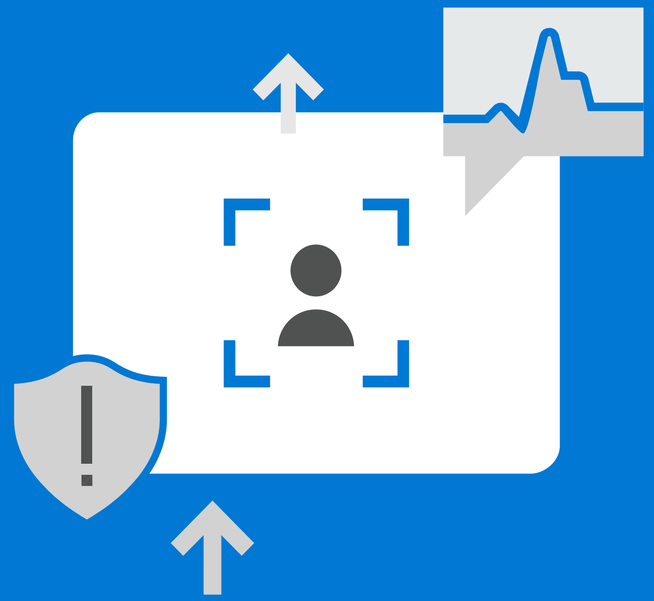
Six common cybersecurity mistakes you can fix now

Introduction

Cybercriminals are clever and on the lookout for vulnerable businesses. They exploit common mistakes and flaws to breach systems, then steal, disrupt, or hold businesses for ransom. But here's the good news: you don't have to be an easy mark. You can make changes right now to reduce the likelihood of a successful attack. **Here are six common cybersecurity mistakes and how to fix them:**



Mistake 01

Piecemeal approach

It’s tempting to stack new security measures on top of existing ones as new threats emerge. But this results in too many products and not enough integration. Every product has its own dashboard, controls, and alerts. And someone has to stay on top of it all.

This lack of integration between security products makes it difficult to see threats holistically, and even harder to respond quickly and effectively. Instead, look for products designed to work together, and partner with companies that actively seek collaboration with the security industry.

Mistake 02

Insufficient security expertise

Cyberthreats continue to increase every day, and 43% of cyberattacks target small businesses,[1] which usually have limited IT resources in-house. Everyone else is focused on running the business, not security. You need help.

Consider automated, software-based processes that can monitor your systems continuously and even take action when a threat is detected. Smart automation can save you time and energy, allowing you to focus on other priorities. Also, consider partnering with a specialized security provider. And finally, invest in educating your employees on security awareness so everyone can be part of the solution.

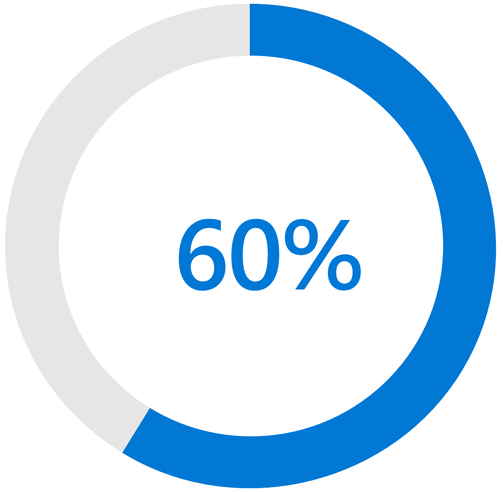
[1] Small Business Trends, Jan. 3, 2017, CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know

