FREE RESOURCE / XBITIUM SECURITY

The Small Business Security Checklist

27 things that actually matter, in the order they matter.

Most security checklists are written to be comprehensive. This one is written to be **survivable**. The items are ordered by how small businesses actually get breached — not alphabetically, and not by how easy they are to explain. If you only ever do the first section, you will have eliminated the majority of the real-world risk to a business your size.

HOW TO USE THIS

Work top to bottom. Do not skip ahead to the interesting parts. Section 1 is boring, and it is where nearly every breach of a company under 100 people actually begins. Anything you cannot answer confidently is a finding, not a shrug.

1. The front doors (critical)

Automated software scans every IP address on the internet, constantly, looking for these exact things. It does not check your revenue first. This is how it happens.

Done	Control	Why this one matters
☐	**No remote desktop (RDP/3389) exposed to the internet**	The single most common ransomware entry point for companies under 100 people. If anyone can reach it from anywhere, assume it is being attacked right now. Put it behind a VPN.
☐	**Multi-factor authentication on email, VPN, and admin accounts**	Stolen passwords are worthless without the second factor. This one control defeats the majority of account takeovers. Turn it on today, not next quarter.
☐	**Firewall and VPN firmware patched within 30 days**	The device guarding your network is often the least patched thing you own. Edge devices are attacked within days of a vulnerability being published.
☐	**No default or shared admin passwords anywhere**	A default login on a printer, camera, or NAS is a doorway into everything else on the same network.
☐	**Staff emails checked against public breach dumps**	If someone reused a password that leaked from another site, an attacker already has valid credentials. Check haveibeenpwned.com for your domain.
☐	**Nobody uses a personal email account for company business**	You cannot secure, monitor, or recover an account you do not control.

2. When it goes wrong anyway (high)

You will eventually have a bad day. These items decide whether it is an inconvenience or the end of the business.

Done	Control	Why this one matters
☐	**Backups exist, and at least one copy is offline or immutable**	Ransomware deliberately hunts and encrypts backups first. A backup an attacker can reach is not a backup.
☐	**You have actually RESTORED from backup in the last 90 days**	An untested backup is a hope, not a plan. Most failed restores are discovered on the worst day of the year.
☐	**A written incident response plan exists and names who to call**	At 2am nobody improvises well. Written down, or it does not exist.
☐	**Cyber liability insurance is in force and you know what it requires**	Many policies are void if you did not have MFA enabled. Read the conditions before you need to claim.
☐	**Critical systems are documented (what runs where, who owns it)**	You cannot protect or rebuild what nobody has written down.

3. People (high)

Your staff are the largest attack surface you own, and the only one that can be talked into opening the door voluntarily.

Done	Control	Why this one matters
☐	**Staff know how to report a suspicious email, and are never punished for it**	The goal is a fast report, not a perfect employee. Shame guarantees silence, and silence is what turns a click into a breach.
☐	**Payment and bank detail changes are verified by phone, on a known number**	Invoice fraud costs small businesses more than ransomware does. Never trust a bank-change request that arrived by email, even from your boss.
☐	**Departing staff lose access the same day they leave**	Ex-employee accounts are a favourite way back in, and nobody is watching them.
☐	**Admin rights are given only to people who genuinely need them**	If everyday users are administrators, one bad click compromises the whole machine.
☐	**Password manager in use; no passwords in spreadsheets or sticky notes**	Humans cannot remember 40 strong unique passwords. Stop asking them to.
☐	**Security awareness training happens more than once a year**	Annual training is a compliance ritual. Short, frequent, realistic practice is what actually changes behaviour.

4. The machines (medium)

Done	Control	Why this one matters
☐	**Operating systems receive automatic security updates**	Unpatched workstations are how a phishing click becomes a network-wide event.
☐	**Endpoint protection is installed AND someone reads the alerts**	Antivirus that nobody monitors is a smoke alarm with the battery removed.
☐	**Disk encryption is on for every laptop**	A stolen laptop is a data breach. Encrypted, it is just a stolen laptop.
☐	**No unsupported software still running (old Windows, old server apps)**	End-of-life software never gets patched again. The vulnerabilities are public and permanent.
☐	**Guest WiFi is separate from the business network**	Your guest network should never be able to reach your file server.

5. Everyone else's problems, which become yours (medium)

Done	Control	Why this one matters
☐	**You know which vendors can access your data or systems**	Your security is only as strong as your least careful supplier. Many breaches arrive through a trusted vendor's connection.
☐	**Vendor access is removed when the relationship ends**	Old integrations and API keys outlive contracts constantly.
☐	**Cloud storage is not publicly readable**	Misconfigured buckets and open shared drives leak data with nobody hacking anything.
☐	**You know where your customer data actually lives**	You cannot protect it, or report on it after a breach, if you cannot name it.

6. Proving it (low, but it wins you deals)

Done	Control	Why this one matters
☐	**Written security policies exist, even if short**	Increasingly required by clients, insurers, and regulators. Two good pages beat forty unread ones.
☐	**Someone is accountable for security by name, not by committee**	If everyone is responsible, nobody is.
☐	**You scan for vulnerabilities more often than once a year**	New vulnerabilities are published every day. An annual scan is a photograph of a moving target.
☐	**You can answer a client's security questionnaire without panicking**	This is now a sales blocker, not an IT problem. Deals die here.

THE UNCOMFORTABLE PART

Read back through the items you left unchecked. Now imagine explaining each one to your largest client, your insurer, or a regulator — *after* an incident, with the benefit of hindsight. That is the real test, and it is the one that eventually gets applied.

WHEN YOU WANT TO KNOW WHAT IS ACTUALLY EXPOSED

A checklist tells you what *should* be true. A scan tells you what *is* true. Xbitium will scan your public-facing systems and send you a real report in 48 hours — free, nothing to install, no obligation. If you are in good shape, we will say so and leave you alone.

Request your free external scan at xbitiumsecurity.com