CyberKarl®

Helping You Defend What Matters

THE CYBERKARL BUSINESS OWNER SERIES

CYBER SECURITY SURVIVAL GUIDE

Protect the people, information and services your business relies on.



CYBERKARL LTD / UK EDITION 2026

cyberkarl.com

CYBERKARL LTD / UK BUSINESS EDITION

A practical guide to cyber security

Helping you defend what matters.

Cyber security should help your organisation keep operating, protect its people and earn the confidence of customers and partners. It should not be a collection of expensive tools that nobody understands.

This guide is written for UK business owners and managers who need clear advice, sensible priorities and practical questions to ask their IT teams or suppliers.

It begins with the risks you need to understand, moves through the controls that matter most, and finishes with incident response, governance and a plan for turning advice into action.

Use this as an introduction and a working reference. The advice is general and should be adapted to your organisation, its activities, its legal obligations and its appetite for risk.

CYBERKARL LTD

Cyber Security & Governance · Privacy & Data Protection · AI Security & Governance · vCISO & Assurance

cyberkarl.com | hello@cyberkarl.com

PUBLICATION INFORMATION

Copyright and important information

CyberKarl edition, November 2026.

CyberKarl branding, editorial updates and original additions © 2026 CyberKarl Ltd. The underlying book text is adapted from commercially licensed material. Rights in third-party material remain with the respective rights holders.

This guide provides general information and is not tailored legal, regulatory, insurance or technical advice. Requirements may change. Check current official guidance and take specialist advice where appropriate.

Statements about how safeguards work assume that the measures are correctly implemented, maintained and tested. No organisation can eliminate all cyber risk.

The main body retains the depth and practical structure of the licensed Cybersecurity Survival Guide manuscript. Specific unsupported statistics and US-focused references have been replaced, and UK guidance and original checklists have been added.

For enquiries: hello@cyberkarl.com | https://cyberkarl.com

YOUR ROUTE THROUGH THE BOOK

Contents

PART ONE • UNDERSTANDING THE RISK

INTRO Why a book on cyber security? 6

01 What cyber security is 9

02 The return on security investment 12

03 The most common threats 16

04 Follow a framework: UK Cyber Essentials 25

PART TWO • PRACTICAL PROTECTION

05 People and identity 28

06 Devices and endpoint security 36

07 Email, web and collaboration 42

08 Data protection 48

09 Networks and cloud basics 54

10 Supplier and third-party risk 59

PART THREE • ASSURANCE AND RESILIENCE

11 Incident response and business continuity 65

12 Compliance and governance 74

13 Putting it all together 80

14 Cyber security jargon decoder 85

FURTHER RESOURCES

Using AI safely at work 88

Your first 30 days 91

Sources and further reading 93

About CyberKarl 95

START HERE

Three questions before you begin

What matters most?

List the services, information and people the business cannot afford to lose.

What could stop us operating?

Think about unavailable systems, stolen payments, exposed personal data and suppliers failing.

How would we know our controls work?

Ask for current evidence, not just a policy or reassurance that someone is “looking after it”.

Security works best when it becomes a series of small, repeatable business decisions. Pick one improvement, name the person responsible and check the result.

PART ONE / UNDERSTANDING THE RISK

INTRODUCTION

Why a book on cyber security?

You do not need to become a technical expert to make sensible decisions about cyber risk. You need a clear explanation of the threats, an achievable set of actions and a way to check that those actions are working.

For many business owners, cyber security feels complicated. It competes with everyday pressures such as customers, staff, cash flow and keeping services running.

Because many business owners still see cyber security as a big, scary word they would do anything to avoid. For many, it creates that same stomach-crunching, heart-in-your-throat feeling they get when they're about to visit their dentist.

That feeling often stems from the unknown and from years of fearmongering. So, cyber security remains somewhat of a fringe topic, often pushed aside for "better" subjects like sales, marketing, and operations.

After all, no one wants to contemplate the horror scenarios their business or even their lives could face, especially when they could be focusing on how to grow their business instead.

The bad part about this is that fear can lead to "technostress" and apathy. If a problem seems too overwhelming or complex, business owners tend to feel helpless and disengage completely, ironically making them more vulnerable to those very threats they fear.

The aim of this guide is not to frighten you into buying tools or services. It is to make security easier to understand and more manageable.

The goal of this book is to demystify cyber security, make it digestible, and, at the risk of pushing it too far, maybe even exciting.

It aims to give you the confidence that you can implement cyber security in your business without being an expert, providing you with knowledge of how cyber security works and how simple it can be if you follow a framework.

You will learn how to protect the systems, data and people your business depends on, one practical step at a time.

Now, I can't promise that just reading this and putting it into practice will make your business totally unbreachable, as that's just not realistic. But it will make your defences a whole lot stronger!

The truth is, there's no such thing as a 100% secure business or organisation. If an IT provider tells you that, they're probably not being completely straight with you.

Even big governments, with all their fancy resources, can get hit by sophisticated attacks.

Many damaging incidents exploit familiar weaknesses: reused passwords, missing updates, excessive access or poorly understood recovery arrangements. A disciplined approach to these basics can make a substantial difference.

The good news about this is that it also means it's straightforward to put effective safeguards in place.

And as we go further, you'll see that a big part of cyber security is just about building new, consistent habits. Easy, actionable steps that you and your team can add to your everyday routines.

Take this book one step at a time.

Don't feel like you need to implement everything at once. Instead, just pick one or two practical things from each chapter that you can start doing right away. The main goal here is to make incremental progress, rather than stressing about being perfect overnight.

We'll kick things off by getting a good handle on the basics, and from there, we'll walk through the most important habits for keeping both your people and your valuable data safe and sound.

Start with the actions that matter most to your organisation. You do not have to do everything at once.

CyberKarl Ltd
Helping you defend what matters.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Identify one service that cannot stop** Name the business process and its critical systems
☐	**Name the person who owns cyber risk** Record their role and decision authority
☐	**Choose one practical improvement** Give it a date and a way to show completion

PART ONE / UNDERSTANDING THE RISK

CHAPTER 01

What cyber security is

I want to start this chapter by clarifying what cyber security is NOT. Tech experts often make simple subjects complicated, and that's exactly what I aim to avoid in this book.

Cyber security need not be overwhelming for an SME. Some organisations face complex, specialised threats, but the foundations of managing people, access, devices, information and recovery are relevant to every business.

Cyber security isn't a product you buy. It's a collection of smart business habits to manage digital risk. Essentially, cyber security is how we reduce the likelihood and impact of events that could misuse, disrupt, or expose valuable data and systems. It's simply risk management for the digital parts of your company.

Size does not make a business invisible. Criminals use automated tools, stolen credentials and convincing messages to identify organisations with weak controls. A small organisation can be affected through its own systems, its employees or one of its suppliers.

Many successful attacks exploit ordinary weaknesses rather than sophisticated technology. The good news is that practical safeguards are available to organisations of every size. The aim is to prioritise them and check that they work.

So, how do you protect against these common threats? You just need a simple way to think about it. Everything in cyber security really comes down to three core pillars:

The first is **Identity**. This is all about who has the keys to your business, your people, their accounts, and the devices they use. If your habits here are sloppy, like sharing passwords or not removing access for ex-

employees, your entire business is fragile. Strong identity management is your first line of defence.

The next is **Data**. This is what you're trying to protect, your financials, your customer lists, your secret sauce. Knowing where this data is stored, controlling who has access to it, and keeping reliable, tested copies of it is your ultimate safety net.

And finally, **Operations**. This is the discipline to keep things updated, monitor for strange activity, and have a plan for when things go wrong. It's where your habits live, like the two-minute phone call to verify a change in bank details before making a payment or regularly backing up your systems. Effective operations ensure your defences are always active and ready.

These three pillars form the foundation of effective cyber security for any business. The solution to managing cyber risks, which this entire book is built on, involves two core concepts: building a few key habits and following a clear plan. Much of this is about small, consistent actions that you and your team take every day. And just like any other area of your business, using a simple, proven framework brings order to chaos and prevents you from wasting time and money on things that don't matter.

This brings me to the single most important point in this entire chapter. Cyber security is not an "IT thing." It is a leadership responsibility. You would never let your bookkeeper be the only person who cares about the company's financial health; you, as the owner, ultimately have that responsibility. The same is true for the digital health of your business. Your IT team or provider can do the work, but accountability starts and ends with you. This book is designed to give you the confidence to ask the right questions, set the right expectations, and lead your team to a safer way of operating.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**List your essential services** Identify the people, systems and data behind each service

☐	**Assign accountability** Confirm the senior person responsible for decisions
☐	**Agree what failure would cost** Consider downtime, loss of data and loss of trust

PART ONE / UNDERSTANDING THE RISK

CHAPTER 02

The return on security investment

So, what's the return on investment for cyber security?

The answer isn't something you'll find in your bank statement, at least not if everything goes as planned.

The ROI of investing in cyber security is similar to investing in sturdy locks for your doors or a sprinkler system for your warehouse.

You're spending a bit of money now to significantly reduce the risk of a much larger, more painful loss later. In business terms, you're simply lowering your expected loss.

It's a simple formula: **Expected Loss = Financial Impact of Incident × Likelihood of Happening.**

Your entire goal with cyber security spending is to aggressively push both of these numbers down.

Let's make that "financial impact" number more real, because it's not just about a ransom demand.

First, consider the cost of downtime. What would it cost for your business to be completely shut down for three days?

For example, if a business normally takes £10,000 in revenue each day, three days of disruption could put £30,000 of revenue at risk. This is an illustration, not a prediction of actual loss.

Add to that three days of payroll for a team that can't do their work, and then all the overtime you'll have to pay to catch up once you're back online.

Next is direct financial theft, often through fake invoices, compromised email accounts or a fraudulent change in supplier bank details. Ask what a single unexpected payment would mean for your cash flow.

Finally, there are the cleanup costs. This is the bill you receive after the attack is over. This includes emergency cyber security experts, forensic investigations, system restoration, legal advice, and regulatory compliance.

Then there are response and recovery expenses: specialist support, investigation, service restoration, legal advice, communications and, where applicable, regulatory work. The actual cost depends on the nature of the incident and your business.

Not every incident results in a fine. Legal and regulatory obligations depend on the facts, the data involved and the relevant law. Prevention and preparation are still more cost-effective than avoidable disruption.

When you add it all up, the total financial impact of a single incident can easily climb into the high six figures, which is why so many small businesses don't survive an attack.

So, how do you push those numbers down? You start by making investments that offer the biggest and clearest payback.

To reduce the chances of these attacks, year after year, data shows that attackers typically gain access through a few common entry points: stolen passwords and outdated software. This tells you exactly where to focus your efforts.

To **reduce the likelihood of theft**, begin with strong identity controls.

The most important of these is multi-factor authentication (MFA), which is that small code you receive on your phone when you log in. It stops most attacks that rely on stolen passwords. The cost of enabling MFA is tiny compared to the six-figure fraudulent transfer that never happens because an attacker couldn't get past the login screen.

To **reduce the financial impact of ransomware**, you need tested, offline backups.

This investment transforms a potential multi-week, business-ending disaster into a manageable one-weekend recovery. When your files are

locked and a criminal demands a ransom, the difference between "we can be back up and running by Monday" and "we have to consider paying these guys" is a clean copy of your data that the attacker couldn't touch.

A protected backup and a tested recovery process can greatly reduce the impact of ransomware. Neither guarantees a quick recovery, so agree a realistic recovery target and test it.

To **reduce your cleanup costs**, you need modern endpoint protection and a routine for keeping your software updated.

Old antivirus software is no longer sufficient. Modern tools look for suspicious behaviour, not just known viruses. This can stop an attack in its tracks, containing it to a single computer instead of allowing it to spread across your entire network.

But good security does more than just prevent bad things from happening; it can also become a tool for growth.

Good security also supports your conversations with insurers. A cyber insurance policy is not a substitute for effective controls.

Insurers may ask about multi-factor authentication, backups, patching and incident response. Cover and claim decisions depend on policy wording, the facts of a loss and the accuracy of information provided. Check the conditions with your broker or insurer.

The other way it helps you grow is by helping you win bigger deals.

When you demonstrate robust cyber security, you're proving to your prospects that you are a professional, reliable partner they can implicitly trust with their sensitive data and business operations.

This confidence can be the deciding factor in competitive bids, allowing you to secure lucrative contracts that might otherwise go to less secure competitors.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Estimate the impact of one day offline**

	Record the assumptions and affected business processes
☐	**Prioritise MFA and recovery** Confirm those controls work as intended
☐	**Review insurance questions** Compare declared safeguards with actual practice

PART ONE / UNDERSTANDING THE RISK

CHAPTER 03

The most common threats

If you run a small or mid-size business, the cyber threats you face look nothing like they do in the movies.

