SMB SECURITY TOP 10 CHECKLIST

uplevel SYSTEMS

		GOOD	BETTER	BEST
Passwords	Do you use & train users on creating secure passwords? Do you enforce a password policy?	No default or commonly used passwords to protect against simple guessing of passwords.	Enforced password policy that ensures policy compliance including complexity and reset frequency.	Multifactor authentication (MFA) to ensure multiple, unrelated criteria are needed to login.
Endpoint protection & anti-malware	Do you use and train users on creating secure passwords? Do you enforce a password policy?	Free / built-in options: Windows Defender, free version of Malware Bytes	Paid anti-malware tools that provide enhanced protection to malware	Endpoint protection solutions that protect against malware and ransomware recovery
E-mail	Is your email protected against spam, viruses, and phishing?	Free services that provide automated scanning and spam classification such as Gmail.	Paid services with that verify sender authenticity, block spam, and maximize uptime.	Automatic encryption of email to protect message privacyEmail service with automatic encryption
Backup	Ultimate protection against data loss.	Local backups protect against data loss due to user error and ransomware on file servers.	Local + cloud backups protect against site catastrophes such as flooding.	Automated snapshots provide for business continuity on critical devices.
Firewall	What type of firewall do you use ?	Stateful firewall blocks unsolicited Internet traffic from the LAN	Intrusion detection and preventions systems protect against malware embedded inside requested traffic.	Virtual execution-based inspection protects against many zero-day threats injected through code execution.
Updates	Do you regularly apply the latest patches from vendors ?	Automated OS and application patches to all IT components and malware signature updates for all endpoint protection.	Automated OS and application patches to all IT components and malware signature updates for all endpoint protection.	Automated OS and application patches to all IT components and malware signature updates for all endpoint protection.
Encryption	What types of your transactions use data encryption?	Remote connections over the Internet should be encrypted end-to-end & application servers should require a VPN to connect.	Data at rest ensures that any data that is stored locally or in the cloud is encrypted.	Email encryption should be used to protect against inspection or modification.
Web filtering	Do you filter communications in or out of your network to detect & remove threats?	Black lists generally allow users access to most websites on the Internet except specific sites.	White lists generally block users access to most websites on the Internet except specific sites.	Dynamic categories block user access to entire categories of websites such as alcohol, or social media.
Security Assessments	Do you perform regular assessments of your security defenses & procedures?	Annual security assessments are run and deficiencies corrected in slowly changing businesses.	Every 6 months security assessments	Every 3 months security assessments are appropriate for highly-regulated or high-churn businesses.
Training	What training do you provide staff /employees ?	Basic training is presented in person and explains best practice and company policies.	Advanced training uses online curriculum to explain and quiz users on data security.	Expert training actively tests users through live activities.