18 Ways To Protect Your Business From A Cyber Breach.

Expert cyber recommendations for SMBs to safeguard their most valuable business assets.

PACE TECHNICAL

Table of contents.

PACE TECHNICAL

18 ways to protect your business from a cyber breach.

#1 Endpoint security.

Also known as Anti-virus, Anti-Malware software but newer next-gen apps are referred to as Endpoint Security. Look for next-gen options that use web-based, real-time definitions.

68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure.

#2 Password management.

Password Management refers to all areas of managing passwords. This includes implementing password policy (expirations, required format, etc.) as well as implementation and management of a password tool.

51% of people use the same password for work and personal accounts.

#3 Spam & phishing protection.

Most businesses already have some form of SPAM protection to reduce unwanted emails. Phishing protection protects your users if they inadvertently click on a potentially malicious link.

#4 Firewall & VPN.

Firewall management is the process of efficiently managing your firewall rules, configuration, logs and alerts. Most modern firewalls have the built-in VPN functionality to securely connect to business systems from remote locations.

18 ways to protect your business from a cyber breach.

#5 Mult-factor authentication.

Multi-factor authentication is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to authenticate.

Only 20% of employees use MFA.

#6 Backup/DR/ business continuity.

Backup technology has changed significantly over the years. Know your recovery objectives and implement a solution that meets your requirements. If you don't have a Disaster Recovery (DR) Plan, consider putting even a basic plan in writing.

64% of your employees have access to 1,000 or more sensitive files. In other words, there's a solid chance that your intern can accidentally create, update, and delete vital documents without you knowing.

18 ways to protect your business from a cyber breach.

#7 Computer updates & patching.

Patching and updates fix bugs and potential security vulnerabilities and keep systems functioning at their peak. Ensure you have the right process around this and dedicated resources to ensure it is done for all systems.

37% of breached businesses confirmed they don't scan their systems for vulnerabilities.

#8 Proactive security & IT alignment process.

Cybersecurity is 25% tools and 75% hygiene which must include proactive system checks and alignment to IT security standards. When you have the right proactive security and IT alignment process your tools function better, systems are more resilient, and you are more secure. Tools without hygiene are vulnerable!

#9 Documentation & reporting.

Documentation of your key assets and systems is a basic but critical part of a cybersecurity plan. Reporting needs to go beyond the basics of assets and uptime and give you an understanding of where you have gaps, risks and vulnerabilities in your network.

18 ways to protect your business from a cyber breach.

#10 Dark web monitoring.

Dark web monitoring is the process of searching for and keeping track of personal information found on a portion of the internet not accessible via normal means.

500,000 stolen Zoom passwords were available for sale in dark web crime forums in 2020.

#11 Security awareness training.

Security training provides employees with a basic understanding of the potential cybersecurity threats and how to respond. Some tools offer simulated phishing email tests to see if your users would fall victim to a phishing email.

39% of Canadian businesses are unaware that employees are their top vulnerability to a cyber attack.

#12 Cyber insurance.

When all else fails, make sure you have good insurance. Not all cyber-insurance plans are equal and how your network is managed and maintained will affect your cost. Speak with your insurance agent to confirm what is and isn't covered in your plan.

48% of companies purchased cyber insurance after being the victim of a cyber attack or cyber loss.

18 ways to protect your business from a cyber breach.

#13 Mobile device management.

(MDM) allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints.

50% of firms that allow BYOD were breached via employee owned devices.

#14 Encryption.

Encryption scrambles text into an unreadable format to protect your data should an unwanted user gain access to your data. Encryption can be used for mobile devices, file data, emails and more.

Though awareness is high about the need for data encryption, fewer than 30% of firms have implemented it.

#15 Web app security.

Detect abnormal user behavior like unfamiliar sign-in properties, or suspicious manipulation within cloud-based apps.

56% of the largest cyber incidents in the past five years related to a web app security issue.

18 ways to protect your business from a cyber breach.

#16 Advanced endpoint detection & response.

(EDR) is a cybersecurity technology that addresses the need for continuous monitoring and response to advanced threats. It is a subset of endpoint security technology and a critical piece of an optimal security posture.

68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure.

#17 SIEM/LOG management.

SIEM (Security Information & Event Management) collects and analyzes logs and activity across multiple devices to detect suspicious activity and potential threats. This aids the ability for security analysts to search for and identify potential malicious activity.

69% of security practitioners say their enterprise cybersecurity focused on reactions and incidents; therefore, they don't work on proactive cybersecurity activities like threat hunting or incorporating threat intelligence.

18 ways to protect your business from a cyber breach.

#18 Security standard compliance (ISO27001, NIST, CIS, ETC).

Cybersecurity controls are the counter-measures that companies implement to detect, prevent, reduce, or counteract security risks.

Have questions about critical cyber controls or compliance requirements your business might need?

Let's Chat!

Managed IT.
Managed Better.

Want to see our approach to your cybersecurity firsthand?

Call us today to talk with one of our seasoned consultants.

We're happy to answer your questions, provide recommendations, and audit your current IT network.

Request your initial consultation today!
Phone: (905) 763-7896 Email: inquiries@pacetechnical.com

PACE
TECHNICAL