Criminals operate like a business. Like you, they seek efficient ways to make money. This means they rely on a playbook: a small set of reliable, high-return strategies that work repeatedly.

In this chapter, we'll examine this playbook, one category at a time. We'll explore tactics they use against your people, technology, and daily operations. Understanding these plays will help you protect against them.

Category 1: Threats Targeting Your People

Most security incidents don't begin with a hacker bypassing a firewall. They start with a person.

People remain central to many cyber incidents. Attackers exploit trust, workload and urgency to persuade people to reveal information or approve fraudulent requests.

Attackers know your team is your biggest asset, and they exploit this strength to find an opening.

Threat #1: Phishing & Social Engineering

At its core, phishing is a con game. It's a deceptive attack designed to trick someone into doing something they shouldn't, such as clicking a malicious link, opening a dangerous attachment, or revealing their password.

The most common form is the broad phishing campaign, where an attacker sends millions of generic emails hoping a small percentage of recipients will fall for it. These include fake FedEx delivery notices or urgent "Your Microsoft account is about to be suspended" alerts.

However, the more dangerous version is "spear phishing."

Here, the attacker does their homework. They research your company, identify key personnel in departments like accounting, and craft a personalized email that appears to come from you or a trusted vendor.

This often leads to Business Email Compromise (BEC), one of the most financially damaging attacks a small business can face. Attackers might insert themselves into an ongoing email conversation, wait for the right moment, and then send a message like, "Hi, we've updated our bank details. Please send this month's payment to this new account." Because it looks legitimate and is part of an existing conversation, it's incredibly effective.

Business email compromise can cause serious financial loss. A simple independent verification process for changes to payment details is one of the most practical protections.

At this point, you might be thinking "My employees are too smart to fall for this." And you're probably right. The problem is that these attacks don't rely on intelligence.

They exploit the distractions we all are exposed to during a busy workday. Data shows that when someone falls for a phishing email, it happens quickly, as the median time from receiving the email to clicking the link is **less than 25 seconds**.

So, how can you and your team recognise these attacks? They almost always share a few common traits:

A sudden sense of urgency. The email creates pressure, insisting you act now or face negative consequences. Words like "Urgent," "Important," and "Attention" are common in scam subject lines. This is a psychological trick designed to induce panic and bypass normal safety checks.

A request that breaks the rules. The message will ask you to do something outside your normal company process, often with a reason to keep it quiet. For example, "I'm in a meeting and can't talk, can you please just pay this invoice for me and not mention it to anyone?"

Slight imperfections. The sender's email address might be off by one letter, or if you hover your mouse over a link, the destination address won't

match the displayed text. These are small details that are easy to miss when you're in a hurry.

Threat #2: Insider Threats

This is a sensitive topic because it involves people you've hired and chosen to trust.

An insider threat occurs when a current or former employee, contractor, or partner uses their authorised access to harm the business.

Insider risks are not always malicious. They may arise from mistakes, excessive permissions, poor offboarding or deliberate abuse of access.

Sometimes, it's an **unintentional insider threat**. This involves a well-meaning employee who makes a mistake.

For example, they might email a sensitive customer list to their personal Gmail account to work on it over the weekend. While they don't intend harm, they've moved company data outside your control, creating a security risk.

Other times, it's a **malicious insider**. This could be a disgruntled employee about to quit who downloads a copy of your client database to take to their next job. Or it could be a contractor whose project has ended, but their access was never revoked, allowing them to snoop around weeks later.

While you should trust your team, implementing security controls is essential.

You implement financial controls not because you assume your bookkeeper is a thief, but because it's the correct way to protect the company's money. The same logic applies to your data. Good controls protect the business from intentional harm and prevent good employees from making accidental mistakes.

Recognizing an insider threat can be difficult because the person already has legitimate access.

The signs are usually changes in behaviour:

Accessing unusual amounts of data. An employee in marketing suddenly trying to access engineering blueprints, or someone downloading thousands of files right before they go on vacation.

Working at odd hours. A user who normally works 9-to-5 suddenly logging in at 2 AM and accessing sensitive folders.

Trying to bypass security controls. An employee repeatedly attempting to access parts of the network they're not authorised for, or asking coworkers for their passwords.

Category 2: Threats Targeting Your Technology & Supply Chain

While many attacks begin by targeting your people, they almost always succeed by exploiting a gap in your technology.

Even if an attacker tricks an employee into revealing a password, they still need a technical "door" to enter. This is where the automated, high-volume aspect of their business model becomes evident. They use software to constantly scan the internet, searching for the digital equivalent of an unlocked window.

Threat #3: Use of Stolen Credentials

Your employees' usernames and passwords are the keys to your business. The problem is, these keys are frequently copied and sold. When a major company like LinkedIn or Adobe experiences a data breach, the lists of stolen usernames and passwords from that breach often appear for sale on the dark web.

Criminals purchase these massive lists and then use automated software to try those same username and password combinations on other websites, such as your company's email login page.

This is called credential stuffing. It works because people reuse the same password across multiple services. Unique passwords and phishing-resistant multi-factor authentication are effective safeguards.

If your employee used the same password for their old Myspace account that they now use for your company's payroll system, a breach from a decade ago can suddenly become your problem today.

Stolen credentials are a common route into online services. They may be used to access email, cloud applications or business records where additional verification is missing.

So, how do you recognise if this is happening? Here's what to look for:

Login alerts from unusual times or locations. You might receive an email from Microsoft indicating someone tried to log into your account from a different country at 3 AM.

Getting locked out of your own account. If an attacker repeatedly tries to log in with the wrong password, the system might lock the account for security reasons, preventing even you from accessing it.

Seeing activity you don't recognise. You might notice emails in your "sent" folder that you didn't write, or observe that files have been accessed or downloaded when you weren't working.

Threat #4: Exploitation of Unlocked Digital Doors

Criminals constantly scan internet-facing systems for exploitable weaknesses. Unpatched software and insecure remote access are particularly important to identify and address.

There are two main types of "unlocked doors" they look for.

The first is **software vulnerabilities**. Think of this like a car manufacturer discovering a faulty lock on one of their models and issuing a recall. As soon as that recall is announced, car thieves know exactly what to look for.

The same thing happens with software. When a company like Microsoft or Google finds a security flaw in their product, they release a fix, called a "patch."

Once a security fix is public, criminals may begin scanning for systems that have not yet been updated. Keep an accurate inventory and prioritise updates according to exposure and risk.

The second type of unlocked door is **misconfigured remote services**. These are the tools your team uses to work from outside the office, like a VPN or Remote Desktop Protocol (RDP). These tools are essential for

modern business, but if they're set up with weak, default passwords or aren't protected with multi-factor authentication, they become a wide-open door visible to the entire internet.

Criminals can weaponize a new vulnerability in a matter of hours, while it takes the average organisation around **55 days to patch just half of their critical flaws**. This massive gap is the window of opportunity attackers exploit.

And the only evidence that someone gained access through an unpatched piece of software or a poorly secured remote login is what they do next, which is often installing ransomware and locking up all your files.

Threat #5: Supply Chain Compromise

Your business doesn't operate alone. You work with many outside vendors like IT providers, accounting firms, and payroll services, and you use various software tools daily. A supply chain attack happens when criminals hack into one of these trusted partners. They then use that partner's legitimate access to get into your systems.

This is an increasingly popular and efficient tactic. Why attack one hundred small businesses individually when you can attack the single piece of software they all use and gain access to all of them at once?

A supplier incident may affect many customers at once. The priority is to understand which partners have access to your information or systems and what would happen if they were compromised.

Third-party exposure deserves its own place in your risk assessment. Consider outsourced IT, payroll, finance applications, cloud hosting and software providers.

Limit supplier permissions, agree incident notification arrangements and review the security of services that are critical to your operations.

And if you’re thinking that your vendors’ security is not your problem, that's no longer true in a modern, connected business.

Your security is only as strong as the weakest link in your supply chain. If your payroll provider is breached, your employees' data is at risk. If your IT provider is compromised, attackers could gain the keys to your entire

kingdom. You must consider your key vendors an extension of your own company and hold them to a reasonable security standard.

Recognizing a supply chain attack is extremely difficult because the attack often originates from a source you already trust:

A breach notification from your vendor. Often, the first you'll hear about a problem is when one of your vendors sends you an email stating they've had a security incident and that you might be affected.

Suspicious activity from a legitimate account. You might observe one of your vendor's user accounts logging in at odd hours or attempting to access parts of your system they don't normally touch. Because the account is legitimate, it can be very hard to spot.

Your security tools flagging a trusted application. Your endpoint protection might suddenly flag a routine update from a trusted piece of software as malicious. This can happen when an attacker has managed to inject their own malicious code into a legitimate software update.

Category 3: Threats Targeting Your Operations

Once an attacker gets past your people and your technology, their next step is to disrupt your operations and turn their access into a payday. These are the threats that directly target your ability to make money, serve your customers, and keep your doors open.

Threat #6: Malware & Ransomware

Malware is a general term for any malicious software an attacker installs after gaining access. It could be spyware that steals information from your computers, or a keylogger that records everything you type.

Often, this kind of malware runs in the background for weeks or months, gathering information and providing the attacker with a clear picture of your business.

However, the type of malware that grabs headlines is ransomware, and for good reasons.

Ransomware is the final payload, a malware with a business model.

Once the attacker has explored your network, they launch the ransomware, which spreads rapidly and encrypts all your important files. Everything is locked, and the only way to recover it is to pay the attacker for a decryption key.

Some ransomware operators also steal data and threaten to publish it. This is often called double extortion. The risk extends beyond encrypted files to confidentiality, customers and reputation.

So, how do you recognise these threats?

Malware is often hard to notice. The signs can be subtle, such as unexplained slow computers, strange pop-ups, frequent crashes, or software you don't remember installing. Malware may also cause unusual network activity or disable your security tools, making detection difficult without proper monitoring.

Ransomware is the opposite. The signs are impossible to miss. You'll see a ransom note on the screen, and none of your files will open. It's designed to cause an immediate and total work stoppage.

Threat #7: Denial-of-Service (DoS/DDoS) Attacks

Not all attacks aim to steal data or money. Some are simply about causing disruption.

Imagine your business has a single phone line, and a prankster arranges for a hundred people to call it at the exact same time, repeatedly.

Your legitimate customers wouldn't be able to get through. That's essentially what a Denial-of-Service (DoS) attack does to your website or online services. It floods them with so much junk traffic that they become overwhelmed and unavailable to real customers.

When that junk traffic originates from thousands of computers all over the world simultaneously, it's called a Distributed Denial-of-Service (DDoS) attack.

Denial-of-service attacks can disrupt online services. The scale of incidents varies greatly, so focus on knowing which systems are exposed and what protection your hosting or network providers offer.

Ask your website, network and cloud providers how they mitigate unusual traffic and how you would receive updates during an incident.

So, how do you recognise a DoS or DDoS attack?

Your website or online systems suddenly become extremely slow or completely unreachable for legitimate customers.

There may be a sharp surge in Internet traffic, often far beyond normal volumes.

You might receive an email or message from the attacker demanding payment to stop the flood of traffic, a common extortion tactic.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Check payment verification procedures** Use a known telephone number for bank detail changes
☐	**Review exposed logins** Apply MFA, patching and access restrictions
☐	**Review key suppliers** Know how an incident at a provider affects you

PART ONE / UNDERSTANDING THE RISK

CHAPTER 04

Follow a framework: UK Cyber Essentials

When you're starting to build a security programme, it's easy to get lost in the details, buy a bunch of tools you don't need, or just feel completely overwhelmed. A good framework prevents that.

Cyber Essentials is a UK Government-backed scheme developed by the NCSC. It provides a clear baseline of technical controls against common internet-based threats. [S2]

The UK Government's Cyber Security Breaches Survey 2025/2026 reported that 43% of businesses identified a cyber breach or attack in the preceding 12 months, including 46% of small businesses and 65% of medium businesses. These are survey findings, not the likelihood that any particular organisation will be attacked. [S1]

What Each Part Means for Your Business

What makes Cyber Essentials so useful for a business owner is that it's a clear, straightforward certification. It gives you a specific target to aim for and a credible way to prove you've hit it. The programme has two levels, so you can choose which one is right for your business.

Cyber Essentials is an independently assessed self-assessment certification against the scheme requirements. An applicant answers a questionnaire and an accredited certification body assesses the submission.

Cyber Essentials Plus assesses the same scheme requirements and adds independent technical verification within the applicable certification process.

The NCSC describes five technical control areas for Cyber Essentials: firewalls, secure configuration, security update management, user access control and malware protection. [S2]

Firewalls: This is about having a secure barrier between your internal company network and the internet. It means making sure that barrier is set up correctly to block unwanted traffic.

