Six common cybersecurity mistakes you can fix now
Introduction

Hackers are clever, their methods continue to evolve, and building more and bigger walls just isn’t enough.

You need a strategy that’s always-on and assumes a breach is on the way. Plan for protection, detection, and response.

Start by fixing these six common mistakes.
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.
Small and medium-sized businesses usually have limited IT resources in-house. And 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. Partner with a specialized security provider if needed, and invest in educating your employees on security awareness.

Mistake 02
Insufficient security expertise
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.¹

Identity and access management (IAM) eliminates the complexity of multiple 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.

Cyber criminals increasingly target smaller businesses assuming that you may be complacent and unprepared. A study by the Better Business Bureau found that more than one in five businesses with 250 employees or fewer reported having been the target of a cyberattack, with a median loss of $2,000.²

With ever-increasing and evolving threats, you’ll never be able to maintain 100 percent protection. Adopt an “assume breach” approach, with a strategy for maximizing protection, detection, and response. Have an incident response plan in place and continuously monitor for suspicious activity.

Six common cybersecurity mistakes you can fix now

Jun
2018

Security is complex, and most small and medium-size businesses simply don’t have the resources in-house 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 on-premises. Be sure to evaluate cloud service providers using international standards, and look for vendors that publish detailed information about their security and compliance measures.

Mistake 05

Overlooking cloud advantages

Security is complex, and most small and medium-size businesses simply don’t have the resources in-house 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 on-premises. 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.

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

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 work-arounds 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.
Take a holistic approach—one step at a time:

Modern cybersecurity requires a coordinated, multifaceted approach. But there's no need to be overwhelmed. Every step you take makes a difference. Assume you will eventually be a target, 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