



technical drive



CYBER SECURITY

**AN SMBs GUIDE FOR
STAYING CYBER SECURE**



Introduction

A worrying comment we sometimes hear is “we’re too small’ to be targeted by cyber-crime” or “it doesn’t happen in our industry”.

It can happen to a business of any size in any industry.



Small-to-medium sized businesses (SMBs) may think they’re not at risk from cyber crime, but unfortunately, that’s not the case. It may be data breaches and cyber hacks that happen to large corporations that usually make the headlines, it actually happens more frequently to SMBs.

Enterprises usually have the resources to invest heavily in IT security strategies, however very few SMBs have dedicated personnel to address IT issues and run routine security checks. Even those who do have in-house IT, often find that their internal resources are too busy with other tasks to properly address security upkeep.

By not investing in adequate cyber security protection, you’re leaving your business vulnerable to cyber criminals. You take measures to protect your physical environment to prevent criminals from gaining access, you should adequately protect your digital environment.

81%

of cyber-attacks and data breaches targeted SMBs.

UK Government Cyber Security Breaches Survey 2024

SMBs are most at risk of cyber attacks

Government statistics back-up that SMBs are a common target for cyber criminals.

At Technical Drive we want to help prevent businesses suffering from cyber-attacks.

This guide explains the risks and offers some practical advice on the steps you can take to ensure your business is protected.

Government statistics back this, The UK Government Cyber Security Breaches Survey 2024 found that:



of cyber-attacks and data breaches targeted SMBs.



of UK businesses reported cyber-attacks or security breaches in the past year



of small businesses in the UK experienced phishing, the most common cybercrime

How do cyber criminals make their money?

By the time you're aware of a hack the damage has been done

The strategies and techniques of cyber criminals are constantly evolving, and it's now seen as more lucrative to target multiple smaller businesses than look for one 'big heist'.

Cyber criminals, often steal data in small increments over time to avoid detection. With this approach, organisations that don't monitor their systems may not even realise there has been a breach for days or even weeks – by which time the damage has already been done.

Another common tactic by cyber criminals is Distributed-Denial-of-Service (DDoS) attacks. The objective of this type of attack is to disrupt your technology infrastructure and prevent you accessing your own network. If ransomware is deployed within your IT infrastructure, it will put your data and systems under lock and key, with the hacker demanding a high price to give you back control.

**SMBs can't afford to think
"it won't happen to us"...**

Owners of SMBs may see a DDoS attack in the media and think it's not relevant to them. However, it's estimated that there are an average of 1.29 DDoS attacks every two minutes throughout the world, and any one can be a victim.



It may not be your data they want!

Cyber criminals know that poor IT security can often provide a gateway to either your supply-chain or clients.

Trojan attacks

If you're connected to your suppliers, clients or regulators, it makes you an attractive entry point for stealing the data of a larger organisation or company, which may have more sophisticated security processes in place.

Smaller associated organisations can, often unknowingly, become a **'Trojan horse' for a hacker using Malware** to gain backdoor access to a larger organisations' data.

For this reason, many companies and organisations will ask you for specifics on how their data will be safeguarded before they sign an agreement.

Can you prove that you're secure?

Some enterprises may require an independent security audit of your systems to be conducted before they will do business with you. Increasingly, businesses that are unable to prove that their infrastructure is secure are losing out on potential business.

It has also become common for larger organisations to demand those in their network gain **Cyber Essentials certification** before they'll do business with them.

Speak to Technical Drive about how we can help your business obtain Cyber Essentials certification.

How do I keep my business secure?



There are many reasons that your business could be affected by cyber threats, from malware infecting an unsecure network to being targeted by a phishing attack. Data breaches aren't always of criminal or negligence, sometimes they're the result of a technology failure or an employee making an innocent mistake.

The good news is you don't necessarily need a large budget or team of experts to protect your systems and data. A secure environment is possible, even on a smaller budget by following some key security steps.

8 steps you can perform to secure your business.

1.

Educate and train your team:

People and not technology are often the most vulnerable part of an organisations network. Cyber criminals often take advantage of unsuspecting staff to break into networks, especially via phishing attacks. You should carry out regular IT security awareness training to increase knowledge of potential threats and reduce breaches. It's important to involve your entire team, because it's often those that you wouldn't expect that can be seen as easy targets. It is also important to have a regularly updated security policy for stakeholders and members, identifying best practice on areas such as password security.