Secure Configuration: This means your computers and software need to be set up securely from the start. This involves simple but critical things like changing all the default passwords on your devices and software and removing any programmes you don't need.

Access Control: This is the "principle of least privilege." It just means your employees should only have access to the data and software they absolutely need to do their jobs, and nothing more.

Malware Protection: You have to protect your business from viruses, ransomware, and other malicious software. This means using up-to-date anti-malware or modern endpoint protection software on all your computers and servers.

Security update management: use supported software and devices, and apply updates within the timescales required by the current scheme requirements. Check the latest requirements before assessment.

Putting the Framework to Work

Because it's a recognized government standard, it gives you a ready-made, credible answer when customers ask about your security. It can be a real competitive advantage and can help you win deals you might otherwise lose, especially if you want to work with UK government departments or large private companies, as certification is often a requirement.

Certification creates a useful baseline and evidence of action. It does not guarantee that every threat is covered, nor does it replace risk management, continuity planning or privacy obligations.

A quick note before we move on: The next part of this book will walk you through the specific actions and controls you need to implement, the "how-to" for things like MFA, backups, and securing your devices.

Work through these controls as part of a simple, repeatable plan. Review what has changed, keep evidence and improve the areas that need attention.

The wider security picture

Cyber Essentials is a strong UK starting point. As your organisation grows, ISO/IEC 27001 can help build a management system for continual improvement, and CIS Critical Security Controls v8.1 Implementation Group 1 provides a prioritised set of technical safeguards. These approaches support one another; none should be treated as a guarantee of security. [S3] [S4]

For smaller organisations, use a framework to set expectations and priorities, not to create paperwork for its own sake. Keep evidence that the important controls are working.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Read the current Cyber Essentials requirements** Check scope, devices, services and technical controls
☐	**Assign one lead for certification preparation** Record gaps and dates
☐	**Review ISO 27001 and CIS Controls v8.1 when useful** Use them to mature governance and technical controls

PART TWO / PRACTICAL PROTECTION

CHAPTER 05

People and identity

Your business has important digital stuff: customer lists, prices, and sales plans. Without good planning, these can get out when an employee leaves, or worse, get stolen in a cyberattack.

This chapter will show you how to control who gets into your systems and data, so your key info stays safe.

Everyone who works for you, employees, contractors, and even your accountant, needs specific access to do their job. Also, the software you use often needs to talk to other apps.

The goal is to make sure everyone and everything only gets access to what's needed, and only for as long as needed. For example, your sales team needs sales software, but they shouldn't see payroll records. When a contractor's project ends, their access should be cut off right away.

You wouldn't let an ex-employee keep their office keys, and it's the same for your digital systems, and so on.

What To Do

You only need four basic habits to get the maximum return with the lowest effort. If you do these four things right, you'll fix most of the problems we've talked about before.

1. Use Multi-Factor Authentication (MFA).

You probably use MFA every day for your bank app. It's that extra code you get on your phone after typing your password. MFA is just a second check to make sure it's you. Your password is the first check ("something you know"), and the code on your phone is the second ("something you have").

A criminal might steal your password, but it's much harder for them to also have your phone.

MFA is important because passwords get stolen often. It's not a question of if your employees' passwords get exposed, but when, and how many.

Without MFA, a criminal who gets one of your employee's reused passwords can easily get into your systems. But with MFA, that stolen password is useless. The criminal might have the password, but when they try to log in, the system will ask for the code from your employee's phone, stopping the attack at the door.

Multi-factor authentication is one of the most valuable protective measures for email, remote access and privileged accounts. Where supported, prefer phishing-resistant methods such as passkeys or security keys.

Why it matters:

A password can be stolen, reused or tricked out of someone. MFA adds a further barrier to account compromise. No single control is a complete defence, so use MFA alongside monitoring and access reviews.

Apply MFA to important systems, check enforcement and avoid leaving exceptions unreviewed.

Do not assume that having an MFA setting available means it is enforced for every relevant user. Ask for a report of actual coverage.

This is the biggest difference between good security and what businesses actually do.

Your insurer may ask whether MFA is used. Review the policy requirements rather than assuming that one answer automatically guarantees or prevents a claim.

Keep evidence of enforcement and review any insurance proposal answers carefully with your broker.

2. Use a Business Password Manager.

Let's be real about passwords. The average person manages dozens, and for some jobs, it's closer to a hundred. Remembering that many unique,

complex passwords is impossible. So, people take shortcuts: they reuse passwords, use small changes, or use personal details like their kid's name or pet's name. They also write them on sticky notes.

Finding shortcuts is part of our human nature, so there's nothing you can do about that. But these habits create a huge security risk for your business.

Data clearly shows that weak or stolen passwords are why most business breaches happen.

Instead of just telling your team to "use better passwords," you need to give them a tool that manages passwords for them: a business password manager.

This is a secure programme where your team can safely create, save, and share passwords. Each employee gets their own encrypted account and only needs to remember one strong master password to open it.

The password manager does the rest, creating random, impossible-to-guess passwords for every website and app they use, and remembering all of them.

This is important for several reasons.

First, it completely solves the password reuse problem. When every site has its own unique, strong password, a data breach at another company doesn't affect you. If an employee's LinkedIn password is stolen, it doesn't matter because their company email password is completely different.

Second, it stops the use of weak, easy-to-guess passwords. Believe it or not, common passwords like "123456" and "password" are still widely used. A password manager makes it easy to use a complex password like "Tr0c3[sub4dour\&R3fls2za@eX\!" for every site, because the user doesn't have to remember it.

Weak and reused passwords still create avoidable risks:

A password reused across services can be exposed by an incident at another provider.

Names, birthdays and familiar words can be easier to guess than long, unique passwords.

A password manager helps people use a different strong credential for each service instead of relying on memory.

A business password manager also provides a safe way to handle shared accounts. Think about your company's social media accounts or a shared vendor login.

How do you share those passwords now? In a spreadsheet? An email? Hopefully not (fingers crossed).

A password manager lets you give specific team members access to that login without them ever seeing the password itself. When an employee leaves, you can remove their access to all shared accounts with one click, turning an unsafe process into a controlled one.

3. Follow the "Principle of Least Privilege."

An employee should only have the absolute minimum access needed to do their job, nothing more.

Your marketing person needs social media accounts and the marketing drive, but not your accounting software.

Your sales team needs the Customer Relationship Management (CRM) software, but they shouldn't see employee HR files.

While this seems like common sense, in many businesses, access is given freely "just in case" someone might need it and is rarely checked or removed.

Over time, this means almost everyone can get into almost everything. One study found that in a typical company, thousands of sensitive files are open to every single employee.

This principle is important, because if an employee's account is ever hacked, the damage is limited.

If an attacker steals a password from one of your sales team members, their first goal will be to move around your network to find valuable stuff, like financial data or server backups. This is called "lateral movement." But if that salesperson's account never had access to the financial system, the attacker is stuck.

Restricting access helps contain damage if an account is compromised. Review permissions for each role, especially administrator accounts, and remove access no longer required.

4. Have a Clear Process for When People Join or Leave.

This solves the problem we talked about at the start of the chapter. You need two simple, non-negotiable checklists: one for when a new person starts and one for when a person leaves.

The "joining" checklist, or onboarding process, makes sure a new employee only gets access to the systems needed for their specific role, based on the rule of least privilege.

They don't get a general login that everyone else has; their access is custom-made for their job from day one.

The "leaving" checklist, or offboarding process, is even more important.

The moment you know an employee is leaving, this process should start right away. It should be a simple list of every account that person has, from their email and main network drive to all the software-as-a-service tools the company uses.

The goal is to shut off all access within minutes, or at the very least within hours.

Offboarding should be prompt and complete. Disable access, recover devices and tokens, check shared credentials and confirm third-party access is removed when someone leaves.

Without a strict offboarding process, you end up with "ghost users", old, active accounts from former employees on your network.

Dormant and unused accounts can create avoidable exposure. Regularly review accounts against the people and services that still need them.

These accounts are a goldmine for attackers. They are often not watched, and if an attacker gets the password for one, they can access your network looking like a real, though old, employee, making them much harder to spot.

Cleaning up these old accounts and having a process to stop new ones from being created is essential.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding a few common mistakes that can undo all your hard work. These seem small but create huge openings for an attacker.

Sharing "admin" accounts.

This is very common, especially in smaller businesses. You might have one main "admin" login for your server or a key piece of software, and everyone who needs it shares the password for convenience. This often happens with outside IT help, where their whole team uses one "admin" login.

The problem is you have no idea who did what.

If someone makes a mistake and takes a system down, or worse, does something bad, you have multiple suspects but no proof. You can't hold anyone responsible because there's no record of who was logged in.

When something goes wrong, you need to be able to check a log and see exactly which person's account made the change. This is the only way to quickly figure out what happened and fix it.

The rule must be simple: one person, one account. Always. This is especially true for any account with the power to change your systems.

Thinking of security training as a one-time thing.

Nobody learns anything from a boring, one-hour security video they're forced to watch once a year.

They click through it to finish, forget everything a week later, and it doesn't change how they act.

What works is short, regular reminders. The goal is to build a habit of healthy caution over time.

People are a key factor in the vast majority of breaches, so this isn't a small issue either.

What to Ask Your IT Provider

As a business owner, your job isn't to do the technical work, but to hold your IT team or provider responsible. You do this by asking simple, direct questions that request proof.

These three questions will tell you almost everything you need to know about how well your people and their access are being managed.

"Can you show me a report that proves 100% of our employees are using MFA on their email?" This is a yes or no question. Don't accept "we're working on it" or "most people are." You need to see proof. Email is the front door to your business, and if even one account isn't protected, it's a huge risk.

"What's our formal process for when an employee leaves? How quickly can you guarantee all their access will be shut off after we tell you?" The first part of this question forces them to have a real, written process, not just an informal "we'll get to it" plan. The second part needs commitment. The answer you're looking for is a specific time, like "within 30 minutes of your notification."

"I need a list of everyone who has admin rights to our network. Let's review it together next week." This is one of the most important reviews you can do. Admin rights are the keys to the kingdom. Those who have them can do anything, including creating new users, deleting data, and turning off security controls. Your IT provider can give you the list of who has these rights, but only you, as the business owner, can decide if they *still* need them.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Enforce MFA for critical accounts** Record coverage and approved exceptions
☐	**Remove unused accounts and privileges** Keep access review evidence
☐	**Provide a business password manager** Discourage reused or shared credentials

PART TWO / PRACTICAL PROTECTION

CHAPTER 06

Devices and endpoint security

Every laptop, computer, and phone used for work is a potential entry point into your business. If these devices aren't secured and kept up to date, they create serious risks. For example, an old, unmanaged laptop can become infected with ransomware, quickly spreading to your main file server and shutting down your entire business. This chapter focuses on managing all devices that access your company's data. Our goal is simple: make sure every device is known, secured, and updated. We're moving from controlling *who* has access to controlling *what* they use for that access.

What You Need to Do

Securing your devices involves a few basic habits. Get these right, and you'll prevent most problems.

1. Keep a Live Inventory of All Devices.

This is the basis for everything else. You need a complete, current list of every computer, laptop, and phone used for your business. A list you update regularly (this is very important) showing what's connected to your business right now.

You can't protect a device you don't know exists.

This is also important if a laptop is lost or stolen. You need a list to know what's missing so you can remotely lock it or wipe its data. If a security incident happens, the first question is always, "What device was involved?" Without an inventory, you're guessing, wasting critical time when trying to stop an attack.

You can't secure what you can't see. An inventory is your single source of truth for what you need to protect.

It's an early warning system. A good inventory system alerts you when a new, unknown device connects to your network, or when a known device hasn't checked in and might be missing.

It's essential for incident response. When an attack happens, knowing which device was the entry point is the first step to containing the problem.

2. Enforce a Secure Setup for Every Device.

Once you know what devices you have, make sure each one has standard, required security settings. This isn't optional. If a device accesses your company's data, it must meet these minimums. Two parts are non-negotiable:

First, every laptop and computer must have **full-disk encryption** turned on. This feature is built into modern operating systems like Windows and macOS. It scrambles all data on the hard drive, making it unreadable without the password. If an employee's laptop is lost or stolen, encryption makes all data useless to the thief. Without it, a thief gains access to your customer list, financial documents, and payroll. With encryption, they just have hardware to sell. It turns a potential data breach into a minor inconvenience of replacing a machine.

Second, your employees should not have **local administrator rights** on their computers for daily work. "Admin rights" means the ability to install software and change core system settings. If employees have these rights, they can accidentally install malware from an email. Worse, if their account is compromised, an attacker can use those rights to install malicious tools, disable security software, and spread across your network. This "lateral movement" turns a small problem on one laptop into a company-wide crisis. Removing these rights creates a huge roadblock for most attacks. If an employee needs new software, your IT provider should have a simple process to approve and install it. This small workflow change makes a huge difference in your security.

