**SMB Cyber Security Health Check Toolkit**

**Prepared for: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Prepared by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Version: 1.1 | Last Updated: July 2025**

**Author:**

GitHub: [Nanobyte1991](https://github.com/Nanobyte1991)

**Introduction**

Cyber security isn’t just for big companies.

If you run a small or mid-sized business, you’re a target. That might sound worrying, but being prepared doesn’t have to be complicated, expensive, or highly technical.

This toolkit was built specifically for **SMBs** like yours. It avoids confusing jargon and unrealistic expectations. Instead, it gives you a **simple, practical way to check how protected you are right now, and where you can make improvements.**

**What This Toolkit Helps You Do**

* Understand your biggest risks
* Get a clear score to track progress
* Build a short list of quick improvements

Most of all, it gives you **clarity and peace of mind**.

**How This Toolkit Fits Best Practice**

This toolkit aligns with recognised cyber security frameworks but keeps things simple.

| **Security Area** | **Industry Reference** |
| --- | --- |
| Know your systems & services | Asset Management (NIST, CIS) |
| Control access properly | Access Management (NIST, CIS) |
| Protect computers & devices | Device Protection (CIS) |
| Keep everything updated | Patching & Hardening (CIS) |
| Detect problems early | Threat Detection (NIST) |
| Plan for incidents | Incident Response (NIST, CIS) |
| Backup your data | Backup & Recovery (CIS) |
| Manage supplier risks | Vendor Security (NIST, CIS) |
| Keep improving | Ongoing Review (NIST, CIS) |

**Cyber Security Health Checklist**

**Systems & Equipment**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you have an up-to-date list of all computers, cloud services, and staff accounts? |  |
| Are the most important systems (email, backups, admin accounts) clearly flagged as critical? |  |
| Do you keep track of any unofficial or unauthorised IT use (known as ‘Shadow IT’)? |  |
| Do you review your list of systems regularly (monthly or when things change)? |  |

**Passwords & Access**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you use Multi-Factor Authentication (MFA) for key systems? |  |
| Are admin accounts properly restricted and monitored? |  |
| Do you have a clear process for adding and removing user access? |  |
| Do you review who has access every few months? |  |

**Protecting Devices**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Is anti-virus or endpoint protection installed and active on all devices? |  |
| Are protections set up so staff can’t turn off security by mistake? |  |
| Do you review security alerts from devices in one place? |  |

**Keeping Software Updated**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you install updates quickly when they’re released? |  |
| Do you follow security settings and hardening guides for devices? |  |
| Do you keep track of any exceptions? |  |

**Spotting Problems Early**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you have logging turned on for email, firewalls, and key systems? |  |
| Are alerts set up to notify you of important issues (not just noise)? |  |
| Do you have a process for escalating security concerns? |  |

**Being Ready for an Incident**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you have a simple plan for incidents like phishing, ransomware, or data loss? |  |
| Do staff know who is responsible for what in a crisis? |  |
| Have you tested your plan at least once a year? |  |

**Backups**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you back up important data every day? |  |
| Do you test restoring a file regularly (at least quarterly)? |  |
| Do your backups include cloud services (e.g. Microsoft 365, Google)? |  |

**Cloud & Online Services**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Is MFA and logging switched on for services like Microsoft 365 / Google? |  |
| Are admin roles limited and reviewed? |  |
| Are shared files and permissions reviewed regularly? |  |

**Suppliers & Partners**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Do you keep a list of suppliers who have access to your systems? |  |
| Do contracts cover security basics like breach notification and MFA? |  |
| Do you review supplier security at least once a year? |  |

**Keeping Security on Track**

| **Question** | **Answer (Yes / No / Partial)** |
| --- | --- |
| Is someone clearly responsible for each security area? |  |
| Do you have a roadmap of improvements? |  |
| Do you track progress with basic metrics (alerts, updates, incidents)? |  |

**Scoring & Progress**

Give yourself points for each section:

| **Category** | **Max Points** | **Your Score** |
| --- | --- | --- |
| Systems & Equipment | 10 |  |
| Passwords & Access | 15 |  |
| Protecting Devices | 10 |  |
| Keeping Software Updated | 10 |  |
| Spotting Problems Early | 10 |  |
| Incident Planning | 15 |  |
| Backups | 10 |  |
| Cloud Security | 10 |  |
| Supplier Security | 5 |  |
| Ongoing Review | 5 |  |
| **Total** | **100** |  |

**Maturity Levels**

| **Score Range** | **Level** | **What It Means** |
| --- | --- | --- |
| 0–30 | Basic | Urgent fixes needed (MFA, backups, patching). |
| 31–60 | Defined | Some protections in place, but inconsistent. |
| 61–85 | Proactive | Good coverage—review and improve regularly. |
| 86–100 | Mature | Strong posture—focus on keeping it that way. |

**Quick Wins for Small Businesses**

Here are **5 easy things you can do right now**:

1. Turn on **Multi-Factor Authentication (MFA)** for emails, cloud apps, and admin accounts.
2. Check your backups are running—and try restoring a file this week.
3. Remove unused accounts, especially for people who have left.
4. Install any pending software and security updates.
5. Send staff a reminder about spotting phishing emails.

**Common Cyber Threats**

| **Threat** | **How This Toolkit Helps** |
| --- | --- |
| Phishing | Access Control, Alerts, Incident Planning |
| Ransomware | Backups, Updates, Response Planning |
| Stolen Passwords | Access Control, Device Protection |
| Data Loss | Backups, Device Protection |
| Supplier Risk | Supplier Management, Access Control |
| Outdated Software | Updates & Patching |
| Malware | Device Protection, Alerts |
| Insider Risk | Access Control, Reviews |

**Risk Prioritisation Example**

| **Risk** | **Likelihood** | **Impact** | **Priority** | **Action** |
| --- | --- | --- | --- | --- |
| Phishing attack | High | Medium | High | Enable MFA & Train Staff |
| Unpatched software | Medium | High | High | Install Updates |
| Leaver account active | Low | High | Medium | Remove Access |

**Next Steps**

1. **Complete the checklist**
2. **Review your scores and pick top risks**
3. **Fill in the action plan below**

**Action Plan Template (exsamples)**

| **Top Risk** | **Next Action** | **Who’s Responsible** | **By When** |
| --- | --- | --- | --- |
| Phishing | Turn on MFA | IT Lead | Next Week |
| Backups | Test Restore | Operations | End of Month |

**Resources & Support**

Free guidance is available:

* [NCSC Small Business Guide (UK)](https://www.ncsc.gov.uk/collection/small-business-guide)
* [CISA SMB Resources (US)](https://www.cisa.gov/small-business)

**Author:**

GitHub: [Nanobyte1991](https://github.com/Nanobyte1991)