Citation Cyber

Cyber security fundamentals for businesses:

the ultimate guide and what you need to know

v01

Introduction

You've watched your business leap forward from being an idea in your head to a fully functioning operation. You've learned immense amounts of information about running a business and know your sector inside out. Now, it's all about strengthening your roots, seeking out new opportunities and growing.

Unfortunately, among all the excitement and long days that accompany the growth of a business, security is often overlooked. You might have a decent lock on your office door, but is your data safe? These days, especially with so much information stored in the cloud, your data can be a looming vulnerability that no lock and key can protect.

Security is one of those things that are difficult to measure in terms of cost and benefit. The perfect security system protects you so well that you hardly even realise the risk exists, and you are never troubled by breaches. Strangely, that can itself lead to issues, as complacency can set in. Cyber security is an ongoing arms race between criminals and honest businesses, and standing still is not an option.

In this guide, we'll look at the importance of cyber security, and how taking some relatively simple steps can potentially save your business.

The importance of cyber security

As a growing business, it is essential to prioritise cyber security. Cyber attacks can lead to data breaches, financial losses, damage to reputation and legal consequences. By investing in cyber security measures, you can protect your sensitive information and maintain trust with your customers.

Security threats can come from many different angles. Most commonly, it's criminals aiming to breach your data for financial gain. That can mean simply stealing money from you, perhaps in ways that are barely traceable. But it can also mean taking sensitive information and blackmailing you to prevent its release.

It can also manifest itself in stealing private data, such as customer information or product development plans, which would be useful to competitors. The actions are not necessarily instigated by your rivals, but the data might prove useful to them, assuming they don't do the right thing when offered it.

Finally, a breach could effectively shut down your business, especially if you have a notable online presence, whether that's eCommerce or taking orders online. How long could you survive without your website or online payment system?

Businesses grow by building up customer numbers and increasing spend per customer. In fact, without those customers, your products, warehousing, distribution networks, manufacturers, and sales staff – and therefore your business itself – are worth nothing.

Protecting your cyber security all boils down to maintaining your strong relationships and trust with your customers. It's the basis of a good business strategy.

Hopefully now there's no doubt in your mind about the importance of cyber security. Let's look at the basic steps you can start taking today that will mitigate your risk of cyber criminals accessing your data.

Conduct risk assessments

Start by assessing your current security posture. Identify potential risks and vulnerabilities that need improvement. Try to put a value on each element of your cyber infrastructure, and channel your efforts at protecting them accordingly.

Regularly reassess and update your security measures to stay ahead of emerging threats. Why not **bookmark our blog page**, where we address the ever-changing landscape of cyber threats?

Develop a security plan

Create a comprehensive security plan tailored to your business needs. This plan should include policies and procedures for data protection, employee training, incident response, disaster recovery and any legal or regulatory requirements specific to your industry.

We'll go through these factors below. Sticking to the plan, and having regular meetings dedicated solely to the subject of cyber security, will stand you in good stead for the future. You should also develop an incident response plan, so you can get up and running should the worst happen.

Employee training

Educate your employees about cyber security best practices. At a basic level, you should **train them** to recognise phishing emails, use strong login credentials, and follow safe browsing habits.

The majority of breaches come from slips made by staff members, in fact, 74% of breaches involve the human element. So, drilling security into their everyday lives can protect you from a huge amount of risk.

Regularly communicate updates about emerging threats and provide guidelines for handling sensitive data. It's worth considering **social engineering training**, too, as staff can wrongly divulge information to those who seem trustworthy.

Secure your network

Implement strong firewalls and secure Wi-Fi across all your networks. Our CREST-certified ethical hackers can perform **Wi-Fi penetration testing**, which can often reveal glaring holes that you were completely unaware of.

In today's flexible workplace, it's vital that you use virtual private networks (VPNs) for remote workers. Whether they are working from home, at a hotel, in a coworking space or at a cafe, providing that extra layer of security on the network can stop breach attempts in their tracks.

Regularly update software and apply patches to fix vulnerabilities and restrict access to sensitive information by implementing role-based user access controls.

