10 REASONS WHY MOST BUSINESSES ARE VERY VULNERABLE TO CYBERCRIME

AND HOW TO
SECURE YOUR BUSINESS
AGAINST THEM

HOOK
SECURITY

10 Reasons Why Most Businesses Are Very Vulnerable to Cybercrime.

Cybercrime is rampant, with worldwide costs expected to double from $3 trillion in 2015 to $6 trillion by 2021. And it is not just Fortune 500 companies that are paying the bill. Small businesses are in the crosshairs and they are losing the fight against cybercrime because they are:

1. Underestimating Risk: “My business is too small to be a target of cybercrime”

Many small business owners make the erroneous assumption that cybercrime affects only big business and that their small enterprise is not even a blimp on the radar of threat actors. An industry survey from 2017 found that a whopping 45% of small business owners do not think they are at risk.

In reality however, **small businesses are increasingly being targeted** by cybercriminals and already about 50% of all security breaches occur at small businesses. Small businesses have a 47% chance of experiencing a cyberattack at least once in 12 months, and a 21% chance of being hit multiple times.

2. Lacking cybersecurity expertise

Even if small businesses understand that cybercriminals are out to get them, they usually do not have the resources to keep an **IT security expert** on staff. A recent survey found that only 30% of small and medium businesses

(SMBs) employed someone with this role, while 52% of surveyed businesses had staff members sharing cybersecurity responsibilities next to their main jobs. Defending against cyber threats is obviously a lot tougher without a security specialist on the payroll.

3. Using outdated, unpatched software

The limited resources of most small businesses also result in many of them relying on **outdated software** that is not being patched against known vulnerabilities, either because proper **patch management** is not a priority within the organization, or because the software manufacturer has dropped support for the archaic products being used.

For example, in the U.S. 46 million commercial PCs are still running Windows 7, 30% of which (almost 14 million) are used in SMBs, even though Windows 10 is much safer to use.

4. Unprepared and unwilling to learn (not even the hard way)

Even if small business owners understand that their companies are potential targets for cybercrime, they often fail to put in place a proper **cybersecurity strategy**. A recent industry survey found that almost 3 out of 4 SMBs were not prepared to deal with the cybersecurity risks they faced.

To make things worse, almost two-thirds of small businesses do not improve their cybersecurity strategy even after they have suffered a cyberattack.

5. Failing to provide employee cybersecurity training

Despite the current cybercrime boom, many companies still fail to provide adequate cybersecurity training for their employees. Small businesses are even less likely to invest in teaching employees to stay safe from criminals lurking in cyberspace, as they lack the staff to provide **cybersecurity**

training and are reluctant to invest in specialized training programs. Consequently, employees are the leading cause of cybersecurity breaches at small businesses, instead of being part of their defense, which they should be.

6. Struggling with Identity and Access Management

The risk posed by employees with little cybersecurity awareness is often exacerbated in small businesses because they, like bigger businesses, are not properly managing **privileged accounts**. As a result, employees are often given unnecessary access to confidential information that could be compromised if they fall victim to a cyberattack.

A recent study found that 70% of businesses also fail to adequately limit **third-party** access, while, 55% of businesses do not revoke privileged access when a **(disgruntled) employee** leaves the company, putting the business further at risk.

7. Lacking resilience

Security breaches tend to have more far reaching consequences for small businesses than is true for larger corporations, as they have fewer resources they can utilize to recover from a cyberattack. In 2017, the cost of a cybersecurity incident for SMBs averaged $120,000. The **financial cost** of a data breach or a ransomware attack may therefore be enough to put a small company out of business. And even if that doesn't happen, **reputational damage** might just do the trick by hampering business in the long term.

8. Being hit with targeted and sophisticated attacks

Cybercrime is on the rise in both quantitative and qualitative terms, meaning that businesses of all sizes are facing more threats *and* that those threats are becoming increasingly advanced. Cyberattacks involve more and more **planning**, increasingly **complex malware**, and higher levels of psychological manipulation, known as **social engineering**, to deceive victims.

To make things worse, small businesses are lagging behind when it comes to investing in protective measures like proper **password management** and the adoption of **multi-factor authentication** (MFA).

9. Facing cybercrime-as-a-service

Another worrying trend for small businesses is the emergence of a massive cybercrime economy across the Dark Web, built around cybercrime organizations providing criminal services. **Cybercrime-as-a-service** covers things like the exchange of stolen data, money laundering services, cybercriminals for hire, the sale of phishing, ransomware and other malware tools with instructions, known as "**kits**". Some of these are offered as subscriptions that include software patches and customer service.

Cybercrime-as-a-service allows expert hackers to earn over $166,000 a month, and enables virtually anyone with an internet connection to become a cybercriminal.

10. Not purchasing cybercrime insurance

All things considered, cybercrime is clearly a critical threat to small companies. A serious security breach can easily mean bankruptcy for a small firm, especially because only 21% of small enterprises are covered by a specific **insurance policy** for cybersecurity incidents. This effectively means that in the midst of a growing cybercrime epidemic, 4 out of 5 small business owners are operating on little more than a wing and a prayer.