Mistake 03

Unsecured personal devices

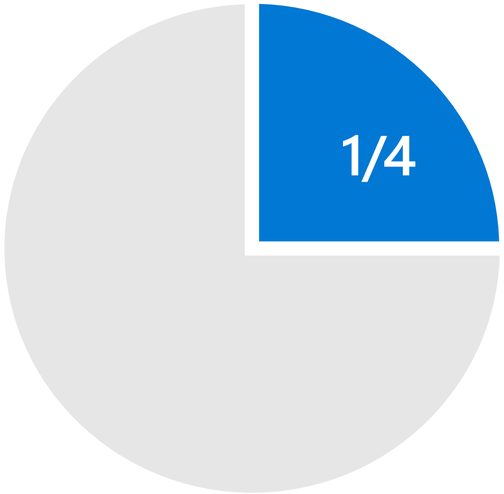
How many ways do you access your business data? Even small businesses may have multiple computers, laptops in remote locations, personal smart phones, and tablets. A determined hacker can attempt access through many possible endpoints. In fact, 60% of breaches stem from a compromised endpoint, such as a personal device.[2]

Identity and access management (IAM) eliminates the complexity of multiple user credentials by giving each employee a single, secure identity to access all your network resources. And multi-factor authentication (MFA) offers another layer of protection, requiring a user to present a password plus secondary authentication such as a fingerprint or code sent via SMS.



Breaches stem from a compromised endpoint, such as a personal device.

[2] Johnson, Ann. "Top Five Security Threats Facing Your Business and How to Respond." Microsoft Secure Blog. October 18, 2016. https://cloudblogs.microsoft.com/microsoftsecure/2016/10/18/top-five-security-threats-facing-your-business-and-how-to-respond/



One in four businesses targeted, with a median loss of $79,841.

Mistake 04

“I’m too small to be a target”

Cybercriminals increasingly target smaller businesses assuming that you may be complacent and unprepared. A study by the Better Business Bureau found that nearly one in four businesses with 250 employees or fewer reported having been the target of a cyberattack, and the overall annual average loss for smaller businesses from these attacks is estimated to be $79,841.[3]

Make sure to invest in security, but realize that no program is 100% foolproof. Assume that you can be attacked and breached. Prepare an incident response plan, ensure continuous monitoring for suspicious activity, and organize the resources needed for a quick response to reduce the damage to your business.

[3] Better Business Bureau. “2017 State of Cybersecurity Among Small Businesses in North America.” https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Mistake 05

Overlooking the security of the cloud

Security is complex, and even well-funded enterprise IT departments struggle to stay on top of it. The right cloud partner can do much of the heavy lifting for you and provide smart ways to encrypt and backup your data.

Moving to the cloud doesn't have to mean starting over from scratch. Evaluate your needs, and make the move in stages. Or even employ a long-term hybrid strategy where some of your systems remain onpremises. Be sure to evaluate cloud service providers using international standards, and look for vendors that publish detailed information about their security and compliance measures.

Public cloud providers offer better security than a small business or even a big enterprise is able to achieve. This is due to the investments that cloud providers are making to build and maintain their cloud infrastructure.[4]

Rene Buest,
Senior Analyst and Cloud Practice Lead, Crisp Research

[4] Trotter, Paul. "Top Cloud Security Fears & How the C-Suite Is Tackling Them." May 20, 2015. http://www.cio.com/article/2924390/cloud-security/top-cloud-security-fears-and-how-the-csuite-istackling-them.html

Mistake 06

Leaving data unprotected

Data travels outside your control when it's shared by employees, partners, and customers. But trying to lock down everything discourages productivity and innovation, and eventually leads to employee workarounds if the inconvenience proves too great. Balance protection with productivity by focusing on security at the data level.

Categorize your data based on how sensitive and critical it is to your business. Better yet, automate your data classification so the appropriate protections and monitoring are in place when the data is created. Protect what's most important with the strongest measures, such as restricted access, limited sharing privileges, and encryption.

Build your security strategy—one step at a time

Modern cybersecurity requires a coordinated, multifaceted approach. But it's a journey, and every step you take makes a difference and reduces your risk. If you haven't been attacked yet, assume that you will be a target eventually and look for partners to help. Start with this free security assessment tool, and get prepared to protect, detect, and respond to the threats that come your way.

Learn more