloud app security and the Internet of Things (IoT). It's a lot to think about, making it particularly challenging for small businesses to enforce consistent levels of security across a wide variety of devices, apps and locations. **And it's about to become more complicated with the rise in IoT.** In the near future, cybercriminals could be targeting your video doorbell or wireless thermostat to hack your security defenses!

Misconception #5

"Regulatory compliance is something that big companies have to worry about, not us."

If you think that regulatory compliance just applies to big companies, you're right… some of the time. New regulations such as Europe's GDPR and California's CCPA, for example, don't apply to businesses with less than $7 million in annual revenue. But other regulations, such as HIPAA and PCI DSS, do apply to small businesses. So whether you run a dental practice that collects patient data or a flower shop that processes credit cards, you need to be protecting personally identifiable information (PII).

Not sure where to start? You're not alone. Many small businesses struggle to understand the nuances of security compliance, such as how much encryption is enough or what data is safe to share with business partners. This is where having a trusted security advisor can make a lot of sense, particularly for those businesses that don't have IT personnel with security expertise.

Misconception #6

“My employees are careful enough to choose strong passwords.”

The most commonly used passwords are “guest” and “1234.” Need we say more? Selecting strong passwords (and changing them often), frequently rotating your encryption keys, updating software when new releases are available and downloading the latest patches are all part of what experts call good security hygiene. Proving that an ounce of prevention is worth a pound of protection, practicing good security hygiene is the single-most important thing you can do as a small business owner to prevent cyberattacks.

It’s important to remember, however, that the cause of poor security hygiene is its lack of simplicity. Employees may feel they don’t have the time or energy to create new passwords for every application and change them every three months. That’s why it’s so important to automate these processes where possible. **The more seamless and simple you make security processes, the more likely that your employees will get on board with them.**

What can you do about it? All signs point to Privafy.

We understand that, as a small business owner, you want to save money. And the truth is that, by spending a few dollars a day on the right security solution, you can save yourself thousands of dollars a year in unnecessary hardware costs and multiple software tools from different vendors. Where can you find a solution like that? Ask your managed service provider about Privafy.

Privafy is a complete, proven security solution delivered as a cloud-based service that provides 24/7 monitoring, internal and external threat protection, AI-driven analytics, automated threat response, simplified security hygiene and more. With Privafy delivered and managed by your service provider, your business can improve its security posture, save money and stop cyber criminals from stealing sensitive data:

Block, stop and mitigate external and internal threats with total network traffic analysis driven by AI technology and advanced machine learning

Fully automate essential security tasks including software patches, passwords and encryption keys

Protect your most important data on mobile devices and in your network through Privafy's patented key encryption/exchange technology

Gain a 360-degree view into your real-time security status through easy-to-use dashboards, alerts and logs

Guard your business 24/7/365 with tier one, two and three support delivered by trained security professionals

You don't have to go it alone. Contact your managed services provider today and discover how Privafy can keep your business and your data safe.

Sources
1. Morgan, Steve, "Global ransomware damage costs predicted to hit $20 billion (USD) by 2021," Cybercrime Magazine, October 21, 2019 (Last accessed February 6, 2020), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.
2. Freed, Benjamin, "Ransomware hits everywhere, but governments pay 10 times more," Statescoop.com, July 16, 2019 (Last accessed February 6, 2020), https://statescoop.com/ransomware-local-government-pays-10-times-more/.
3. Spadafora, Anthony, "One trillion phishing emails sent every year," techradar.com, June 12, 2019 (Last accessed February 6, 2020), https://www.techradar.com/news/one-trillion-phishing-emails-sent-every-year.

Privafy, Inc.
2 Burlington Woods Drive
Burlington, MA 01803

www.privafy.com