ingenio
TECHNOLOGIES

Cyber Security Health Check Guide

ingenio TECHNOLOGIES

Clarity.
Real examples.
Clear actions to take.

Cyber security isn't about fear, jargon or expensive tools.

It's about understanding where your business is exposed and fixing the gaps before they become incidents.

Here at Ingenio Technologies, we work with organisations across the South East who haven't had a breach – but can see that risk is quietly building through everyday IT decisions.

This guide explains what a Cyber Security Health Check really is, what it should cover, and how it helps business owners regain clarity and control.

No scare tactics.
No box-ticking.
Just practical guidance.

1. WHAT IS A CYBER SECURITY HEALTH CHECK?

A cyber security health check is a structured review of how well your business is protected against cyber threats, data loss and operational disruption.

It looks beyond antivirus software and focuses on how technology is actually used across your organisation.

A proper health check helps you understand:

- Where your real risks sit today
- How exposed your business would be if something went wrong
- Whether your controls match your size, sector and obligations

It's not about perfection.
It's about visibility and prioritisation.

Why it matters now

Cyber incidents are no longer rare – and they don't just affect large organisations.

UK Government research shows that around half of UK businesses experience a cyber security incident each year, with phishing being the most common entry point.

What we see most often is this:

- Security evolves slower than the business
- Access is added but never reviewed
- Cloud platforms are assumed to be "secure by default"
- Responsibility for cyber security becomes unclear

A health check brings structure, ownership and focus back into the picture.

2. UNDERSTANDING RISK VS EXPOSURE

These two terms are often confused, but the difference matters.

Risk

The likelihood of something going wrong

Exposure

The impact if it does

Example:

- A phishing email landing in an inbox is a risk
- A compromised account with access to finance systems, client data or backups is exposure

Reducing risk helps.
Reducing exposure limits damage.

A cyber security health check looks at both.

UK Government research shows that around 50% of UK businesses experienced a cyber security breach or attack in the past 12 months.

What's notable is that many of these incidents were not the result of sophisticated hacking, but everyday weaknesses such as phishing emails, weak account security and unreviewed access.

Source: UK Government Cyber Security Breaches Survey

3. WHAT A HEALTH CHECK SHOULD COVER

User access and permissions

- Who has access to which systems
- Whether access matches job roles
- Use of administrator accounts

Too much access increases exposure if an account is compromised.

Email security and phishing resilience

- Email filtering and threat detection
- Multi-factor authentication (MFA)
- How suspicious emails are reported

Email remains the most common entry point for attacks.

Device and endpoint security

- Patch management and updates
- Antivirus and endpoint protection
- Encryption on laptops and mobiles

Unpatched devices remain one of the easiest ways in.

Backup and recovery readiness

- How often backups run
- Whether they are monitored and tested
- Protection against ransomware

Backups only matter if they work when needed.

4. CLOUD, POLICIES & OWNERSHIP

Cloud security configuration

- Microsoft 365 security settings
- MFA enforcement
- External sharing controls
- Audit logs and alerts

Cloud platforms are powerful – but not secure by default.

Policies, processes and ownership

- Clear responsibility for cyber security
- Incident response planning
- Supplier and third-party risk awareness

Technology alone doesn't create security.

4. WARNING SIGNS

Signs a health check is overdue

You may be overdue if:

- Your business has grown quickly
- You rely heavily on Microsoft 365
- You're unsure who has access to what
- Backups have never been tested
- Cyber security has never been formally reviewed
- You operate in a regulated or data-sensitive sector

! Most businesses don't realise the risk until something breaks.

What a cyber security health check is not

It is not:

- A penetration test
- A compliance audit
- A sales pitch for more technology
- A generic checklist

It is a practical way to gain clarity and confidence.

4. OUTCOMES

What good outcomes look like

After a proper health check, you should have:

- A clear view of your current risk posture
- A prioritised list of improvements
- Practical, phased recommendations
- Confidence in what actually needs attention

At Ingenio Technologies, we focus on proportionate improvements that fit how your business really operates.

Rather than just sell you everything and hope that you're secure, we take a different route and perform a comprehensive security assessment to understand your risk.

We'll identify if your risk is high and requires a multi-layered security approach or if you only require basic security because you only use Microsoft Office and an app or two in the cloud.

Our security analysts conduct a thorough evaluation of your current security infrastructure, looking at potential security vulnerabilities and assessing your security posture.

This allows us to tailor our security service offerings to your specific needs, ensuring that your business is adequately protected without unnecessary costs.

Want a clearer view of your cyber security?

CONTACT US TODAY.

01273 806211
hello@ingeniotech.co.uk
www.ingeniotech.co.uk