9 Cybersecurity Tips Every Business Should Follow

The global shift to remote working environments has created an open season for cybercriminals. No business—big or small—is exempt. Strengthening your company's security posture is essential right now.

1. Conduct a security risk assessment. Understand the most critical threats to your business, like system failures, natural disasters, malicious human actions and determine the impact they may have on your company.

2. Train your employees. Conduct employee awareness training across your entire workforce to educate users on common scams and avoidance techniques. Cybersecurity threats are constantly evolving, make sure your training curriculum is relevant and updated frequently.

3. Use multiple layers of protection. Implement a password policy that requires strong passwords. Monitor your employee accounts for breach intel with dark web monitoring. Deploy a firewall, VPN, and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Require everyone to have multi-factor authentication. Deploy ongoing network monitoring and encrypt sensitive data.

4. Keep software up to date. Unpatched or out-of-date software will allow some kind of threat to breach your security. Cybercriminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

Managed service providers (MSPs) can automate updates with a remote monitoring and management tool.

5. Create straightforward cybersecurity policies. Create and distribute a clear set of guidelines on cybersecurity practices for employees. Every business should include an acceptable use policy based on their business. Other important policies to consider are social media use, bring your own device (BYOD) and authentication requirements.

6. Back up your data. Daily (or more frequent) backups are a requirement to recover from data corruption or loss resulting from security breaches. Consider using a data protection tool with your MSP's help that takes incremental backups of data periodically throughout the day to prevent data loss.

7. Enable uptime. Choose a powerful data protection solution that enables "instant recovery" of data and applications. In fact, 92% of MSPs report that clients with business continuity disaster recovery (BCDR) products in place are less likely to experience significant downtime from ransomware. Application downtime can significantly impact a business' ability to generate revenue.

8. Know where your data resides. The more places data exists, the more likely it is unauthorized individuals will be able to access it. Use data discovery tools to find and secure data along with business-class Software-as-a-Service (SaaS) applications that allow for corporate control of data.

9. Control access to computers. Each access point poses an individual risk, so limit employee access to specific data they need to perform their jobs. Plus, administrative privileges should only be given to trusted staff.

Partnering with a managed service provider will alleviate your cybersecurity concerns. Working with an MSP will give you access to expert advice on what technologies you need to protect your organization in the fight against cybercrime. To learn more about our services, contact us today.

www.icscomplete.com