A lost or stolen device can expose information if it is not appropriately secured. Full-disk encryption reduces the risk of a thief reading data from the device.

Unnecessary administrator privileges make it easier for attackers to change settings and move between systems. Provide elevated access only where needed and review it.

3. Use Modern Endpoint Protection (EDR).

Traditional antivirus software, which you've likely had for years, is no longer enough. It stops known threats but is blind to modern attacks designed to look like normal activity, using the computer's built-in tools.

You need a modern tool called Endpoint Detection and Response, or EDR.

An EDR system actively monitors your computer systems for suspicious activities and attack patterns. It can identify when a seemingly normal programme, such as Microsoft Word, begins to exhibit unusual behaviour, like attempting to encrypt files, and will then alert you to the potential threat.

The "Response" part of EDR is also critical. When it spots a problem, a good EDR can automatically stop the attack from spreading. For example, it can immediately quarantine an infected computer, cutting it off from the rest of the network. This turns a potential company-wide crisis into a contained problem on one laptop. But the tool is only half the solution.

Someone must monitor the alerts and know how to act when a real problem is spotted.

Employee devices are important entry points. Keep a reliable inventory, maintain supported software and apply protective settings consistently.

Modern attacks are designed to be invisible. Attackers now use "malware-free" techniques, using your computer's legitimate tools against you. Traditional antivirus misses this, but an EDR watching for suspicious behaviour catches it.

A quick response is everything. The difference between a minor incident and a major breach is often minutes. An EDR that can automatically isolate a device buys you critical time to respond before the situation escalates.

4. Have a Consistent Process for Security Updates (Patching).

This is one of the most important and most overlooked parts of basic security. When a company like Microsoft or Google finds a security hole in their software, they release a fix called a "patch" or an update.

The moment they announce that patch, a race begins. You and your IT provider try to install it on all your computers. At the same time, bad actors use automated tools to scan the internet, looking for businesses that haven't installed it yet. They know exactly what the unlocked door looks like and have powerful tools to find it.

This is why a consistent, repeatable process for installing updates is so important. You can't put it off. Attackers can exploit newly announced vulnerabilities in hours. If you only install updates monthly or whenever convenient, you leave a massive window of opportunity for them to get in.

Your process doesn't have to be complicated, just consistent. Critical updates for operating systems and web browsers should be installed weekly. For severe, "zero-day" vulnerabilities under active attack, the patch needs to be applied within a day or two. Your IT provider should manage this automated process, and you should get a simple monthly report showing the percentage of your computers that are fully up to date.

Attackers exploit vulnerable systems, especially those exposed to the internet. Prioritise high-risk fixes, track exceptions and confirm updates are applied.

New software vulnerabilities are reported continually. A repeatable process matters more than chasing every headline in isolation.

The gap between patching and attacking is where you get hit. The average organisation takes around **55-67 days to install patches for half of their critical vulnerabilities**. Attackers can exploit those same vulnerabilities in hours. A consistent, fast patching process closes that dangerous gap.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding common mistakes that can undo all your hard work. These seem small but create huge openings for attackers.

Letting employees be administrators on their own computers.

This common mistake is usually for convenience. When an employee has "admin rights," they can install any software and change any setting.

The problem is, if they click a malicious link, any malware installed also gains those admin rights. It can embed deep into the computer, disable security, and spread to other network computers.

Excessive access can enable an attacker to spread from one system to another. Least privilege and network segmentation reduce the opportunities.

Removing these rights is a simple, huge win for your security.

Having no plan for personal devices.

It's common for employees to use personal phones or laptops for work, known as "Bring Your Own Device" (BYOD). The problem is, you don't know if that personal device is secure. Is it encrypted? Does it have a password? Is its software updated?

Personal devices used for work can put company information at risk if they are unmanaged or lost. Decide what is permitted and how to enforce those rules.

You can't ignore this. If employees use personal devices for work, those devices must meet your minimum security standards, like having a passcode and encryption. Simple tools can enforce this without accessing personal photos or texts.

What to Ask Your IT Provider

“Can you show which devices access our company information, which are encrypted and which fall outside our policy?” Ask for a current report and an explanation of gaps.

"What is our process if an employee's laptop is lost or stolen? How quickly can you guarantee it can be remotely locked or wiped?" The first part forces them to have a real, documented process. The second part is for a commitment. You need to know you can contain the damage from a lost device before someone tries to break into it.

"What endpoint protection tool are we using? Is it being actively monitored for alerts by a person?" This two-part question is critical. First,

what tool? You want to hear it's a modern EDR, not just basic antivirus. Second, and more important: is a person watching the alerts? You need to know that if an alert comes in at 2 AM, someone will see it and act.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Keep a current device inventory** Include portable and personal devices used for work
☐	**Check encryption and updates** Record compliance and exceptions
☐	**Confirm endpoint protection is working** Review alerts and coverage

PART TWO / PRACTICAL PROTECTION

CHAPTER 07

Email, web and collaboration

Email, web browsers, and collaboration tools like Microsoft Teams, Slack, and Google Drive are essential for business. They're how teams communicate internally and with customers, carrying everything from invoices and contracts to sensitive customer information and private company plans.

Unfortunately, this makes them prime targets for cyberattacks.

Business email compromise can lead to fraudulent payments or disclosure of information. Verify unusual or changed payment requests through a trusted, separate channel.

Phishing remains a common way to target employees. Focus on reporting, practical training, protective email controls and a culture that encourages people to check.

This chapter will show you how to protect these vital communication channels by putting smart filters and safeguards in place to stop attacks and keep your information private.

What You Need to Do

Here are four simple habits and tools to protect your company's communication channels. Get these right, and you'll have a strong defence against the most common attacks.

1. Use an Advanced Email Security Tool.

Basic spam and virus filters in Microsoft 365 or Google Workspace are good for junk mail and known viruses, but they aren't designed to stop targeted, well-crafted attacks. An advanced email security tool adds an

extra layer of protection, like a deadbolt and a security camera, to catch more sophisticated threats.

These tools do things basic filters can't. When an email with an attachment comes in, a good security tool opens it in a safe, isolated environment (a "sandbox") to see if it's malicious. If the attachment tries to install malware, the tool blocks the email before it reaches your inbox.

It also analyzes links in emails. If an employee clicks a link, the tool checks the destination in real-time. If it leads to a fake login page or a site with malware, it blocks the connection and warns the user. This is your best technical defence against phishing attacks and catches mistakes when busy employees click something they shouldn't.

The numbers show how critical this is:

Email and collaboration systems are used to deliver malicious links and attachments. Security filters, safe configuration and staff awareness all matter.

2. Create a Non-Negotiable Process for Financial Transactions.

This is a business rule, not a technology solution, and it's the most important thing you can do to prevent wire transfer fraud. Any request to change a vendor's bank details or make an unusual or urgent payment must be verified with a live phone call to a number you already have on file for that person.

An email or text message is not enough. You must talk to a real person on the phone using a legitimate number you know, not one provided in the email request.

This is crucial because technology alone can't solve this process-based defence.

The scam works by tricking a person. Attackers weaponize your trust in your vendors and your team. The only way to break that deception is to step outside the attacker's channel (email) and use a different one (the phone).

This simple habit, when it becomes a non-negotiable part of your company's culture, stops the most common and costly form of email fraud.

It protects your employees from difficult situations and safeguards your company's bank account.

3. Filter Your Team's Web Traffic.

Think of this as a mandatory seat belt for the internet. A web filter automatically blocks your employees from accessing known malicious or suspicious websites. While these filters used to be physical boxes in the office, now, with remote work, this protection must be installed directly on employee laptops, so it travels with them wherever they are.

This is important because it acts as a critical safety net. Many attacks start with a bad link in an email. A web filter is your last line of defence when a busy employee makes a mistake and clicks. If the link leads to a website known for malware, the web filter blocks the connection before their computer gets infected. If it leads to a fake Microsoft 365 login page designed to steal passwords, the filter blocks it before they can type anything.

It protects your employees from split-second mistakes that can cause company-wide disasters. It's an automated guardrail that keeps them on the safe part of the road.

The numbers show why this safety net is necessary:

Social engineering exploits attention and trust. Give employees a straightforward way to report a suspicious message, even if they have already clicked.

When people fall for these scams, it happens incredibly fast. The median time for a user to click a phishing link is **less than 25 seconds**. This isn't enough time to stop and think, which is why you need an automated tool.

Make it easy for colleagues to verify unexpected requests. A short phone call to a known number can prevent a costly mistake.

4. Set Secure Defaults for File Sharing.

Collaboration tools like Microsoft Teams, SharePoint, and Google Drive are great for work, but they often prioritise ease of sharing over security. The most dangerous feature is the "share with anyone" or "public link" option,

which creates a link anyone on the internet can use to access a file or folder without a password or login.

Sensitive data often leaks from these platforms when an employee accidentally creates one of these public links. They might be trying to share a folder with a single client but, in their rush, click the wrong option. Now that folder, potentially containing sensitive contracts or financial information, is public. The link can be forwarded, posted online, and sometimes even found by search engines.

This is why it's vital to configure these tools so that any new file or folder is **private by default**.

Sharing should be an intentional act, not the default. Make the secure way the easy way. An employee should take extra steps to share something publicly, forcing them to think about their action. Setting the default to private prevents this entire category of accidental data breaches.

The data shows how widespread poorly configured cloud tools have become:

Cloud data can be exposed by overly broad sharing settings, misplaced information or incorrect permissions. Configure services intentionally and review access.

Cloud services are not automatically secure simply because the provider is well known. Customers retain responsibilities for identity, settings, data and access.

Common Mistakes to Avoid

As we previously established, getting the big things right is half the battle; the other half is avoiding common mistakes that can undo all your hard work. These seemingly small things create huge openings for attackers.

Assuming the default security in Microsoft 365 or Google is enough.

Many people think the basic security that comes with Microsoft 365 or Google is sufficient. These default filters often aren't good enough to stop well-crafted, targeted attacks, like the fake invoice scams we've discussed. Attackers know what these filters look for and design their attacks to

bypass them. You need an additional layer of security specifically designed to spot these more advanced, targeted threats.

Trusting email for anything involving money.

This is a big one. Email was never designed to be a secure way to move money. Attackers can easily make an email look like it came from someone you trust. They can fake the sender's name and sometimes even the email address itself, making it very hard to spot. Any time money is involved, you must assume the email could be fake.

Thinking security training alone will stop phishing.

Security training is important; you should absolutely teach your team what to look out for.

However, you can't expect training alone to solve the problem. People get busy, distracted, and make mistakes. Attackers design their scams to exploit these moments of distraction. A person only needs to make one mistake on one busy afternoon for an attacker to get in.

That's why you need the technical controls we've discussed, like an advanced email filter and a web filter. They are the safety net for when a person inevitably makes a mistake.

What to Ask Your IT Provider

Your job as the owner isn't to do the technical work, but you must hold your IT team or provider accountable. Do this by asking simple, direct questions that require proof, not just promises.

"What specific tool are we using for email security that goes beyond the basic built-in filter? How does it protect us from someone clicking a bad link?" If they can't explain in simple terms how the tool protects you from a bad link, then it isn't doing its most important job.

"Can you configure our email system to put an automatic warning banner at the top of all emails that come from outside our company?" This is a simple but incredibly effective control. A banner saying "**EXTERNAL EMAIL**" at the top of an email constantly reminds your team to be a little more skeptical. It's especially helpful for spotting scams where an attacker

tries to impersonate you or another company leader. It's a simple nudge that can prevent a huge mistake.

"Are our company's file-sharing settings in Teams/Google Drive set to 'private by default'? Can you show me the policy that enforces this?" This question checks if you're protected from accidental public sharing leaks. The answer should be a simple "yes." The second part, "Can you show me the policy," is where you get the proof. They should be able to show you a screenshot of the administrative setting that enforces this across your entire company. This confirms it's a real, enforced rule, not just a suggestion.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Protect business email** Review MFA, filtering and external sharing settings
☐	**Verify payment changes independently** Train staff on the agreed process
☐	**Make reporting simple** Record suspicious emails and lessons learned

PART TWO / PRACTICAL PROTECTION

CHAPTER 08

Data protection

Losing your business data in a cyberattack or technical failure can mean the end of your business. This chapter shows you how to keep your data safe and always available.

We'll cover two key areas: confidentiality, which means only authorised people can see your data, and availability, which means you can always access it.

What You Need to Do

Protecting your data comes down to four basic habits. Get these right, and you'll have a strong safety net for your business data.

1. Follow the 3-2-1 Backup Rule.

This simple, proven strategy helps you recover from any data loss.

