CYBERSECURITY
SELF-ASSESSMENT

Essential Best Practices for Protecting Small Business

All small businesses face the risk of a cyber-attack that can disrupt or devastate their organizations. However, not many small businesses have a clear understanding of what is needed for cybersecurity protection from today's threats and where they stand in being prepared.

Cybersecurity is not just a technical problem that can be handed to your IT resources to be dealt with. It requires an all-in approach involving top management, IT staff, cybersecurity experts and every employee. It is important to understand everyone's responsibilities, resources needed, and technologies involved to establish a solid approach to protecting your business from cyber-attacks.

Instructions

This self-assessment tool is intended to help senior leaders to get a handle on how their organization stacks up against today's small business best practices.

It is organized into three focus areas: 1. Cybersecurity Management, 2. Cybersecurity Expertise, 3. Cybersecurity Technologies. Questions with a "No" or "Don't Know" response represent a weakness in your cyber defenses and a potential threat to your business. It is advised that top management oversees the closure of these gaps as soon as practical to secure your business.

Part 1: Cybersecurity Management *Use the questions below to determine responsibilities of senior management to be involved in your cybersecurity program.*	Yes	No	Don't Know
1. Do you regularly communicate the importance of cybersecurity to all employees?			
2. Do you have regular training for all employees on cybersecurity? Does it include phishing tests?			
3. Do you have documented policies and procedures for cybersecurity?			
4. Do you have a dedicated budget for cybersecurity?			
5. Do you maintain an ongoing list of improvements needed for cybersecurity?			
6. Do you have an independent 3rd-party regularly conduct a gap assessment of your cybersecurity?			
7. Do you have cybersecurity metrics that are reviewed at the executive level?			
8. Do you have a cybersecurity plan in place for remote workers?			
9. Do you have a cybersecurity insurance policy and/or breach insurance policy?			
10. Are you confident that your business could resist/survive a cyber-attack within the next 12 months?			

DIGITAL
NETWORKING SOLUTIONS
TECHNOLOGY BASED SOLUTIONS FOR YOUR BUSINESS CHALLENGES

Part 2: Cybersecurity Expertise *Use the questions below to evaluate your people resources focused on cybersecurity.*	Yes	No	Don't Know
1. Do you have a cybersecurity expert (3rd-party or in-house) separate from your IT team/resource?			
2. Does your cybersecurity expert monitor, report and take action on potential incidents or suspicious activity?			
3. Do you have someone who regularly evaluates and reports on new external cybersecurity threats to your business?			
4. Does your cybersecurity expert(s) have a CISSP, CompTIA Security+, or other advanced cybersecurity certification?			
5. If using a 3rd-party managed service provider (MSP), have you reviewed the service-level agreement (SLA) to ensure all services are being provided?			

Part 3: Cybersecurity Technologies *Use the questions below to review your cybersecurity technologies. You may wish to review this list with your IT resources (internal or external).*	Yes	No	Don't Know
1. Do you have a business-class firewall that is monitored and updated regularly?			
2. Do you have a daily, encrypted, off-site backup of your critical data and is restoration regularly tested?			
3. Do you have multifactor authentication (MFA) activated for all applications where it is available?			
4. Do you have a password management application in use such as LastPass or 1Password?			
5. Do you conduct regularly scheduled internal and external vulnerability scans?			
6. Do you have a patch management solution (RMM) in place?			
7. Do you have antivirus and endpoint detection and response (EDR) applications for all devices and are they updated regularly?			
8. Are device and system logs turned on and monitored 24x7 with a security information and event management (SIEM) system or equivalent?			
9. Do you have a web filtering application in place?			
10. Do you have a mobile device management (MDM) application for all mobile devices?			

Your Results

23-25 marked with "Yes": You're on the right path.

18-22 marked with "Yes": You have several critical vulnerabilities that should be addressed ASAP.

Less than 18 marked with "Yes": Your cybersecurity efforts are not effective, and your business is highly vulnerable to a cyber-attack.

Want Help?

Digital Networking Solutions can help you address any gaps on this list of essential cybersecurity best practices. Contact us at digitalnetworkingsolutions@protonmail.com or call us at **(246) 231-4269** to review your results and learn about our affordable support programs to help you shore up your company's cybersecurity protection.

DIGITAL
NETWORKING SOLUTIONS
TECHNOLOGY BASED SOLUTIONS FOR YOUR BUSINESS CHALLENGES