Cybersecurity Checklist

According to a recent SEC report, SMBs are the “principal target” of today’s cyber attacks. Use this checklist to be sure your critical business data is protected.

☑ Keep software up-to-date

It is essential to use up-to-date software products and be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

☑ Caution using virtual private networks

While VPNs provide an encrypted tunnel between workstations and servers, it’s a direct connection so all the same safeguards you have in your office must be deployed on the computer connecting through VPN.

☑ 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” by using business-class SaaS applications that allow for corporate control data.

☑ Protect your network and devices

- Implement a password policy that requires strong passwords that expire every 90-days.
- Implement multi-factor authentication.
- Deploy firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Ongoing network monitoring is also considered essential.
- Encrypt hard drives.

☑ Implement End Detection and Response (EDR)

Protecting against viruses and ransomware still is one of the most important things you can do to protect yourself. Make sure your EDR/virus protection is connected to a Security operations center.

☑ Back up your data

Daily backups are a requirement 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.

☑ Enable uptime

Choose a modern data protection solution that enables “instant recovery” of data and applications. Application downtime can significantly impact your business’ ability to generate revenue.

☑ Train your 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 pratices (e.g., lock laptops when away from your desk). Hold employees accountable.

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

www.visualedgeit.com | learnmore@visualedgeit.com