If a certain employee doesn't need access to a particular system, don't grant it, and make sure your managers are on top of who has access to what. The smaller the number of people who have access to any element of your cyber infrastructure, the safer it is.

Data encryption

Encrypt sensitive data both in storage and in transit. This ensures that even if an attacker gains access to the data, they will not be able to decipher it without the encryption key. All too often we hear chilling stories of major businesses leaking data that's completely raw.

That means customers' names, addresses, account numbers, bank details, and other sensitive data being readable by anyone who can access the database. Bearing in mind that a lot of breaches are down to staff errors rather than forced entry, encryption is a sensible and potentially business-saving step.

Secure cloud storage

If your business uses cloud storage services, ensure that they have proper security measures in place. Pick reputable providers that offer encryption, multi-factor authentication, and regular backups. Implement strong access controls and regularly review permissions.

Ensure that access is only granted to people who need it, for as long as they need it and no longer. If restricting access to specific IP addresses or geographic locations would help, implement such measures too, albeit remembering that such info can be faked.

Develop a software update regime

Many software updates are for performance improvements, new features, or simple modernisation.

But some are critical security updates that are made in response to a discovered threat. It's vital that you keep all software, including operating systems and applications, up to date. In fact, it's best practice to enable automatic updates, where possible, and ensure updates are applied within 14 days of them being released.

Use multi-factor authentication

Implement multi-factor authentication (MFA) for all accounts and devices. MFA adds an additional layer of security by requiring users to provide multiple forms of verification, such as a password and a unique code sent to their phone.

It's sometimes called two-factor authentication (2FA), as it requires a password and a device (such as a key card or a known phone) to access a certain asset. MFA can mean two or more factors. Security needs to be balanced with the inconvenience and inefficiency of repeatedly having to use multiple devices and knowledge to access cyber assets.

Regularly back up data

Regularly back up your data to a secure location and separate network. In the event of a cyber attack or data loss, having backups allows you to quickly restore your systems and minimise downtime.

Book security audits

Conduct regular security audits to identify any weaknesses in your infrastructure and address them promptly. Consider hiring **external security experts** to perform assessments to ensure an unbiased evaluation.

Constantly test and improve

Continuously test your security measures through penetration testing and vulnerability assessments. Most importantly, you should update and improve your security protocols based on the findings.

Even if a test gives you the all-clear, your risk will start to grow larger the longer you leave it. Think about every application you install, every time someone accesses the database, every time someone logs in from a hotel, and every staff member you recruit or dismiss. Each one chips away at the security assessment that was arrived at during your last appraisal.

