

Cyber Fitness Plan



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH EAST

Get your cyber health in shape this 2023 with our top workouts for your business.



Password Management

- Power up your security by switching your passwords to passphrases, a series of random words with no relation to one other.
- Introduce a password manager to store your credentials in a secure location - this helps prevent password fatigue.
- Enable multi-factor authentication to your company accounts and devices - adds an additional layer of security in the login process.

Software Updates

- Keep track of which versions of software are installed on your devices so that you can promptly target security updates.
- Install software updates as soon as they become available in order to fix exploitable bugs in your devices.
- Enable automatic updates for OSs, applications, and firmware, if possible.



Update Your Response Plan

- If you don't currently have a response plan in place, look to implement one throughout your organisation covering data backups, communications process, and steps to recovery.
- Once this is in place, ensure this is tested every 6-12 month - this includes looking at how long your backups take to restore your data, what communication methods you use, and ownership of each action.

Cyber Security Health Check

- A cyber health check will help you gain valuable insight into your organisation's current risk level.
- Identify the gaps in your security so you can implement the appropriate security defences that your business needs.
- Remain compliant with regulations such as the UK GDPR 2021.



Security Awareness Training

- Power up your human firewall with targeted training that equips your staff with the latest guidance to remain cyber secure.
- Ensure training is regularly introduced to help keep your workforce ahead of the curve with the latest security defences.
- Take your training one step further by implementing phishing simulations to keep your people vigilant and robust.

Vulnerability Assessment

- A Network Vulnerability Assessment tests your IT system configuration using the same techniques used by hackers to ensure your company is not wide open to a cyber attack.
- We can scan and review your internal networks and systems looking for weaknesses such as poorly maintained or designed systems, insecure Wi-Fi networks, insecure access controls, or opportunities to access and steal sensitive data.



@SouthEastCRC



CRCSouthEast



crc-south-east



enquiries@secrc.co.uk



secrc.co.uk



Backups

- It's critical for businesses to back up their data, as restoring your files from a backup is the quickest way to regain access to your data.
- Remember it's vital to keep one copy of your data separate to the original home of the data.

Phishing Scams

- Phishing scams are becoming harder to spot, poor grammar and spelling and low-quality versions of recognisable logos are common signs of Phishing attacks.
- Other things to look out for include checking the sender's email address to see if it looks legitimate or whether a company logo has been manipulated to look legitimate.



Board Training

- New regulations (such as GDPR) as well as high-profile media coverage on the impact of cyber incidents have raised the expectations of partners, shareholders, customers, and the wider public.
- Quite simply, organisations - and board members especially - have to get to grips with cyber security. If you are not regularly talking about cyber security at your board meetings, it's critical that you start.
- The National Cyber Security Centre have produced a [Board Toolkit](#) to help encourage essential discussions about cyber security to take place between the Board and their technical experts.



Cyber Security Policies

- Every business will follow a First Aid or Fire Alarm procedure, so why is cyber security any different? There are several policies that businesses need to adopt, they include a Bring Your Own Device Policy, Social Media policies and Risk Management/Incident Response policies.
- Take a look at our Cyber Incident Response Plan that will help you to identify the gaps within your business <https://www.secrc.co.uk/post/cyber-incident-response-plan>.



Supply Chain

- Cybercriminals target supply chains as a means of reaching the broadest possible audience with their malware. It's often perceived that small businesses are not big enough to be hit by a supply chain attack, however, it is not about how many people work for you or how many office locations you have.
- A supply chain attack can be carried out through the systems that you use. To help you secure your supply chain, you should ensure that your suppliers regularly conduct security audits or have security certifications and put this within your contract with them.

Cyber Essentials

- Cyber Essentials is an effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.
- Recently, the National Cyber Security Centre announced they are running a funded Cyber Essentials programme which will help small and micro businesses to implement baseline security controls and prevent the most common types of cyber-attacks.
- Qualifying organisations will receive around 20 hours of remote support with a Cyber Essentials Assessor. To qualify for this scheme, an organisation must either be a **micro or small business (1 to 49 employees) that offers legal-aid services or a micro or small charity that processes personal data, as defined under GDPR**



Learn more <https://www.ncsc.gov.uk/information/funded-cyber-essentials-programme>