Keep at least **3** copies of your data: your live data plus two backups.

Store those copies on **2** different types of storage, like your server and a separate backup device, or a local device and a cloud service.

Keep **1** of those copies offsite and completely separate from your main network.

This rule protects you from a single event destroying everything. For example, if a fire destroys your office, your cloud backup remains safe.

The most important part of this rule today is the **one isolated copy**. This is your best defence against ransomware. Attackers know businesses use backups, so they often target backups first, encrypting or deleting them before locking your main files.

An isolated copy is one an attacker can't reach from your main network. There are two main ways to achieve this: an "air-gapped" backup or an "immutable" backup.

An air-gapped backup is physically disconnected from the network, like an external hard drive you plug in, use, and then unplug and store safely.

An immutable backup, offered by many cloud backup services, prevents anyone, even you, from changing or deleting a backup for a set period. This protects against ransomware attacks that spread to connected backup drives, like the one in the story we began with.

Attackers may attempt to damage or delete backups as part of a ransomware incident. Protect backups from ordinary administrator accounts and keep resilient copies.

Recovery times depend on what is backed up, how much data must be restored and whether the affected services are available. Test against real business needs.

Backup failures are common. One study found that backup errors, including corrupted backups from ransomware, contributed to about **one-third of all data loss incidents**.

2. Test Your Backup Restores Regularly.

A backup is only good if you can use it. The "Success" message on your backup software doesn't mean you can recover your business. It only means files were copied. You won't know if those files are usable or if you have everything you need until you test a restore.

A restore test is a scheduled drill where you recover files, folders, or even entire systems from your backup. You don't have to restore your whole company every time, but you do need to test regularly.

These tests help you find problems when the stakes are low. You want to discover a critical folder was missing, a database is corrupted, or a needed software licence key is missing during a test, not during an actual ransomware attack.

Plus, doing these drills helps to build your team's muscle memory. In a real crisis, they'll follow a practiced checklist instead of trying to figure things out for the first time.

An untested backup is an assumption, not a reliable recovery capability. Restore a meaningful sample and record the result.

Include backup restore tests in your regular maintenance schedule, with clear owners and evidence.

3. Know Where Your Most Important Data Lives.

You can't protect your most important data if you don't know where it is. Just as you know where physical assets are kept in your office, you need to know where your digital "crown jewels" are. This is often harder to track.

Over time, data spreads out. A critical sales proposal might be saved to someone's desktop instead of a shared drive. An important financial spreadsheet could end up in a personal Dropbox folder. An old customer list might be on a spare laptop in a closet. When data is scattered, it’s hard to protect it.

Files on desktops or in personal cloud folders aren’t backed up by your company system and lack the same security as files on your main server.

Ask yourself these questions:

Where are our accounting files?

Where is our main customer database?

Where are our employee HR records stored?

Where do we keep our signed contracts and intellectual property?

Once you know where this critical data should live, you can protect it. You can confirm that location is backed up and apply tighter security controls, limiting access to only those who need it. This lets you focus your efforts on what truly matters.

Shared cloud folders can accumulate sensitive data and broad permissions. Review where important information is stored and who can access it.

Most companies don't track data well. Another study found that **only one out of every 10 companies** had a good system for labeling files, making it nearly impossible to track sensitive data.

4. Encrypt Devices That Store Company Data.

You must enable the built-in encryption on all company laptops. This is a feature you already have; you just need to turn it on for everyone.

Encryption scrambles all data on the hard drive, making it unreadable without the password. This is crucial because laptops are often lost or stolen. If an employee leaves a laptop in a coffee shop or it's stolen from their car, an unencrypted device gives a thief full access to your customer lists, financial documents, payroll information, and saved passwords. This is a full-blown data breach.

With encryption, a stolen laptop is just hardware. The data remains safe. This turns a potential disaster, which you'd have to report to customers and your insurance company, into the simple inconvenience of buying a new laptop.

Encryption is particularly important for devices that can be lost or stolen. It reduces confidentiality risk when correctly configured and managed.

Check encryption status centrally where possible and keep recovery-key procedures secure.

Common Mistakes to Avoid

Getting the big things right is important, but avoiding a few common mistakes is equally vital. These seemingly small errors can create big security holes.

Keeping your only backup copy connected to the main network.

Hackers are smart. They often target and destroy backups first, then launch ransomware, leaving you with no way to recover.

Your only safe copy must be isolated from your main network, either physically disconnected (air-gapped) or protected in the cloud where it can't be changed (immutable).

Forgetting to back up key data.

This happens often when you don't know where your important data lives. Your main server might be backed up, but a top salesperson could be saving important proposals to their desktop.

Your finance team might have a critical spreadsheet in a personal OneDrive folder. This data isn't backed up by your company's system. If that laptop dies or the employee leaves, the data is gone. You need to identify your "crown jewel" data and ensure it's saved in centrally managed locations, so it gets properly backed up.

Confusing a cloud sync service with a true backup.

Many people believe that because their files are in Dropbox, Google Drive, or OneDrive, they are backed up. This is incorrect. These are file synchronization services, great for collaboration, but not backups.

If you accidentally delete a file, it's deleted from the cloud. If ransomware encrypts your files, those encrypted files sync to the cloud, overwriting your good copies.

A true backup is a separate, point-in-time copy of your data, protected from such changes. A sync service is not designed to be a safety net.

What to Ask Your IT Provider

These three questions will tell you almost everything about your data protection.

"When was our last full restore test? How long did it take, and can I see the report?" This is a direct accountability question. Don't accept "we run backups every night." You need to know about the *restore*. The answer should be specific, like: "We did a test last quarter. We restored the main file server. It took four hours, and here's the one-page summary of the results." This proves they are testing and gives you a real idea of how long you'd be down in a crisis.

"Show me how our offsite backup copy is protected from a ransomware attack. Is it offline, or 'immutable'?" This question addresses the biggest threat to your recovery plan. If offline, ask them to describe the physical process. If immutable, ask them to show you the setting in the cloud backup service that confirms it can't be deleted. This confirms you have a safe copy an attacker can't destroy.

"Can you provide me with a list of the critical data locations that are being backed up to confirm we haven't missed anything important?" This addresses the "know your data" problem. Give your IT provider a list of your most important data locations, the accounting folder, customer database, contracts drive. They should return with a report or screenshot showing these exact locations are included in the backup job.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Identify critical and personal information** Know where it is stored and who can access it
☐	**Protect and test backups** Record restore results
☐	**Limit access and sharing** Review permissions and encryption

PART TWO / PRACTICAL PROTECTION

CHAPTER 09

Networks and cloud basics

Your business network is like the nervous system of your company. It connects everything: your employees' laptops, your servers, and your cloud services. If an attacker breaches this network, you know what comes next... your entire business is at risk. Yes, this can be said for most of the topics we discussed, and it's true for your network as well.

This chapter will show you how to set up a secure "floor plan" for your network and cloud services, creating separate, secure zones. This prevents problems in one area from spreading to your whole company, keeping your data private and protected.

What You Need to Do

To manage your network and cloud services securely, focus on these three habits. They prevent most of the problems.

1. Segment Your Network.

Think of your network as an office building. You wouldn't let a visitor from the lobby walk freely into your server room. The same applies to your computer network. Network segmentation means putting up walls inside your network to create separate, secure zones.

At a minimum, create a separate Wi-Fi network for guests. This guest network should only allow internet access and be completely isolated from your main business network. This simple step stops threats like malware on a guest's laptop from reaching your company's systems.

For even better security, use three separate zones:

A main network for trusted, company-managed computers.

A guest network for visitors, with internet-only access.

A third network for less-secure devices like smart TVs, security cameras, or employees' personal phones.

This segmentation contains threats. If an attacker compromises your smart TV, they can't use it to attack your main server. It limits damage. Without these internal walls (a "flat network"), attackers can move freely, known as "lateral movement", to find your most valuable data. Segmentation makes this much harder.

Network segmentation can limit how far an intruder can move. Prioritise critical systems and separate guest or untrusted networks.

It protects you from things you can't control. You can't control the security of visitors' laptops or employees' personal phones. Segmentation gives them internet access without exposing your business to device risks.

2. Secure Your Remote Access.

As more employees work remotely, how they connect to your company's systems becomes a major target for attackers. You must lock down these digital doors.

Never expose tools like Remote Desktop Protocol (RDP) directly to the internet. RDP is a built-in Windows tool for remote computer control. Exposing it to the internet is like plastering a “hack me” sign over your business.

Ransomware gangs use automated tools to scan the internet 24/7, looking for this mistake.

They will find your open RDP server and use other automated tools to guess the password. If they get in, they have full control of your server, and a ransomware attack is often hours away.

All remote employee access should go through a modern, secure gateway that requires multi-factor authentication (MFA). This means even if an attacker steals an employee's password, they can't log in without the employee's phone to approve access.

This is a primary target for ransomware. Microsoft repeatedly states that unprotected RDP is a top attack method ransomware gangs use to enter businesses.

Remote access is valuable but must be secured. Limit exposed services, require strong authentication and monitor for unusual use.

3. Set Cloud Services to "Private by Default."

When using cloud services like Microsoft 365, Google Drive, or Dropbox, understand your security responsibilities.

The provider (Microsoft, Google, Amazon) secures the cloud itself, physical data centers, servers, and core networks. You are responsible for security in the cloud, how you set it up, who has access, and how you protect your data.

The biggest cloud mistake comes down to simple human error, like many things in cyber security.

An employee, in a hurry to share a folder with a client, clicks "share with anyone" or "public link." They've just made that folder, and everything in it, public. Anyone with the link can access it without a password or login.

This is why you must set a rule: any new cloud storage, a new SharePoint folder, a new site, a new Amazon S3 "bucket", must be created with the most secure, private settings.

Access should never be open by default. You should grant access deliberately, one person at a time. The secure way should be the easy way; the risky way should require extra steps and approvals.

This mistake is the most common cause of massive cloud data breaches. An employee doesn't mean to leak your customer list or financial projections, but if the default is "public," it's incredibly easy to do accidentally. Setting the default to "private" prevents this type of data leak. It's a simple change that acts as a powerful safety net against everyday human error.

Misconfiguration is a significant cloud risk. Review internet exposure, access permissions, logs and unused services regularly.

Understand your organisation's share of cloud security responsibilities. Provider security does not remove the need to manage your own identities and information.

Common Mistakes to Avoid

Getting the big things right is crucial, but avoiding these common mistakes is just as important. They may seem small but create huge openings for attackers.

Assuming your cloud provider manages all your security.

This is a costly misunderstanding. When you use services like Microsoft 365 or Google Workspace, you're in a "Shared Responsibility Model." The provider secures the cloud itself, physical data centers, servers, and core networks.

You are responsible for security in the cloud, controlling access, permissions, and data sharing. The cloud provider gives you the security tools, but you must use them.

Using a shared password for your main Wi-Fi network.

This is another convenience-driven mistake that creates big risks. If you have one password for your main company Wi-Fi and give it to every new employee, what happens when an employee leaves? To revoke their network access, you must change the password, then update every device in the office.

This is a huge hassle, so it rarely happens. This means an ex-employee could potentially connect to your internal business network months or even years later. Modern Wi-Fi systems solve this by letting each employee log in with their unique username and password, the same one they use for their computer. When they leave, you simply disable their account, and their Wi-Fi access is gone.

What to Ask Your IT Provider

These three questions will tell you almost everything you need to know about how well your network and cloud services are managed.

"Is our guest Wi-Fi network completely separate from our main business network? Can you show me the configuration that proves it?" This is a yes or no question. They should show you a screenshot of firewall rules or network configuration clearly blocking traffic from the "Guest" network to the "Internal" network. This is a simple visual confirmation that the wall is in place.

"Do we have any services, especially Remote Desktop (RDP), exposed directly to the internet? I need confirmation that all remote access is routed through a secure, managed gateway." This confirms they've closed the most dangerous door and replaced it with a secure one requiring multi-factor authentication.

"What is our process for ensuring a new folder or site in SharePoint is created with private, not public, settings by default?" This checks if you're protected from accidental cloud data leaks. The IT provider should show you the administrative setting in Microsoft 365 or Google Workspace that enforces this for all users company wide. It shouldn't be a suggestion to employees; it should be a technical control that makes the secure option the default. This proves they manage your cloud environment proactively, not just reacting to problems.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Review internet-facing services** Remove unnecessary exposure
☐	**Separate guest connectivity** Keep guests away from business systems
☐	**Audit cloud sharing and permissions** Check access, logging and ownership

PART TWO / PRACTICAL PROTECTION

CHAPTER 10

Supplier and third-party risk

All businesses rely on outside partners and vendors to function. Each of these connections is a potential entry point for cyber attackers, even if your own security is strong.

A problem at one of your vendor's companies can quickly become a disaster for your business.

