datto

9 Cyber Security Tips for MSPs to Bring to Their Clients

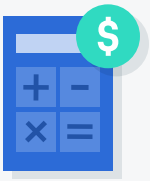
A massive global shift to remote working environments has created an open-season for cybercriminals. No business—big or small—is safe. Small and medium businesses (SMBs) seemingly have a target on their backs, so strengthening your clients' security posture is essential right now.

There are ways to protect business data against ransomware attacks. Here are nine tips you can share with clients to help them boost resilience to cyber attacks:

1. Conduct a security risk assessment. Understand potential security threats, like downtime from ransomware, and the impact they may have on your business.

Show your clients how costly just a few hours of downtime can be.

CALCULATE DOWNTIME COSTS →



2. Train your employees. Because cyber security threats are constantly evolving, an ongoing training plan should be implemented for all employees. This should include examples of threats, as well as instruction on security best practices.

3. Protect your network and devices. 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. Be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data. Managed service providers (MSPs) can automate this for businesses with a remote monitoring and management tool. Don't forget to keep your mobile phones up to date as well.

5. Create straightforward cyber security policies. Write and distribute a clear set of rules and instructions on cyber security 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 managed service provider'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 unauthorised 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. Use key cards or similar security measures to control access to facilities, ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted staff.

Small businesses have a trusted advisor in their managed service provider to advise them on the technology, tools, and practices needed to protect themselves in the fight against cybercrime. Stay vigilant, stay in the know, and always err on the side of caution.