CYBER SECURITY CHECKLIST

With cyber attacks on the rise, it's more important than ever to make sure your customers are properly protected from this growing threat. In our cybersecurity toolkit, MSPs can access tools to educate SMBs about protecting their business (and data) from cyber attacks before it's too late. Ransomware continues to attack businesses of all sizes, and lack of employee training is largely to blame. To help MSPs educate businesses about ransomware, we created a checklist to share with clients to help ensure critical business data is protected.

- [ ] **1) Conduct a Security Risk Assessment:** Understand potential security threats (e.g., downtime from ransomware) and the impact they may have on your business (lost revenue). Use this information to shape a security strategy that meets your specific needs.

- [ ] **2) Train Employees:** Because cybersecurity threats are constantly evolving, an ongoing semi-annual training plan should be implemented for all employees. This should include examples of threats, as well as instruction on security best practices (e.g., lock laptops when away from your desk). Hold employees accountable.

- [ ] **3) Keep Software Up-to-Date:** It is essential to use up-to-date software products and be vigilant about patch management. Cybercriminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

- [ ] **4) 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 internet use, social media use, BYOD, authentication requirements, etc.

- [ ] **5) Backup Your Data:** Daily backups are needed to recover from data corruption or loss resulting from security breaches. Consider using a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.

- [ ] **6) Enable Uptime:** Choose a modern data protection solution like Datto's that enables "instant recovery" of data and applications. Application downtime can significantly impact your business' ability to generate revenue.

- [ ] **7) Know Where Your Data Resides:** Maintaining oversight of business data is an important piece of the security puzzle. The more places data exists, the more likely it is that unauthorized individuals will be able to access it. Avoid "shadow IT" with business-class SaaS applications that allow for corporate control of data.

- [ ] **8) Control Access to Computers:** Use key cards or other Multi-Factor Authentication security measures to control access to facilities, and ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted IT staff.

Want to learn more about cybersecurity best practices? **Contact LAN Infotech at (954) 717-1990 or sales@laninfotech.com.**

LAN Infotech
YOUR TECHNOLOGY IS OUR BUSINESS

5100 NW 33rd Avenue, Suite 250 • Fort Lauderdale, FL 33309 • (954) 717-1990 • sales@laninfotech.com