This chapter will show you how to manage these risks. The goal is to understand the risks each partner brings and to set up simple ways to check their trustworthiness and limit their access to only what's necessary.

What You Need to Do

You need to develop four basic habits to manage the risks that come with your partners. If you do these four things well, you'll have a strong, sensible way to protect your business from its supply chain.

1. Sort Your Vendors by Risk.

First, identify all your vendors. In security, a "vendor" or "third party" is any person, company, or software service that connects to your business or handles your data. This includes your IT provider, payroll company, accounting software, CRM for sales, and even your marketing newsletter tool.

Once you have this list, sort them. You can't treat your coffee supplier the same way you treat the company that has access to your server. This isn't efficient or necessary. The goal is to put them into simple groups so you can focus your attention where the risk is highest.

To do this, ask two questions for each vendor:

How critical are they to your daily operations? If they stopped working for a day, would it be a minor or major problem?

How sensitive is the data you're giving them? Are they just getting your public address, or are they getting your employees' personal information and your company's financial data?

This will naturally group your vendors.

Your "high-risk" vendors are those that are critical to your business and that handle your most sensitive data. This list will be short. It typically includes your IT provider, payroll provider, and perhaps your main accounting or operational software. These are the partners that, if they had a problem, could put you out of business. These are the only ones you need to spend significant time on. All other vendors fall into a lower-risk category.

2. Ask Basic Security Questions Before You Sign a Contract.

Once you know who your high-risk vendors are, talk to them about security.

For any new high-risk vendor, have a short, simple list of questions to ask before signing the contract. You're just trying to confirm that they take security as seriously as you do.

Here are some good, direct questions to ask:

Do they use multi-factor authentication (MFA) for all employees who access your data?

Do they have a consistent process for installing security updates on their systems?

How do they protect your data when they store it? Is it encrypted?

What happens if they have a security problem? How quickly will they tell you about it?

This is very important because a problem at your vendor's company can quickly become your problem.

A third-party breach may become your incident if the supplier processes your information or holds privileged access to your systems.

Keep a prioritised supplier list and focus assurance on critical services and sensitive information.

3. Give Vendors Limited and Time-Based Access.

You must strictly enforce this rule. When you give an outside person or company access to your systems, do it in a very specific way.

First, **never use shared accounts.** It's common for a business to create one login, like "IT_Vendor_Admin," and give the password to their entire IT support team. This is a big mistake. If something goes wrong, a file is deleted, a setting is changed that crashes your system, you have no idea who did it.

You only know it was someone from the vendor. This means no accountability. The rule must be simple: every single outside person who needs access to your systems gets their own unique, named account. That way, if "john.smith@itvendor.com" makes a change, you know exactly who it was.

Second, that account should be **limited to only what they need for their job.** This is the "principle of least privilege" we've discussed before, but it's even more important for outside vendors. If you've hired a company to work on your website, their account should only give them access to the website server, not your main file server or your accounting software. This is how you limit the damage if that vendor's account is ever compromised.

Finally, every vendor account must have a **set expiration date.** If you hire a contractor for a three-month project, their account should automatically turn off on the last day of that project. This is critical because it's easy to forget to remove a vendor's access when their work is done. These old, forgotten accounts, often called "ghost users," are a huge security risk.

This is important because it closes one of the most common security loopholes in business. When a project ends, nobody thinks about the login that was created for it. It just sits there, active and unmonitored, sometimes for years. An attacker who compromises that old account can

get into your network while appearing to be a legitimate, if old, partner, making them much harder to spot.

Unused vendor accounts are a common governance weakness. Set expiry dates and review them after each engagement.

4. Include Security in Your Contracts.

The conversations you have with your vendors about security are important, but you need to put those promises in writing. The best way to do that is by adding a simple security clause or a one-page addendum to your contracts with your high-risk vendors.

This is important because it makes security a formal, legal obligation. It sets clear, written expectations for how they will protect your data and what will happen if they don't.

Your security addendum doesn't need to be a 50-page legal document. It just needs to cover a few basic, common-sense points. It should require the vendor to maintain reasonable security practices, like the ones we've talked about in this book, using MFA for their employees, keeping their systems updated, and encrypting your data.

But the single most important part of this contract clause is the **breach notification requirement.** Your contract must state that if the vendor suffers a data breach that affects your data, they must tell you about it within a specific, short timeframe, like 24 or 48 hours.

The longer it takes for you to find out about a breach at your partner's company, the more damage an attacker can do to your business. A fast notification gives you a chance to react, to shut off their access, change passwords, and protect yourself before the problem spreads.

The sooner you learn of a supplier incident, the sooner you can limit damage. Agree practical notification times and contact routes in advance.

Breaches involving stolen credentials take the longest to find. The average time to identify and contain a breach that starts with a stolen password is a full **292 days**. If that stolen password belongs to your vendor, you might not know about the problem for months unless they are legally required to tell you.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding a few common mistakes that can undo all your hard work.

Assuming a vendor is secure because they are a well-known brand.

It's easy to assume that a big, well-known company has perfect security. But that's a dangerous assumption. Big companies get breached all the time. In 2023, a single vulnerability in a popular file transfer tool called MOVEit led to breaches at thousands of organisations, including many household names.

Supplier incidents can affect organisations of every size. A vendor's scale or reputation does not remove the need for due diligence.

You must do your own basic checks and ask your own questions.

Signing up for new software services without any security review.

This is often called "Shadow IT." An employee needs to solve a problem, so they do a quick Google search, find a new software tool, and sign up for it with the company credit card. They've solved their problem, but they've also just created a new security risk.

You now have sensitive company data, maybe a customer list or some financial information, being stored in a service you don't know about, don't manage, and haven't checked for security. You can't protect data you don't know you have.

What to Ask Your IT Provider

These three questions will tell you almost everything you need to know about how well your vendor risk is being managed.

"Can you give me a list of all non-employee accounts with access to our network? Let's review who owns them and when their access is set to expire." For every account on that list, there should be a name of a current employee who is responsible for it (the "owner") and a date when that account's access will automatically turn off.

"What is our process for reviewing the security of a new software tool before a department starts using it?" It should be a simple, fast process where, if a team wants to use a new tool, they fill out a short form, and

your IT provider does a quick, 15-minute check to make sure the tool is reasonably secure before any company data goes into it.

"Let's say one of our high-risk providers had a security breach. Walk me through the exact steps we would take to immediately disable their access to our systems." This is the ultimate "what if" question. It tests their preparedness for a worst-case scenario. They should have a documented "kill switch" plan that details the exact steps they would guide you through to immediately lock them out of your systems to contain the damage.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**List essential third parties** Name business owners and critical dependencies
☐	**Review access rights and contracts** Check expiry, incident notification and data handling
☐	**Prepare for vendor failure** Agree an alternative or recovery approach

PART THREE / RESILIENCE AND ASSURANCE

CHAPTER 11

Incident response and business continuity

At the risk of sounding gloomy, I have to state the obvious: a cyberattack could devastate your business leading to lost revenue, a damaged reputation, and legal issues.

That's obviously something you don't want to happen. Unfortunately, sometimes it does. And even more unfortunate, many small businesses lack a clear plan for what to do when an attack happens, leaving them vulnerable.

The good (or reassuring) news is, this chapter will show you how to create a simple, actionable plan to protect your business and keep it running, even during a crisis.

Your plan should have two key parts that people often confuse, but they serve different purposes.

First is your **Incident Response** plan. This is your "firefighting" strategy.

It focuses on the technical problem: stopping the attack, finding out how it happened, and fixing the damage. It's all about containing the problem and getting your systems back to a safe state.

Second is your **Business Continuity** plan. This plan focuses on your business operations.

It explains how you'll keep taking orders, serving customers, and making payroll while the technical problem is being fixed. For example, if your

main server is down, how will you still ship products? If your accounting system is locked, how will you send invoices? This plan keeps your business functional and money coming in, even when your technology isn't working.

An "incident" is any event that threatens your ability to operate or protect your data. This could be a ransomware attack, a server crash, critical software failing, a stolen laptop with sensitive data, or even a power outage. If it impacts your money, your data, or your customers, treat it as an incident and start your plan.

Step 1: What to Do Before Anything Happens (Preparation)

Your preparation largely determines how well you'll handle an incident. A good plan is a short, simple guide you can use fast, when needed.

Print it out and keep copies in safe, accessible places: in your desk, at home, even in your car. This way, you can get to it even if your office is inaccessible or your computer network is down.

A. Name Your Contacts

Your plan needs a simple list of names and phone numbers. No one should have to guess who to call when something goes wrong. This list should be the first page of your plan. It needs to name the specific people who will form your small incident response team. You only need to cover three main roles, and one person can fill multiple roles.

The Leader: This person manages the overall response. They make big business decisions, like whether to shut down a system or communicate with customers. This is usually you, the owner, or another senior leader.

The Technical Contact: This is the first person anyone in the company calls if they see something strange. They start the technical investigation. This could be your internal IT person or your main contact at your IT provider/MSP.

The Business/Comms Contact: This person manages communication with employees and customers and finds ways to keep the business running. They handle the business continuity side of things.

For each person, list their name, their role, and their personal cell phone number. Don't just list an office extension. In a real crisis, your phone system might be down, so you need a direct way to reach them.

Your contact list should also include key outside parties.

Your cyber insurer: if you have a policy, follow the incident notification requirements promptly. Check whom to contact, what evidence to retain and whether prior consent is required for particular costs.

Law Enforcement: You should report the incident to your local law enforcement. Depending on where you are, you may also need to report it to national or regional cybercrime authorities. This is important for the investigation and for meeting any legal obligations you might have.

Your Lawyer: Have the contact information for your company's legal counsel on this list. You will need their advice on your legal and regulatory responsibilities, especially if customer data was involved.

B. Know Your Critical Operations

This is the business continuity part of your preparation. Sit down with your team and list the parts of your business that must keep running.

Ask questions like:

If our main server goes down, how do we keep shipping products?

If our accounting system is locked, how do we send invoices and make payroll?

If our customer relationship management (CRM) software is offline, how does our sales team track leads and orders?

For each critical operation, figure out a simple, manual workaround. If the shipping system is down, can you switch to paper work orders for a day or two?

If the accounting system is offline, do you have a way to create basic invoices from a template?

Having these fallback plans ready keeps your business from stopping completely while the technical problem is fixed. This list also tells your technical team what to recover first.

C. Create the "Stop and Call" Rule for All Staff

This is the most important rule to teach everyone in your company. If you see anything strange on your computer, stop what you are doing and immediately call the technical contact on your list.

Don't try to fix it yourself. Don't finish that email. Don't assume it's just a glitch. Just stop and call.

This is vital because, in a modern cyberattack, speed is everything. Attackers use automated tools that can spread through a network in minutes.

A recent Palo Alto Networks report found that in nearly one in five cases, attackers were stealing data within the first hour of getting into a network.

An employee noticing something strange and reporting it right away is often your only chance to contain the problem before it becomes a company-wide crisis. An employee trying to "just finish one more thing" can be the difference between a problem on one laptop and a ransomware attack that takes down your entire business.

D. Don't Rely on "Heroics"

When you write this plan, don't rely on one person.

It's easy to think, "We'll just call Bob," because Bob is your IT genius who knows everything. But that creates a single point of failure.

What if the incident happens at 2 AM and Bob's phone is off? What if he's on vacation?

Your plan needs to be a simple checklist that any manager in your company could pick up and follow for the first hour. It should be clear enough that they can make good basic decisions even under stress.

This is even more important with the widespread shortage of cyber security skills. Data shows that breaches at companies with a high security skills shortage cost millions more than those without this problem.

You can't let your entire response depend on one person's availability and expertise. The goal is to create an orderly, repeatable process anyone can follow, not to rely on one specific person to save the day.

Step 2: What to Do During an Incident (Action)

An incident has just been reported. Someone on your team followed the "Stop and Call" rule.

This is where your preparation pays off. The goal now is to move from reacting to acting, following the simple playbook you've already created.

A. Contain the Problem

Your first job is to stop the problem from getting worse. Think of it like a fire: you have to put it out before you can rebuild. In a cyber incident, this is called containment, and speed is key.

The first priority is to isolate the affected computers, without turning them off. If an employee's laptop is acting strangely, your technical contact should immediately take it off the network. Unplug the network cable.

Turn off the Wi-Fi. But keep the device powered on.

This stops the problem from spreading from that one computer to your server or other office computers.

Next, change any passwords that might have been compromised. If the incident started on an employee's computer, assume any passwords they used or saved on that machine are now in the attacker's hands.

Their main network password, email password, and any other important accounts need to be changed right away.

Finally, stop any automated processes that could worsen the problem.

