aunalytics

How to Keep Your Business Thriving in a World of Risks

Managed security can protect your Business from cyber attacks

In the early 2000s, cybersecurity risks began to increase in their effectiveness, but antivirus (AV) solutions kept small and medium-sized businesses (SMBs) safe. With AV updates, employee training, and software patching, most SMBs were able to avoid the worst of cyberattacks—until now.

Incidents like the WannaCry ransomware attack, which affected organizations across the globe, served as wake-up calls for many that cyberthreats are changing, and many companies still aren't prepared. Many SMB owners know someone who's been forced to pay a ransom to retrieve data or even had to shut down because data and systems were too costly to restore or weren't restored as promised. Still others have experienced cleanup costs from other malware attacks.

Many SMB owners think they won't be targeted due to their size or small attack surface. Yet as this chart shows, that simply isn't the case. Cybercriminals increasingly target SMBs, as it much easier to circumnavigate their defenses than those of enterprise companies.

The Dirty Truth About SMB Security	
Yes, you are a target: 43% of all cyberattacks targeted small to medium-size business (SMB) operations in 2018. Source: Verizon.	**Here's why:** Many cyberattackers see SMBs as an easy entry into their larger customers. SMBs were responsible for the Target and JPMorgan Chase data breaches. Even if they aren't targeting larger partners, cybercriminals can still make money off SMBs who have valuable data (and they almost all have valuable data).
You may not know you've been hit: It takes companies an average of 279 days to realize they've been hit by a data breach, increasing the business harm.	**SMB clean-up costs are high:** The average cost of a data breach for organizations with fewer than 500 employees was $2.74M in 2018.
You may face an extinction event: Of the SMBs that are attacked, 60% never reopen.	

The Risks Your SMB Faces Grow Every Day

Businesses today rely on their digital assets. However, that's increasing the risks you face. They include:

Connections are growing: Businesses are using more devices, applications, and cloud services than ever before.	**Shadow IT is a real problem:** Your employees are likely using more cloud services than you know about, creating a blind spot for your IT team and your organization's security.
Passwords are a weak link: Employees often reuse passwords across accounts and use easy-to-guess passwords.	**Human error is hard to prevent:** Your employees may use public Wi-Fi to do their work, accidentally click on phishing emails, or share sensitive data on cloud services or flash drives.
The latest threats elude AV: Weaponized documents, fileless threats, zero-day threats, and ransomware lack signatures and can slip through scheduled AV scans.	**You may have compliance risks:** If your SMB works in a heavily regulated business, you could face regulator fines in addition to cleanup costs.
Data sharing: Your partners may not have air-tight security, exposing your data to unauthorized access.	

What You Can Do About Cybersecurity Risks?

It pays to get tough on cybersecurity. Enhancing your security posture proactively can help you harden your defenses and protect yourself from threats before they hit your company networks and disable your business, systems, and data.

When you invest in managed security, you get:

- A comprehensive solution for all your security needs
- Cloud-based solutions that are updated automatically with the latest threat data
- The ability to “roll back” any systems hit with ransomware to a pre-infection state
- Complete security coverage and simplified cost structures
- An end to security management headaches and worries

Get started with managed security today.

Aunalytics

Need more information?

aunalytics.com

info@aunalytics.com

855-799-DATA