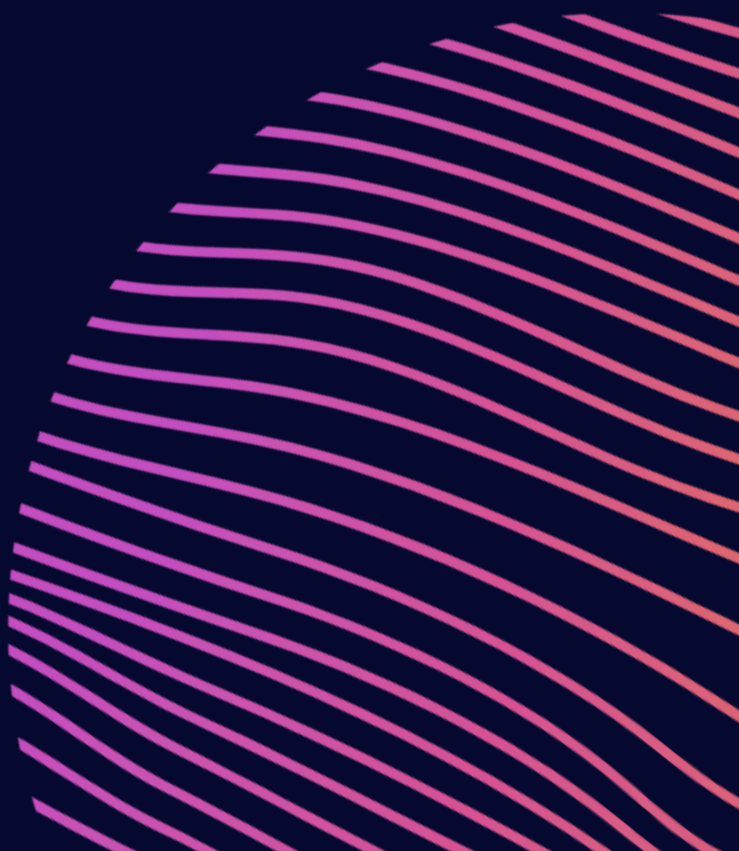
syn-star

Cyber Security Basics for Businesses

Note: This document is for ideas purposes and for information only.



syn-star
IT - Telecoms - Technology

3 MAIN AREAS

To make it easier to understand, we break down cyber security into 3 areas that you can easily measure and implement protection

1.0 Company Wide Data / Systems

Priority No. 1: Protect the entire business.

Data Protection: Safeguard the data itself and control access to it, both internally and externally.

System Security: Ensure the main systems that keep the business running are secure.

2.0 Your Devices

Device Protection: Establish a robust security perimeter around all your devices. This ensures your team can work efficiently while being less vulnerable to individual attacks and threats.

3.0 Your Users

Employee Awareness: Recognise that the majority of cyber breaches are caused by team members accidentally clicking on malicious links, downloading harmful software, or falling for phishing scams.
Educating your team on these risks is crucial.

Website
syn-star.co.uk

Email
hello@syn-star.co.uk

Call
0333 242 2447

syn-star
IT - Telecoms - Technology

PROTECT THE BUSINESS

Areas that are recommended to cover

1.0 Back-ups

Multiple Backups: Ensure you have multiple backups of your data, with at least one being a standalone backup that is not connected to your network.

No Local Storage: Avoid storing data locally on individual devices to prevent data loss in case of device failure or theft.

2.0 Disaster Recovery Planning

Comprehensive Plan: Develop a detailed disaster recovery plan that outlines the steps to take if access to your main database is restricted or if your primary data is lost or corrupted.

Action Steps: Include specific actions for different scenarios, such as data restoration procedures and communication plans.

3.0 Login & Passwords

Administrative Controls: Utilise the administrative controls provided by modern platforms to enforce security measures that prevent unauthorised access.
Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security.
Geographic Restrictions: Set geographic restrictions to limit access based on location.
Access Levels: Define and enforce different levels of access based on user roles and responsibilities.

4.0 Access

Regular Reviews: Regularly review who has access to various software and data within your organisation.

Onboarding and Offboarding: Ensure that access reviews are part of your onboarding and offboarding processes.

Website
syn-star.co.uk

Email
hello@syn-star.co.uk

Call
0333 242 2447

syn-star
IT - Telecoms - Technology

PROTECT YOUR DEVICES

Individual Devices can be network equipment, servers and end user devices

1.0 Automate

Unified Protection: Ensure all devices are part of a cohesive protection system. Avoid having standalone devices that are manually managed by users.

2.0 Fully Managed Protection

Centralised Security: Do not rely on standalone security software that users can choose to run. Ensure that your entire security suite and operating systems are consistently updated and patched.

3.0 Zero Trust & Ransomware Protect

Layered Security: Implement multiple layers of protection to prevent the spread of attacks. Limit user permissions to install software and access certain areas to reduce risks and enhance tracking capabilities.

4.0 Reviews your Security Suite

Continuous Evolution: As hacking methods evolve, so should your security measures. Regularly review and update your security suite to ensure it remains effective against new threats.

Website
syn-star.co.uk

Email
hello@syn-star.co.uk

Call
0333 242 2447

syn-star
IT - Telecoms - Technology

EDUCATE / PROTECT USERS

Your biggest risk to your business is your users accidentally doing the wrong thing

1.0 Cyber Training

Regular Sessions: Conduct short, focused training sessions on a monthly basis to cover various aspects of cyber risks over time.

Induction Training: Integrate cyber security training into the induction process for new employees to ensure they are aware of potential risks from the start.

2.0 Anti-Spam

Email Vigilance: Recognise that emails remain the primary method hackers use to trick employees into installing malicious software or entering sensitive information on fake websites.

3.0 Spoof Phishing Emails

Testing and Awareness: Regularly test your team with simulated phishing emails. This proactive approach helps employees become more vigilant and better at identifying potential fake emails and bogus websites.

4.0 Managed Devices

Centralised Management: Relieve employees of the responsibility for running updates and security scans by having devices managed centrally by an outsourced IT provider. This ensures all devices are consistently up-to-date and secure.

Website
syn-star.co.uk

Email
hello@syn-star.co.uk

Call
0333 242 2447