For example, if you have a system that automatically syncs files between your server and a cloud service, you might need to pause it. Otherwise, it could sync encrypted files from a ransomware attack to your cloud storage, overwriting your good backups.

One more critical point on containment: **you MUST preserve evidence**.

The first instinct in a crisis is to start shutting things down and cleaning things up. You have to fight that urge. The affected computers are now a crime scene, and you need to treat them that way.

Don't turn anything off unless your technical expert tells you to. A lot of important evidence lives in a computer's active memory and disappears the second you pull the plug.

Keep a simple log of every action you take, with the time and the name of the person who took it. This will be incredibly important for the investigation and for any insurance or legal claims later.

Prompt containment matters. Ensure staff know how to report a suspected incident, and that technical responders can disable accounts or isolate devices safely.

B. Keep the Business Running

While your technical team is fighting the fire, you need to keep the business running.

Imagine a manufacturing company hit with ransomware on a Friday morning. All their design files and work orders are encrypted. The business is stuck. But because they had a simple, practiced plan, the team knew what to do.

The floor manager immediately told the operations team to switch to their backup system: paper work orders. They kept production lines moving, just at a slower pace. It was still a huge problem, but not a complete disaster. They could still serve their most important customers because they had a simple, manual workaround ready.

This is what a business continuity plan looks like in the real world.

What's your version of paper work orders? How do you keep taking orders if your main system is down? How do you send invoices? Having these answers ready keeps money coming in during a crisis.

C. Control Communications

Silence is dangerous when under a cyberattack. It creates rumors, fear, and panic. If you don't provide information, employees and customers will make assumptions, usually the worst ones.

You must be the single, trusted source of information.

You don't need all the answers, especially in the early hours. But you need to communicate what you do know, and do it regularly.

Tell your staff and key customers three simple things:

What you know so far (e.g., "We have a system outage affecting our ability to process orders.")

What you're doing about it right now (e.g., "Our technical team is finding the problem, and our operations team is switching to our manual ordering process.")

When you will update them again (e.g., "We will update you in one hour, or sooner if we have major news.")

This shows you are in control, even if the problem isn't solved yet.

To do this effectively, choose one communication channel that isn't dependent on your company's systems.

This could be a private text message group for your leadership team, or a personal email list for all employees. Your company's email or chat system might be down, so you need a reliable way to reach everyone.

Step 3: What to Do After It's Over (Review)

Once the fire is out, systems are restored, and business is back to normal, it's tempting to just sigh with relief and move on. But this is one of the most important parts of the whole process.

You must take time to learn from what happened.

Don’t rush to find someone to blame, though. You need a "no-blame" review to make the business safer, not to punish mistakes. Just gather your small incident response team for a short meeting and ask two simple

questions:

What was the root cause of the problem? Dig past the surface-level answer. Did an employee click a phishing link? Did an attacker get in through an unpatched server? Did someone use a weak, stolen password on a remote login without multi-factor authentication (MFA)? You need to find the actual unlocked door so you can lock it properly.

Ask what one or two changes would have made the biggest difference. Record those actions, their owners and dates, then check they have been completed.

You Must Practice This Plan

A plan that just sits in a binder is useless. The only way to know if your plan works is to test it.

The best way to practice is with a simple, one-hour "tabletop exercise." This is a meeting where you and your small incident response team talk through a fake crisis. It's a fire drill for a cyberattack.

Schedule a one-hour meeting. Get your leader, technical contact, and business contact in a room. Then, present them with a simple, realistic scenario.

"It's 9 AM on a Tuesday. An employee calls and says there's a strange message on their screen demanding Bitcoin payment, and none of their files will open. It looks like we have a ransomware attack. What do we do right now?"

Then, talk it through, step by step. Who calls whom first? What's the first thing the technical person does? How do we tell the rest of the staff what's going on? What's our plan for keeping the business running if the main server is offline?

Talking it through calmly helps you find holes in your plan. You might discover that the contact number for your IT provider is wrong, or that the person making a key decision is on vacation with no backup, or that your plan to switch to paper work orders won't work because the templates are on the encrypted server.

Practising your response can identify gaps before a real incident. A tabletop exercise is a low-cost way to rehearse roles, communications and decisions.

An incident plan that nobody has tested may fail under pressure. Rehearse a realistic scenario and update the plan afterwards.

A short exercise a couple of times a year can help improve confidence, especially for smaller teams.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Publish a one-page incident contact list** Include management, IT, insurer and legal contacts
☐	**Run a tabletop exercise** Test decisions, messages and recovery options
☐	**Practise a real restore** Measure whether the recovery objective is achievable

PART THREE / RESILIENCE AND ASSURANCE

CHAPTER 12

Compliance and governance

Now we're getting in the weeds. Compliance is a boring topic I'm sure you don't want to hear about.

It's overwhelming and often filled with unfamiliar jargon. Which is exactly why this chapter simplifies compliance and governance, turning them into manageable steps.

First, let's clarify what these terms mean. While often used interchangeably, they have distinct roles:

Security is the actual work you do to protect your business. This includes installing modern endpoint protection on laptops, testing backups, and teaching your team to spot phishing emails. It's like the locks on your doors and the cameras in your warehouse.

Compliance is the work you do to prove you're following specific rules. These rules might come from laws (like privacy regulations), industries (like credit card payment rules), or large customers who want to confirm you're a safe business partner. It's the cyber security equivalent of showing the fire inspector your sprinkler system's maintenance records.

Governance refers to who is responsible for security, how decisions are made, and how work is checked. It ensures someone is accountable for security and that you regularly review progress.

You need all three.

Good security without proof makes it hard to land big customers. And compliance paperwork without actual security is a house of cards.

The following pages will help you build a simple, practical system that delivers all three without excessive paperwork.

A Simple, Practical Plan

You don't need a team of compliance experts to achieve this. You just need a practical plan built on a few common-sense habits.

A. Use Your Framework as a Guide

You don't (and shouldn't) have to start from scratch.

Remember Chapter 4, where we discussed security frameworks? That framework is your guide.

It lists the essential steps to protect your business and the things you'll eventually need to prove you're doing.

Whether you use the CIS Controls or the NIST Cybersecurity Framework, the idea is the same: pick one guide and follow it.

You only need one good framework to structure your programme and keep you focused.

B. Name an Owner

While "governance" sounds formal, for a small business, it means naming one person on your team responsible for security. This doesn't have to be a full-time role; in most small businesses, it's a part-time responsibility.

Senior leadership must set expectations and assign responsibility. The technical work can be delegated, but risk decisions and oversight need business accountability.

C. Set a Regular Rhythm

Once you have an owner, set a regular schedule to check in on the security work. A short, 30-minute monthly check-in with the security owner and perhaps your finance or operations lead is enough.

In this meeting, ask these three simple questions:

"What changed in the business this month?" Did you hire new people? Start new software? Sign a new customer? Any business change can create a new security risk, so discuss it.

"Did we have any security issues or near-misses?" Did anyone report a convincing phishing email? Did a security tool send an alert? Discussing near-misses helps you find and fix small problems before they become big ones.

"What are we checking this month?" You can't check everything every month. Pick a few items. For example, this month, review the report showing all laptops are encrypted. Next month, check the log from your last backup restore test.

The "Show Your Work" Habit (Your Documentation)

Documentation often makes business owners groan, but it doesn't have to be a huge, time-consuming project.

You need to get into the habit of "showing your work" as you go. This is what you'll present when a large customer or your insurance company asks for proof of your security.

You only need 3 items:

Policies: These are short pages stating "what we do." For example, a one-page policy might say, "All employees must use multi-factor authentication on their email accounts, and all company laptops must be encrypted." It's a clear statement of your rules.

Procedures: These are step-by-step instructions on "how we do it." For instance, a one-page guide with screenshots could show a new employee how to set up MFA on their phone.

Evidence: This is the most important part: proof that you're doing what you say you do. It's a collection of screenshots, reports, and logs from your security tools. It could be a screenshot from your Microsoft 365 dashboard showing MFA is enabled for all users, a report from your backup system confirming a successful restore test, or notes from your 30-minute monthly meeting.

When you complete a control check, such as a restore test or access review, save dated evidence in a controlled location, for example “2026-11 Backup Test”.

Then, in your monthly meeting notes, add a one-line note saying, "Completed quarterly restore test, report saved in the proofs folder." It takes an extra two minutes, but when an auditor asks you a year from now to prove you did a restore test, you'll have a clean, dated trail of evidence ready.

Handling Audits & Questionnaires

An audit is simply someone checking your work. Whether it's your cyber insurance company, a potential customer, or a regulator, they're asking you to prove you're taking basic, sensible steps to protect your business.

If you've followed the "show your work" habit, this process becomes incredibly simple. When an auditor asks, "Do you have a policy for multi-factor authentication?" you provide the one-page policy you already have.

When they ask, "Can you prove that all of your employees are using it?" you go to your "proofs" folder, grab the screenshot from last month's check, and hand it over.

This shows you're professional, organized, and that your security programme is a real, active part of your business.

The same applies to long security questionnaires from big customers. Your framework is your answer key. The questions they ask will almost always align with the basic controls in your framework.

You can create a simple document with standard answers to common questions, based on your policies. The first time you fill one out might take a while, but subsequent times will be much faster because you've already done the work and saved the answers.

A Quick Note on Privacy

If your business collects any personal data, which almost every business does, even just employee information, you are responsible for protecting it. This issue is growing in importance, and rules are becoming stricter.

You don't need to be a lawyer to grasp the basic principles:

Be clear about why you're collecting data.

Get permission when necessary.

Only keep the data you need for your business.

Securely dispose of data when you no longer have a good business reason to keep it.

A simple privacy notice on your website explaining these points is a good start. However, this is an area where you should consult a lawyer. Specific rules can vary significantly based on where you do business and where your customers are located.

UK organisations handling personal data should consider the UK GDPR and Data Protection Act 2018. International activities may create additional obligations; seek advice on the jurisdictions that apply.

Non-compliance can create regulatory, contractual and reputational consequences. The appropriate response depends on your circumstances and the law.

A short conversation with a knowledgeable lawyer can prevent major problems later.

How to Make This a Manageable, Ongoing Process

To tie all this together and maintain it month after month, use one final tool: a "control register."

This is a spreadsheet listing all your key security controls. It's your master to-do list for your security programme, with columns for:

What is the control? (e.g., "Backup Restore Test")

Who is the owner? (e.g., "Our IT Provider")

How often do we check it? (e.g., "Quarterly")

Where is the proof? (e.g., "The 'Proofs' folder")

Use this list in your 30-minute monthly meeting. The security owner pulls up the list, sees which checks are due that month, and asks the owner for proof.

Don't wait until a customer or regulator asks for proof to start collecting it. That's the biggest mistake you can make. Trying to gather a year's worth of

evidence afterward is a time-consuming, stressful nightmare and looks unprofessional.

You might not even find the proof you need. It's much better to spend a few minutes saving a screenshot each month.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Create a simple control register** Record control, lead, frequency and evidence
☐	**Hold a monthly review** Track gaps, risks and actions
☐	**Check UK GDPR obligations** Document relevant controls and advice received

PART THREE / RESILIENCE AND ASSURANCE

CHAPTER 13

Putting it all together

My goal for this book was to give you a clear, workable path to protect your business without turning you into a security expert.

My hope is that you have found it helpful, and that you now have a better understanding of what cyber security is, and most importantly, what it takes to secure your business against threats (hackers).

As you've seen, most security wins don't come from buying the most expensive complicated tools. They come from doing the basics well, repeatedly.

With that in mind, if you walk away from this book with just a few key ideas, I want them to be these:

Control the Access.

You must be in control of who has the keys to your business. That means you use multi-factor authentication everywhere, no exceptions.

It's the single most effective thing you can do (and you can do it as soon as today).

It means you have a list of all the devices that are used for work, and you make sure they're secure.

And it means you take away admin rights from your employees for their day-to-day work. It's not rocket science, and it's important.

Know Where Your Data Is.

You can't protect your most important information if you don't know where it is. You need to define the specific, "allowed homes" where your sensitive data can be stored, like a specific folder on the server or in your accounting software.

And you need to stop public file sharing by default.

A simple misconfiguration in your cloud storage is one of the most common ways businesses leak huge amounts of data. And that's something you don't want to happen to you.

Have a Plan for When Things Go Wrong.

I don't mean to be pessimistic, but something will eventually go wrong. It's not a matter of if, but when.

What will make the difference between a manageable problem and a disaster is having a plan.

That means you practice restoring your data from your backups, so you know for a fact that it works. It means you run short, one-hour tabletop exercises to rehearse your incident response plan. And it means you keep that plan to a single page, with the names and phone numbers of the people you need to call right at the top (Cyber Insurance Provider, IT Provider, Lawyer, Law Enforcement, etc.).

Separate Your Networks.

