Citation Cyber

Cyber Fitness Plan 2024

v01

Introduction

Let's get your cyber security in shape this 2024! Follow these simple exercises that will help you get the basics right and build a robust cyber security strategy. From passwords management to supply chains, software updates and incident response planning, these routines the ultimate cyber workout.

Exercise One: Passwords

Ensure your passwords are complex, random, and secure! In 2023, compromised credentials were the second highest initial attack vector accounting for 15% of all data breach cases!

- To avoid password fatigue, utilise passphrases when creating login credentials – a series of random words with no relation to one another.
- Introduce a password manager to store your login credentials in a centralised, secure location - also a great way to prevent password fatigue and reusing the same password across multiple accounts.
- Enable Multi-Factor Authentication (MFA) on all applicable accounts and devices – this adds an additional layer of security to the authentication process.

Exercise Two: Software updates

Keep your software up to date! During the winter break, your company devices may need a software update – enabling automatic updates ensures your technologies have the latest security defences and resolves any bug issues.

- Keep track of which versions of software are installed on your devices so that you can promptly enable pending updates.
- Install these as soon as they become available to fix any exploitable bugs on your devices.

Exercise Three: Update your response plan

When did you last test your incident response plan? Keeping this relevant and up-to-date can minimise the fallout in the event of an attack or breach. Hopefully, you won't ever need to use it, but it's absolutely crucial that you have one in place!

- If you have no response plan in place, look to implement one throughout your organisation covering, data backups, communications, steps to recovery, etc. **Need a bespoke incident response plan? Reach out to a member of our team!**
- Once you have your response plan implemented, look to test this every 6 – 12 months. Looking at how long your backups take to restore your data, what communication methods you use, and who has ownerships of each action.

Exercise Four: Cyber security health check

Get cyber secure this 2024! Whether your business is starting out on its cyber security journey, or you would like some peace of mind knowing that your internal capacities are operating as they should be, a **cyber security health check** is the optimal way to get you going.

- Gain visibility into your organisation's current risk level.
- Identify gaps in your security before cyber criminals do!
- Remain compliant with regulations such as the UK GDPR 2021.

Exercise Five: Security awareness training

Strengthen your human firewall with awareness training. Businesses can see a 70% reduction in socially engineered cyber threats when regular **cyber awareness training** is implemented.

- Power up your human firewall with targeted training that equips your staff with the latest cyber security guidance.
- Regularly implement training sessions to keep your workforce ahead of the curve with the latest hacking trends.
- Take your training one step further by implementing phishing simulations to keep your people vigilant and robust.

Exercise Six: Backups

How long could you continue business operations without your data? Up-to-date backups are the most effective way of recovering from an attack or breach as it allows you to promptly restore your company data and minimise downtime.

- Regularly back up your company data, ensuring these are automatically enabled.
- Create offline backups that are kept in an isolated location, separate from your company networks and systems.
- Test the backup restoration process every couple of months to understand how long it takes for you to recover.

Exercise Seven: Board Training

Leadership plays a crucial role in empowering your workforce to prioritise data and device protection. Cyber security is not just an IT issue; it's a core risk management issue and must begin from the top-down. Give your board the knowledge to lead the fight against cyber threats with **board-level cyber security awareness training**.

- Understand your role with defending against attacks.
- Position your business to be resilient against breaches.
- Remain compliant with security regulations.

Exercise Eight: Supply Chain

Securing your supply chain is critical to protect against 3rd-party data breaches. Enforce security protocols and mandate suppliers to comply with robust cyber security measures.

- Vett your suppliers and assess their cyber security measures.
- Ensure all sensitive information is transmitted and stored securely.
- Collaborate with suppliers to create a joint incident response plan.

Exercise Nine: Cyber Essentials

Cyber Essentials certification is a cost-effective, highly effective security tools for organisations of any size and sector. The government-backed scheme is used to demonstrate that organisations have the appropriate security and defences in place against common cyber attacks and data breaches.

- Prevents up to 80% of common cyber attacks.
- Showcase your commitment to device and data security.
- Tender for UK government and MOD contract bids.

We're here when you need us!

Do you want to become cyber secure? With our ongoing cyber security support, you can! We'll test, train, and certify your organisation to minimise data breaches and cyber attacks. Our cyber security packages allow you to rest easy knowing all the fundamentals are covered, whilst allowing you to reduce your risk for less – win, win!

Speak to a member of our team today on **0333 323 3981**
or get in contact with us below to get started!

CONTACT US

Citation Cyber