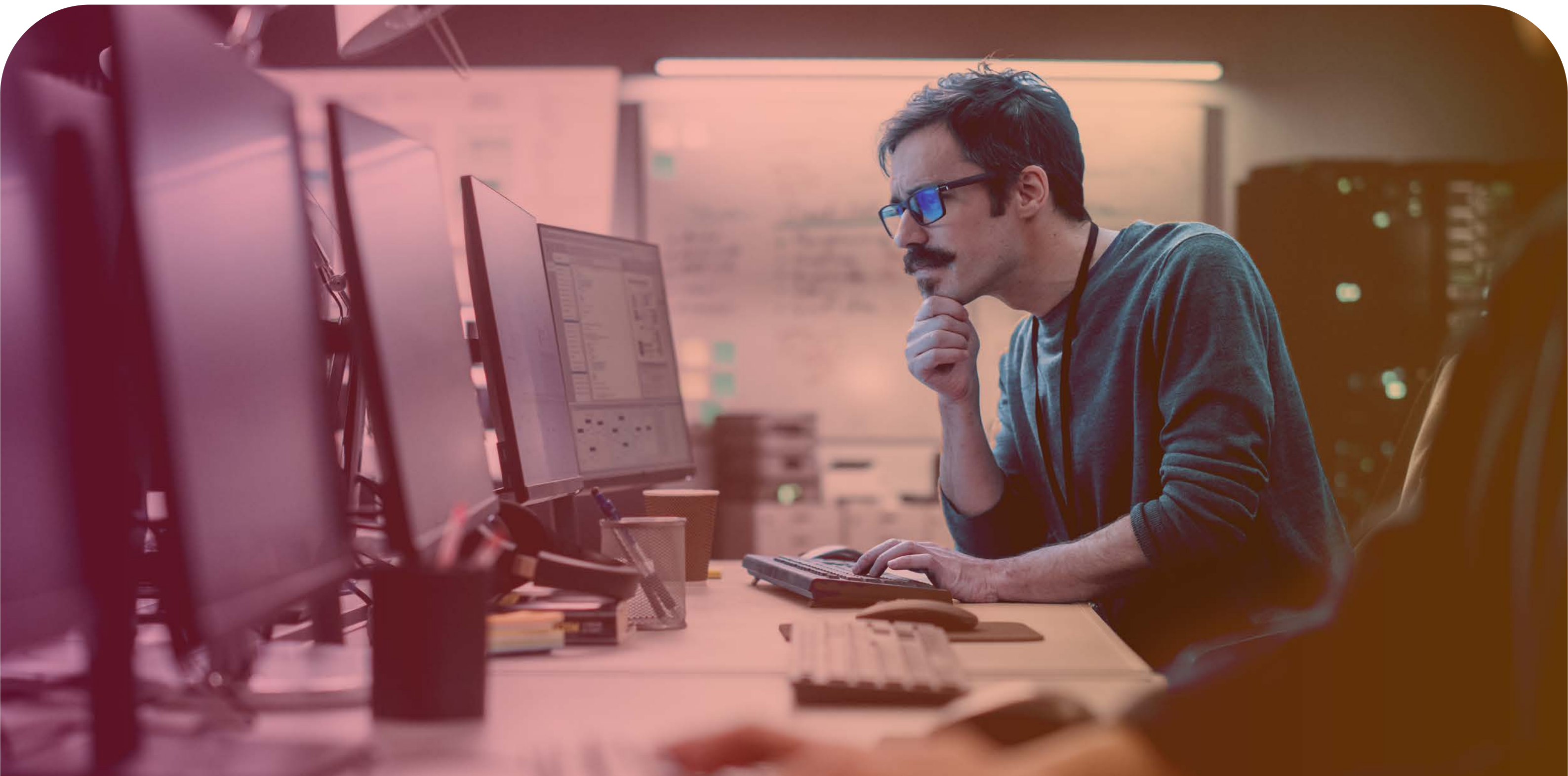
Seek professional help

If you lack the expertise or resources to implement robust cyber security measures, consider outsourcing your security needs to a reputable cyber security company (that's us!).

We can help you monitor and manage your security infrastructure while providing expert guidance on future plans. We'll also perform that all-important vulnerability testing, which imitates the efforts of criminals to ascertain the security status of a particular asset.

As a Cyber Essentials certification body since 2014, we also **offer cyber certifications** which prove that your business has the appropriate defences and procedures in place for reduced risk. That can be hugely reassuring to existing and potential customers.

Remember, cyber security is an ongoing process that requires constant vigilance and adaptation. By prioritising cyber security and implementing proper measures, you can protect your growing business from the vast majority of potential threats.



Your cyber security checklist

Cyber threats continue to evolve, posing significant risks to your sensitive data, financial stability, and reputation. To get your business prepared and safeguard your operations, we've compiled a comprehensive cyber security checklist tailored for your business.

- Create a regular backup schedule for your company data. Ensure this is done automatically and stored on a separate network in a remote location. ○
- Set up an Incident Response Plan. ○
- Enable multi-factor authentication (MFA) on your accounts, if applicable. ○
- Create a device log and monitor what each device has access to (accounts, information, finances, etc). ○
- Where possible, enable automatic software updates on your devices, apps, and browsers – ensure updates have been applied within 14 days of release. ○
- Implement anti-virus software and firewalls. ○
- Introduce a Bring Your Own Device (BYOD) policy if your team use their personal devices for work-related purposes. ○
- Disable/remove any unused extensions, apps, services, etc. ○
- All passwords should be, at least, 12 characters long and unique to every service, device, and account. ○
- Implement a password manager throughout your organisation to avoid password reuse/fatigue. ○
- Develop a cyber awareness training strategy to optimise your human firewall. ○
- Implement a 'Suppliers' Survey' to improve analysis and scope of your supply chain risk level. ○

FAQs

What is the biggest cyber security threat in SME businesses?

