Small Business Cybersecurity Self-Assessment Checklist

Mark Yes / No / Not Sure for each question. Use this checklist to quickly see where your business stands.

Question	Yes	No	Not Sure
--- Foundational Layer - Securing Your Core Assets ---			
Do you maintain an up-to-date inventory of all hardware (computers, mobile devices, routers, IoT etc.) used in your business?	■	■	■
Do you keep track of all software and cloud services in use, including version numbers, licenses, renewal dates, and responsible users?	■	■	■
Do you map out where all critical data is stored (on-site servers, cloud, employee devices), who has access, and how sensitive it is?	■	■	■
Do you have a formal password policy (minimum length, complexity, uniqueness)?	■	■	■
Are strong passwords used everywhere and reused passwords avoided?	■	■	■
Is Multi-Factor Authentication (MFA) enabled on all critical accounts (email, cloud, admin access etc.)?	■	■	■
Do you apply software patches and updates routinely?	■	■	■
Do you have a schedule or process for patching non-critical systems and for firmware updates on devices?	■	■	■
--- Perimeter & Network Security ---			
Do you have a properly configured firewall (hardware and/or software) protecting your business network?	■	■	■
Are the default administrator usernames/passwords on routers, firewalls etc. changed from factory defaults?	■	■	■
Do you disable unnecessary features on network devices (e.g. UPnP) that might increase risk?	■	■	■
Is your WiFi network secured with modern encryption (WPA3 if possible, WPA2 minimum)?	■	■	■
Do you avoid using default SSIDs and weak WiFi passwords?	■	■	■
Do you run a guest network (isolated) for visitors / personal devices?	■	■	■
If employees or you access work resources remotely or on public networks, do you use a VPN or another encrypted channel?	■	■	■
--- Data Protection: Backup, Encryption, Access Controls ---			
Do you follow the '3-2-1 backup' rule (three copies, two different media, one off-site)?	■	■	■
Do you regularly test backups (restore a random set or full) to ensure they actually work?	■	■	■
Do you encrypt sensitive data at rest (on devices, servers) and in transit (over networks)?	■	■	■
Is the 'principle of least privilege' enforced: users have only the access they absolutely need, no shared admin accounts used for daily work?	■	■	■

Question	Yes	No	Not Sure
Do you review user permissions periodically (e.g. when roles change or people leave)?	■	■	■
--- Human Factors: Training & Policy ---			
Do you provide regular security awareness training (phishing, safe behavior, etc.) for all employees?	■	■	■
Do you run simulated phishing or similar drills to test readiness?	■	■	■
Do you have a documented 'Acceptable Use Policy' (AUP) that covers things like email/internet usage, device use, installing software, etc.?	■	■	■
If you allow personal devices (BYOD), is there a formal policy for how employees must secure those devices (e.g. encryption, passcode, remote wipe)?	■	■	■
--- Incident Readiness & Legal ---			
Do you have a written Incident Response Plan (IRP) that specifies what to do at each stage (preparation, detection, containment, recovery, lessons learned)?	■	■	■
Is there a contact list for who to call (IT support, legal, insurance, relevant authorities) in case of a breach?	■	■	■
Do you have cybersecurity insurance (and are you confident it covers things like ransomware, legal liabilities, etc.)?	■	■	■
Are you aware of all legal / regulatory obligations applicable to your business (data protection laws, breach notification requirements, industry standards such as PCI DSS etc.)?	■	■	■
--- Reflection & Prioritization ---			
Which three items from above do you feel are weakest in your current setup?	■	■	■
What is one action you could take this week to improve your cybersecurity posture?	■	■	■