Cyber security: Immediate recommended actions

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Cyber security threats are increasing in scale, sophistication, and impact. Every organisation, regardless of size, sector, or budget, must take steps to reduce its cyber risk. That includes charities, not-for-profits, and SMEs, many of which remain unaware of how exposed they really are.

This article will outline five key areas you can review as a business owner today. Each recommendation is actionable, cost-effective, and designed to immediately strengthen your cyber security posture.

Understanding cyber risk and how to assess it

Cyber risk refers to the potential exposure of business-critical information and systems to unauthorised access, loss, or damage.

Contrary to popular belief, this risk does not only apply to large enterprises. Over the last few years, attackers have increasingly targeted organisations with fewer resources and defences.

This is because cyber criminals often see smaller organisations as low-hanging fruit. Often having limited budgets and overstretched teams, these organisations lack dedicated cyber security expertise and strong defences, making them an easier target.

However, improving your security posture doesn't require expensive tools or a high level of technical knowledge.

In fact, many of the most effective actions are simple, affordable, and within your reach, as long as you know where to start. If you want to assess your cyber security and determine what changes you may need to make, you should adhere to industry standards and guidelines.

The CIA Triad is a globally recognised framework that focuses on three fundamental principles:

- **Confidentiality:** ensuring information is only accessible to those who are authorised
- **Integrity:** making sure data is accurate and unaltered
- **Availability:** ensuring systems and information are accessible when needed.

Understanding and applying the CIA Triad doesn't just enhance day-to-day security, it also forms the backbone of your Business Continuity Planning (BCP) and Disaster Recovery (DR) processes.

These principles help you prepare for and respond to incidents in a way that minimises disruption, protects critical data, and supports a swift return to normal operations.

Five key areas to review

Protecting your organisation doesn't have to be difficult. By focusing on a few fundamental areas, you can make immediate improvements to your security stance.

Here's where to start:

1. Backup your information & data

Disaster recovery depends on access to your data. Whether it's a cyber attack, hardware failure, or natural disaster, losing data can be catastrophic. Backup is your safety net.

Key actions:

- **Identify what needs to be backed up and how frequently.** Not all data is equal. Prioritise critical business data, applications, and systems that are essential to your operations.
- **Store backups away from your live IT systems.** Keeping a copy away from your infrastructure means cybercriminals would need to breach a second system to delete or encrypt your data, reducing the likelihood of ransom demands.
- **Regularly test your backups to ensure data can be restored.** Schedule regular test restores to confirm data integrity and recovery time.
- **Make backup part of your standard operating procedures.** Integrate it into your everyday operations with clear responsibilities, schedules, and checks.

2. Use basic technical controls

Many cyber attacks are preventable with basic technical controls. You don't need a big budget or complex systems, just consistent, good practice.

Key actions:

- Install (and turn on) antivirus software
- Prevent trustees, volunteers, or employees from downloading dodgy apps
- Keep all your IT equipment and software up to date (patching)
- Control how USB drives (and memory cards) can be used
- Switch on your firewall

3. Keep smart phone and tablets safe

With the rise of remote and hybrid working, mobile devices now handle vast amounts of sensitive data. Yet they are often overlooked from a security perspective.

Key actions:

- Install antivirus software on all devices
- Keep operating systems and apps up to date
- Enable device encryption and firewalls
- Limit installation of third-party apps
- Ensure lost or stolen devices can be remotely wiped

4. Use passwords to protect your data

Passwords are a frontline defence. When implemented correctly, they're one of the simplest and most effective security tools available.

Key actions:

- Enable password protection on all devices, PIN, fingerprint, facial recognition
- Avoid predictable or reused passwords
- Change default (manufacturer) credentials
- Use multi-factor authentication (MFA) for important accounts

- Use different passwords for work and personal use

5. Avoid phishing attacks

Key indicators of phishing:

- Email from free providers (e.g., @gmail.com) for "official" messages
- Slight misspellings in domain names (e.g., @microsft.com)
- Poor grammar, typos, and vague language
- Urgent messaging or scare tactics (e.g., "account locked")
- Suspicious links or attachments

What to do:

- Don't click on suspicious links or attachments.
- Don't share personal or financial information over email.
- Check for HTTPS and a padlock icon on websites.
- If unsure, verify the message by contacting the sender using a known contact method.

As a business owner, you must take ownership of your digital risk and take steps to protect your IT systems. For further guidance, speak with one of our specialists today.