Your network shouldn't look like one big open room. You need to put up some simple walls in there.

At a bare minimum, you need to keep your guests on a separate Wi-Fi network from your business. You should also put other less-secure devices, like smart TVs and security cameras, in their own separate zone. This is what prevents a problem on a guest's laptop from spreading to your main server.

Manage Your Vendor Risk.

A problem at your vendor's company can quickly become your problem. You need to sort your vendors by risk and focus your attention on the ones that are critical to your business.

For those high-risk vendors, you need to require them to use unique, named accounts that have an expiration date. And, where possible, you need to use a simple security addendum in your contracts that makes them legally obligated to tell you if they have a security incident.

Get Proof, Don't Just Assume.

You can't just hope that your security is working. You must check. This is the "show your work" habit.

It just means you get into the routine of saving dated reports and screenshots each month as evidence that your controls are working. It's the report that shows all your laptops are encrypted. It's the screenshot that shows all your employees use MFA. And it means you make sure your written policies are short, simple, and match what you do in the real world.

Last but not least... **Security is a habit.**

This is the most important mindset shift you can make. Security isn't a project. A project has a beginning and an end. You don't "finish" security.

It's a habit, a routine, just like doing your bookkeeping, managing your inventory, or locking up the office at night. It's a normal, ongoing part of running a professional business. It's made up of short meetings, small, regular adjustments, and a simple habit of keeping records.

When you treat security like that, it stops being this big, scary, overwhelming thing. It just becomes a series of small, manageable tasks. You check your backups. You review who has access. You make sure your software is up to date. I say "you," but that can (and should) be handled by your IT Provider/MSP.

The real value of this routine shows when something eventually does go wrong.

Because you have a plan and you've practiced it, your team can respond with a clear order of steps instead of panicking.

A rehearsed plan means your team has a clearer order of actions, knows whom to contact and has a better chance of protecting essential services when something goes wrong.

One Last Thing Before You Go

If you've made it this far, nicely done.

Most business owners never take the time to really think through cyber security and the steps needed to implement it properly. You've invested the time, and now you have a clear picture of the necessary steps to secure your business against modern threats.

As a thank you for reading, CyberKarl offers an opportunity to discuss the most useful next steps for your organisation.

Sometimes a short conversation helps turn general guidance into a sensible plan for your particular business.

A discussion can focus on the questions most important to you:

Prioritise the next one or two high-impact security habits for your business.

Figure out the single biggest **low-hanging fruit** security weakness you need to fix right away.

Get clear answers on any topics from this book that might still be confusing.

To start a conversation, contact CyberKarl:

Email: hello@cyberkarl.com

Website: https://cyberkarl.com

Thank you for reading, and I wish you all the best in securing your business!

Regards,

CyberKarl Ltd
Helping you defend what matters.

PUT IT INTO PRACTICE

Choose a priority, agree who will do it and keep evidence that it has happened.

☐	**Choose three priorities for the next 30 days** Assign ownership and due dates
☐	**Retain proof of progress** Use actual reports, records and test outputs
☐	**Plan the next review** Make security a repeated business habit

PART THREE / RESILIENCE AND ASSURANCE

CHAPTER 14

Cyber security jargon decoder

Welcome to the cyber security jargon decoder!

I put this final chapter together to help you make sense of some of the most important and commonly used terms in the industry. It'll come in handy as you implement what you learned in this book and when dealing with IT providers, insurance companies, and vendors.

The A-to-Z Decoder: 30 Terms Every Business Owner Should Know

Authentication — The process of proving you are who you say you are, usually with a password or code.

Botnet — A network of infected computers controlled by a criminal to launch large-scale attacks like sending spam or knocking websites offline.

Business Email Compromise (BEC) — A scam where a criminal impersonates a trusted person via email to trick an employee into sending money or sensitive information.

Cloud Computing — Using someone else's computers and storage over the internet instead of owning and managing your own.

Compliance — The work you do to prove you are following a specific set of security or privacy rules required by laws, industries, or customers.

Cyber Insurance — An insurance policy designed to help your business cover the costs of recovering from a cyberattack.

DDoS (Distributed Denial-of-Service) Attack — An attack that knocks a website offline by flooding it with so much junk traffic that it can't respond to legitimate customers.

Encryption — The process of scrambling your data so it's unreadable to anyone without the correct "key" to unscramble it.

Endpoint Detection and Response (EDR) — A modern version of antivirus that actively watches for suspicious behaviour on your computers, not just known viruses.

Firewall — A digital security guard that stands between your internal business network and the public internet, controlling what traffic is allowed in and out.

Incident Response — The plan and actions you take to manage the aftermath of a security breach or cyberattack.

IP Address — A unique address for a device on the internet, similar to a street address for a house.

Malware — A general term for any software, like viruses, spyware, or ransomware, designed to harm or disrupt a computer system.

Managed Service Provider (MSP) — An IT company that you hire to manage your technology and cyber security on an ongoing basis.

Multi-Factor Authentication (MFA) — A security process that requires more than one method of proving your identity to log in, like a password plus a code from your phone.

Network Segmentation — Dividing your company's computer network into smaller, isolated zones to prevent an attack from spreading.

Patch Management — The process of regularly updating your software and systems to fix security holes before criminals can exploit them.

Penetration Testing — Hiring a team of ethical hackers to try to break into your systems to find security weaknesses before real criminals do.

Phishing — A deceptive email, text, or message designed to trick you into revealing sensitive information or clicking a malicious link.

Ransomware — Malicious software that locks up all your files and demands a payment (a ransom) to get them back.

Remote Desktop Protocol (RDP) — A built-in Windows tool that allows you to control a computer remotely over a network connection.

Risk — The potential for loss or damage when a threat exploits a vulnerability in your business.

Server — A powerful computer that provides data or services to other computers (called clients) on a network.

Social Engineering — The art of manipulating people into giving up confidential information or performing an action they shouldn't.

Threat Actor — Any person or group who has the intent and capability to launch a cyberattack, from individual hackers to organized criminal groups.

Two-Factor Authentication (2FA) — A security process that requires exactly two methods of proving your identity to log in, such as a password and a text message code.

VPN (Virtual Private Network) — A tool that creates a secure, encrypted connection over a public network like the internet, often used for remote work.

Vulnerability — A weakness or flaw in software, hardware, or a process that could be exploited by an attacker.

Zero-Day Exploit — An attack that takes advantage of a security vulnerability on the same day it becomes known to the public, before a patch is available.

Zero Trust — A modern security model built on the principle of "never trust, always verify," which requires continuous authentication for all users and devices.

MODERN BUSINESS RISKS

CHAPTER 15

Using AI safely at work

Generative AI can help businesses draft documents, analyse information and support customer service. It also changes how information is shared, how decisions are made and which systems have authority to act. A useful tool can become a business risk when nobody has agreed what it may see or do.

Start with visibility

Find out which AI tools employees already use. Include chatbots, note-taking tools, built-in AI features in business software and agents that connect to company systems. You cannot manage the risks of tools you do not know about.

Keep a simple register that records the tool, the intended purpose, who owns it, what information is used, who can access it and whether it takes actions automatically. For a smaller business, a short spreadsheet can be enough to begin.

Decide which information must not be shared

Your existing information-handling rules still apply when an employee uses AI. Customer records, personal data, financial details, passwords, commercial plans and confidential contracts should not be pasted into a tool without an approved purpose and appropriate safeguards.

Check the supplier agreement and settings. Understand whether prompts, uploaded files and outputs are stored, who can access them, whether they may be used for training, and how long they are retained. Settings and contractual terms may vary by product and subscription.

Treat AI output as a proposal, not proof

AI-generated text can be convincing and still be inaccurate. For significant business decisions, verify facts against trusted sources and make an accountable person responsible for approval. Record where AI contributes to decisions involving customers, safety, legal matters or regulated processes.

A useful rule is simple: the more serious the consequence of a mistake, the stronger the checking and approval required.

Give connected AI agents the minimum access

An AI assistant that merely drafts text creates a different risk from an agent that can send emails, edit customer records, create purchase orders or change settings. Do not give an agent broad administrator permissions because that is easier to configure.

Limit each agent to the information and operations needed for its defined task. Use separate identities, time-limited permissions where possible, meaningful logs and human approval before consequential actions. Revoke access when the agent is retired or its purpose changes.

Think about how an attacker might manipulate the agent through messages, documents or websites it reads. The NCSC advises organisations to consider limitations, dependencies, monitoring and failure arrangements when adopting agentic AI. [S8]

Make AI part of normal governance

Assign a lead for AI use and have a clear method for approving new tools. Review privacy and security risks, record decisions, train users and include AI-related incidents in the business response plan. If an AI system handles personal data, UK GDPR obligations still apply. [S5]

A simple AI approval checklist

Purpose: What business problem will this solve, and who is accountable?

Data: What information will the tool see, store or disclose?

Access: Which users and systems can it reach, and what actions may it take?

Assurance: How will you check accuracy, safety and compliance?

Monitoring: How would you detect misuse and stop the tool quickly?

Retirement: How will access, data and credentials be removed when it is no longer needed?

Begin with low-risk uses. Put proportionate controls in place before connecting AI to important business systems, and review the results after each pilot.

QUICK-START PLAN

CHAPTER 16

Your first 30 days

A book is only useful when it changes what happens at work. This four-week plan turns the advice into a manageable sequence of actions. Adjust it to the size and risk profile of your organisation.

WEEK 1 / Know what you rely on

Name your essential services, identify the devices, cloud tools and data they depend on, and agree who leads cyber security.

Evidence to keep: A one-page critical-service list and a named lead.

WEEK 2 / Secure access

Check MFA coverage, remove access for people who have left and review administrator privileges.

Evidence to keep: A dated access review and MFA enforcement report.

WEEK 3 / Protect and recover

Confirm which systems are patched and protected, check backup coverage and complete a real restore test.

Evidence to keep: An update report, backup status and restore-test record.

WEEK 4 / Practise and improve

Confirm incident contacts, rehearse one scenario and record the highest-priority gaps, dates and responsible people.

Evidence to keep: A one-page incident plan, exercise notes and an action log.

The aim is not to solve every security problem in 30 days. It is to establish ownership, reduce obvious exposure and create a repeatable cycle of checking and improving.

OFFICIAL GUIDANCE

CHAPTER 17

Sources and further reading

This edition uses official UK and framework publisher information for the updated references below. Survey figures refer to organisations that identified breaches or attacks; they are not predictions of risk for any individual business.

[S1] UK Government, Cyber Security Breaches Survey 2025/2026

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026

[S2] National Cyber Security Centre, Cyber Essentials overview

https://www.ncsc.gov.uk/cyberessentials/overview

[S3] Center for Internet Security, CIS Critical Security Controls v8.1

https://www.cisecurity.org/controls/v8-1

[S4] Center for Internet Security, Implementation Groups / IG1

https://www.cisecurity.org/controls/implementation-groups

[S5] Information Commissioner's Office, A guide to data security

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

[S6] NCSC Small Business Guide

https://www.ncsc.gov.uk/collection/small-business-guide

[S7] ISO/IEC 27001:2022 information security management systems

https://www.iso.org/standard/27001

[S8] National Cyber Security Centre, Thinking carefully before adopting agentic AI

https://www.ncsc.gov.uk/sites/default/files/2026-06/Thinking-carefully-before-adopting-agentic-AI.pdf

Official source pages and certification requirements should be checked again before acting on a specific compliance or certification decision. Sources accessed November 2026.

ABOUT THE PUBLISHER

CHAPTER 18

CyberKarl Ltd

Helping you defend what matters.

CyberKarl helps UK organisations manage cyber risk, protect sensitive information, govern the use of AI and show customers and partners that their security responsibilities are taken seriously.

Cyber Security & Governance: Security strategy, practical controls and assurance, including Cyber Essentials and ISO 27001.

Privacy & Data Protection: Protecting personal information and supporting UK data protection responsibilities.

AI Security & Governance: Managing the opportunities and risks of AI through appropriate governance and safeguards.

vCISO & Assurance: Experienced cyber security leadership and board-level guidance without a full-time appointment.

Whether you are starting from scratch or improving an existing programme, we focus on clear priorities, proportionate action and evidence that controls work.

Start a conversation

Tell us what your organisation depends on and what you are most concerned about. We can help you decide where to start, what to improve and how to demonstrate progress.

hello@cyberkarl.com

https://cyberkarl.com

CyberKarl®

Helping You Defend What Matters

BE BETTER PREPARED. KEEP YOUR BUSINESS MOVING.

Cyber security is not just about technology. It is about protecting livelihoods, maintaining services and giving customers the confidence to trust your business.

This practical guide explains the everyday risks facing UK organisations and the actions that can make a real difference.

HELPING YOU DEFEND WHAT MATTERS.

hello@cyberkarl.com