BREA NETWORKS

9 Cybersecurity Tips Every Business Should Follow

A massive global shift to remote working environments has created an open-season for cybercriminals. No business—big or small—is safe. Small and medium businesses (SMBs) seemingly have a target on their backs, so strengthening your company's security posture is essential right now.

There are ways to protect business data against ransomware attacks. Here are nine tips to help your business boost resilience to cyber attacks:

1. Conduct a security risk assessment. Understand the most critical threats to your business, like system failures, natural disasters as well as 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. Also, because 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 and monitor your employee accounts for breach intel through dark web monitoring. Deploy firewall, VPN, and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Extras: Consider mandatory multi-factor authentication, ongoing network monitoring, and hard drive encryption.

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 Unpatched or out-of-date software will allow some kind of threat to breach your security.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 this for businesses just like yours, with a remote monitoring and management tool. Don't forget to keep your mobile phones up to date as well.

5. Create straightforward cybersecurity policies. Write and distribute a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business but may include policies on social media use, bring your own device (BYOD), authentication requirements, and more.

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 and are back up and running quickly. 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 that unauthorized individuals will be able to access it. Use data discovery tools to find and appropriately 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 quality advice on what technologies you need to protect your organization in the fight against cybercrime. To learn more about our services, contact us today.