The 7-Point Cybersecurity Risk Checklist

EVERY ORGANISATION SHOULD RUN IN 30 MINUTES

Introduction

Is your organisation cyber-secure? *Run this 7-point risk check before a breach does it for you*. This checklist is designed to provide a rapid assessment of your organisation's cybersecurity posture.

How to Use This Checklist

- **Designed for:** Business owners, directors, board members, operations managers, and IT/admin staff.
- **Time Required:** 30 minutes.
- **Instructions:** Be honest with your answers. If unsure, treat the item as a risk. Complete each section and note the number of raised concerns to derive a final risk summary.

1. Email & Phishing Risk

Email is the number one entry point for cyber attacks.

Check all that apply:

□ Staff use strong, unique passwords for email accounts
□ Two-factor authentication (2FA) is enabled on email
□ Staff are trained to recognise phishing and suspicious links
□ No shared email passwords across staff
□ Suspicious emails are reported, not ignored

Risk Indicator: If 2 or more boxes are unchecked → **High Risk**

2. Data Storage & Access Control

Sensitive data is valuable—to you and attackers.

□ Sensitive data (client, staff, financial) is clearly identified
□ Access to sensitive data is limited to authorised staff only
□ Former employees no longer have system access

□ Data is not stored on personal devices without approval
□ Cloud storage access is properly controlled

Risk Indicator: Uncontrolled access = **Immediate Risk**

3. Website & Online Systems Security

Your website is a public-facing attack surface.

□ Website uses HTTPS (secure lock icon)
□ Software, plugins, and CMS are up to date
□ Website admin access is restricted
□ Backups are taken regularly
□ Hosting provider offers security monitoring

Risk Indicator: Outdated systems = **High Breach Probability**

4. Device & Network Security

Every laptop, phone, and router matters.

□ Work devices require passwords or biometric locks
□ Antivirus or endpoint protection is installed
□ Devices are updated regularly
□ Public Wi-Fi usage is restricted or secured
□ Lost or stolen devices can be remotely locked or wiped

Risk Indicator: Unprotected devices = **Silent Exposure**

5. Backup & Incident Preparedness

Security is not just prevention—it's recovery.

□ Critical data is backed up regularly
□ Backups are stored securely and separately
□ Someone knows what to do during a cyber incident
□ Incident response contacts are defined
□ Downtime risks are understood

Risk Indicator: No backup plan = **Business disruption risk**

6. Staff Awareness & Human Risk

People are your strongest—and weakest—link.

□ Staff have received basic cybersecurity awareness training
□ Password sharing is discouraged
□ Clear IT and security policies exist
□ Staff understand data protection responsibilities
□ Cybersecurity is discussed beyond IT teams

Risk Indicator: Untrained staff = **High likelihood of breach**

7. Governance, Compliance & Oversight

Cybersecurity is a management responsibility, not just IT.

□ Leadership understands cybersecurity risks
□ Policies exist and are enforced
□ Regulatory requirements are known
□ Third-party risks are considered
□ Cybersecurity is reviewed periodically

Risk Indicator: No oversight = **Strategic exposure**

🔍Risk Summary

Count how many sections raised concern:

- **0–1 risks:** Low risk (maintain controls)
- **2–3 risks:** Medium risk (action required)
- **4+ risks:** High risk (professional assessment recommended)

This summary provides a high-level indication of your organisation's cybersecurity risk level.

What This Checklist Does—and Doesn't—Do

✓ Helps you **identify risk areas quickly**
✓ Creates awareness and clarity
✓ Supports informed decision-making

✗ Does not replace a professional cybersecurity assessment
✗ Does not fix vulnerabilities automatically

Next Steps

If your results show **medium to high risk**, the next step is **professional review and remediation**.

A structured cybersecurity assessment will:

- Identify hidden vulnerabilities
- Prioritise risks
- Provide clear, actionable recommendations

About Retis Systems

Retis Systems provides **cybersecurity consulting, risk assessments, vulnerability testing, secure software development, and capacity building** for organisations that value security, compliance, and resilience.

Want a Professional Review?

If you'd like a cybersecurity expert to review your checklist results and advise on next steps, you can book a short consultation.

📧 Contact: info@retistech.com
🌐 Website: www.retistech.com