In our digital world, cyber security threats are ever evolving. There is no single threat that businesses need to defend against as an attack or breach can occur through a multitude of different methods. However, recent reporting has identified hacking strategies and common vulnerabilities that could be present in your business:

1. Ransomware
2. Phishing communications
3. Compromised login credentials

Our range of security solutions are here to build your company's resilience to cyber threats whilst helping you remain compliant and secure.

How often should data protection and cyber awareness training be conducted?

The current guidance states that you should ensure your team are receiving cyber awareness and data protection training on, at least, an annual basis with refresher training sessions drip-fed throughout the year. This ensures that your workforce is equipped with the latest knowledge and skills to defend against an attack or breach, and that they understand their role with mitigating risk.

Our awareness training service allow you to manage your training strategy with engaging e-Learning modules designed to strengthen your human firewall. Schedule training sessions at a pace that suits you, and effectively identify areas of improvement throughout your organisation.

How do I know if my business data has been compromised?

The average time is takes for a business to detect and contain a breach is 327 days. During this time, a cyber criminal can cause some serious disruption to your devices and data. Promptly identifying and containing a breach is key to minimising the fallout and beginning the recovery process.

With **intelligent monitoring and vulnerability scanning**, you can effortlessly manage your devices and systems to ensure they are operating as they should be. Through simple reporting and real time results, you can gain a comprehensive understanding of where your vulnerabilities lie and remediate these before an attack or breach occurs.

We already have an IT team in our business, why do we need cyber security?

It's important to remember that cyber security and IT are two separate entities – but they complement each other extremely well! The main difference between the two is cyber security focuses on protecting your digital systems and data from unauthorised access. Whereas IT manages your technology infrastructure and provides support for your various computing needs.

Ultimately, cyber security and IT go hand-in-hand, and one does not replace the other. Together, they can effectively secure your business and optimise your systems.

The key contacts

If you require additional support or need to report a cyber security incident, contact the National Cyber Security Centre at **https://report.ncsc.gov.uk/**

24/7 live cyber fraud reporting for businesses with Action Fraud, **https://www.actionfraud.police.uk/**

Your preventative cyber security wingman, Citation Cyber. Speak to a member of our team who will help develop a bespoke cyber strategy for your business.

The ultimate solution for your business

Do you want to become cyber secure? With our ongoing cyber security support, you can! We'll train, test, and certify your business to minimise data breaches and cyber attacks.

Our solutions are designed to help you become a business that your clients can trust, and what's more is that you'll remain compliant, win more tenders, and improve your overall efficiency. Watch your business soar when you're cyber secure!

Let's make securing your business just that much easier. We cut the faff, the jargon, and keep cyber security as it should be . . . simple!

All our packages can be tailored to meet your specific business requirements, so we recommend kicking things off with a **free business needs assessments and software demonstration**.

Book today by clicking **here** or calling our friendly team on **0333 323 3981**.

As a flavour of the support we offer, our entry-level 'Secure Core' package includes:

- ✓ Cyber Essentials certification
- ✓ Guidance and technical support with your Cyber Essentials assessment
- ✓ £25k cyber insurance
- ✓ 2x External vulnerability scans
- ✓ Dark web monitoring
- ✓ Cyber security awareness course for your team
- ✓ 12x cyber policy templates
- ✓ HR advice line
- ✓ Free employee screening registration
- ✓ Access to the state-of-the-art user hub where you can manage your security solutions, store your company policies, and monitor your training strategy.

FIND OUT MORE

And for those wanting complete cover, we've got our all-in-one 'Secure Pro' including dedicated compliance training modules, and external intelligent monitoring and vulnerability scanning.

Got any questions or ready to get the ball rolling? Call **0333 323 3981** or email us at **info@citationcyber.com**

Watch your business soar when you're cyber secure!

Got any questions or ready to get the ball rolling? Call **0333 323 3981** or email us at **info@citationcyber.com**

Citation Cyber