2.

Identify all the devices on your network:

Many organisations have BYOD (Bring Your Own Device) policies or no controls in place, and employees are free to access their networks via their own devices, including laptops and mobile devices. It's vital to have a clear understanding of what devices are on your network and ensure they are properly managed and secured as you would company devices.

> How do I keep my business secure?

3. Perform regular audits of sensitive data:

To keep your most sensitive information secure, you need to know what you have and where it's stored. To avoid compromising your systems and data, we recommend conducting a quarterly audit, including a detailed record of all devices with access to your network, and ensuring these devices are configured correctly.

4. Utilise the security of the cloud:

Cloud services offer smaller organisations an affordable way to enhance their IT infrastructure with robust security features, including access controls and data encryption. By migrating services like email, backups, documents, and files to the cloud, organisations minimise the risk associated with storing data on individual devices, which could be lost or stolen. This not only lowers the total cost of ownership but also provides access to advanced security measures, improving protection against threats.

5. Ensure systems are kept up-to-date:

Every piece of software has weaknesses. As soon as the provider recognises the flaw, a patch will be created and released to prevent the weakness being used by cybercriminals as a means of gaining access to your systems and data. If you are not effectively patching or updating your software and devices, then you could be giving cybercriminals access to your data.

> How do I keep my business secure?

6. Prepare a backup and disaster recovery:

Improving IT security reduces risk but doesn't eliminate it. To be prepared for cyber attacks, data loss, or system failures, regularly back up your servers and cloud storage. Having these backups, along with a plan to restore your systems, helps you effectively respond to any issues that arise.

7. Gain Cyber Essentials certification:

Cyber Essentials is a government backed scheme created to help you protect your organisation against a range of cyber threats. It involves demonstrating that you have implemented a range of technical controls across your digital environment, including Internet, devices and software, data and that you have adequate protection against viruses and malware. Technical Drive's cyber security experts can guide you through the process.

8. Consult trusted experts in cyber security:

Consult an accredited cyber security expert. At Technical Drive our team operate from our in-house Security Operations Centre (SOC), using best-of-breed solutions and tools. We are accredited to the highest standards, including ISO 27001 for Data Security as well as being Cyber Essentials Plus accredited.

So, whenever you need cyber security advice, you can rely on Technical Drive's team of trusted cyber security expert.

Can I reduce my threat with Managed Services?

Organisations with limited budgets are able to enhance their cyber security protection through outsourced proactive IT support.

An Managed Service Provider (MSP) can recommend and implement cost-effective cyber security solutions to help defend your organisation against cyber attack. Although it would be difficult for an SMB to be able match a large enterprise's internal resources, by using an MSP who takes responsibility for all your security, you will be able to combat cyber threats more effectively.

An MSP can administer complex security devices and manage technical controls like firewalls, patching, anti-spam and virus detection. They will keep all systems and programs up-to-date, which is critical to minimising vulnerabilities.

Modern threats require advanced solutions like Endpoint Detection & Response (EDR), which are designed to proactively detect and address the latest security threats and it's unlikely you will secure cyber insurance without it.

Organisations should also consider Cyber Essentials, a UK government scheme encouraging organisations to adopt good practice in information security. It provides a framework and a set of security controls to protect against cyber attacks.

Technical Drive can provide the following Cyber Security services and solutions


- Patch management & system updates
- Cyber awareness training
- Cyber Essentials certification
- Endpoint Detection Response (EDR)
- Backup and disaster recover
- Multi-factor authentication
- Password management
- Mobile device management
- Email security
- Multi-geo capabilities



[Find out more](#)

technical drive

Contact us





 **01527 880088**

 **communications@technicaldrive.co.uk**

 **www.technicaldrive.co.uk**

 **Head Office**
Technical Drive
Grosvenor House
Market Street
Bromsgrove
Worcestershire
B61 8DA

Get social:

 @TechnicalDriveLtd/
 @technical-drive-limited
 @TechnicalDrive_
 @technicaldrive_itsupport/




technical drive