The Small Business Cybersecurity Survival Guide

BY JANE FRANKLAND MBE

Contents

Introduction: Why I've created this guide

Part 1: Understanding the threats

- **Q1** Isn't my business too small to be targeted by cybercriminals?
- **Q2** How quickly can cybercriminals move?
- **Q3** How is AI changing cyber risk for small businesses?
- **Q4** Should we share passwords, save them in browsers or use facial recognition?
- **Q5** Should I connect ChatGPT or another AI assistant to my business email?
- **Q6** How can we protect ourselves against fake invoices, cloned voices and payment fraud?

Part 2: Technology, suppliers and resilience

- **Q7** If our IT provider says we're protected, isn't that enough?
- **Q8** Is older technology dangerous if it still works?
- **Q9** What about routers, printers, laptops and other devices connected to my network? Are they a cybersecurity risk?
- **Q10** How do we know our backups will actually work?
- **Q11** What happens if our main supplier or cloud service goes down?

Part 3: Responding when something goes wrong

- **Q12** What should I do in the first hour of a cyberattack?
- **Q13** How should we communicate with customers after a cyber incident?
- **Q14** Doesn't cyber insurance mean we're covered?

Part 4: Getting started

- **Q15** Where should an overwhelmed business owner start tomorrow morning?
- **Q16** I'm a micro-business with fewer than ten employees. What cybersecurity protection do I really need, and where can I get help?
- **Q17** What's the single most useful thing I can do in the next 30 days?

Small Business Cybersecurity Checklist

First-Hour Incident Response Checklist

Final thought: Are you protected, or are you prepared?

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Introduction: Why I've created this guide

During Cybersecurity Awareness Month, I joined the LinkedIn UK Editorial team for a 30-minute LinkedIn Live conversation about the cybersecurity challenges facing Britain's small businesses.

We discussed everything from recent attacks on UK retailers to AI-powered scams, ransomware, compromised suppliers, passwords and what business owners should do when something goes wrong.



One thing became clear: small business owners need practical, understandable advice, not another complicated technical framework or a long list of products to buy. They need to know what matters, what to prioritise and how to keep operating when something goes wrong.

And the evidence shows why this matters.

According to the UK government's Cyber Security Breaches Survey 2025/26, 43% of businesses identified a cybersecurity breach or attack during the previous 12 months, including 42% of micro-businesses and 46% of small businesses. Yet only around one in four businesses had a formal incident response plan.

Meanwhile, the government's Business Population Estimates 2025 show that SMEs represent almost 99.9% of the UK's private-sector business population. They employ approximately 16.9 million people and generate around £2.8 trillion in annual turnover.

They're the backbone of our economy. And when they suffer serious disruption, the consequences extend to employees, customers, suppliers and communities.

I've spent almost 30 years working in cybersecurity, from founding one of the UK's early penetration-testing companies to leading cybersecurity services at Accenture and advising organisations on resilience and survivability. But I'm also a micro-business owner myself, and I know from personal experience that accessing the right cybersecurity support isn't always straightforward when you're a very small company.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

You may not have an IT department, a cybersecurity team or the budget to retain specialist advisers. Yet you're expected to manage many of the same threats that larger organisations face.

That's one of the reasons I wanted to create this resource.

One of the most important lessons I've learned throughout my career is that having cybersecurity controls doesn't necessarily mean your business can survive a cyber incident.

This guide expands on our LinkedIn Live discussion with research, practical advice, real-world examples and free resources.

Rest assured, you don't need to become a cybersecurity expert, but you do need to know what matters, who you're depending on and what you'll do when something goes wrong.

> And if you're running a business with fewer than ten people? Jump to Q16 for a practical starting point.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

PART 1

Understanding the threats

Q1. Isn't my business too small to be targeted by cybercriminals?

No. This is one of the most dangerous misconceptions about cybersecurity. Cybercriminals don't necessarily choose targets because they're famous or wealthy. Many attacks exploit volume and, because they're automated, they're looking for vulnerable systems, exposed accounts and weak passwords.

The government's Cyber Security Breaches Survey 2025/26 found:

43%	of businesses identified a cyber breach or attack.
42% and 46%	of micro-businesses and small businesses respectively identified one.
65% and 69%	of medium-sized and large businesses respectively identified one.
Phishing	remained the most commonly identified attack type.

These are identified and self-reported incidents. They don't include attacks businesses failed to detect, and identifying a phishing attempt isn't the same as suffering a successful compromise.

What can we learn from recent incidents?

- **ASOS, October 2026:** Reporting described an incident involving social engineering, compromised access and attacker-controlled customer-facing notifications. ASOS confirmed that certain customer information was affected.
- **TFG London, October 2026:** The group behind Hobbs, Whistles and Phase Eight reported a cyber incident affecting some systems. Its stores continued trading while continuity arrangements were activated.
- **Jaguar Land Rover, September 2025:** A major cyber incident halted production and affected the wider supply chain. The Cyber Monitoring Centre estimated a £1.9 billion impact on the UK economy, with approximately 5,000 organisations affected.

These incidents illustrate three different risks: compromised identities, operational disruption and supplier dependency.

For small businesses, the consequences can be severe. A company relying entirely on one website, payment platform or social media account may struggle to trade if that service disappears.

> **What you should do:** Identify your essential business services and ask what would happen if they became unavailable for a day, a week or longer.

> ***The question isn't whether you're too small to be attacked. It's whether your business could survive an attack.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Q2. How quickly can cybercriminals move?

Much faster than most businesses realise. Attackers increasingly use automation to identify weaknesses and exploit opportunities before organisations can respond. Unit 42 research described malicious scanning beginning within approximately 15 minutes of vulnerability disclosure.

Separately, research highlighted by the Cloud Security Alliance in April 2026 demonstrated that AI-assisted systems could produce working proof-of-concept exploits for certain published vulnerabilities in approximately 10–15 minutes, at a reported experimental cost of around $1.

That does not mean every vulnerability can be exploited for $1, or that every attack takes 15 minutes. The finding demonstrates how automation can compress parts of the exploit-development process under specific research conditions.

How fast do attackers move once they're inside?

CrowdStrike's February 2026 Global Threat Report reported:

29 minutes	Average observed eCrime breakout time.
27 seconds	Fastest observed breakout time.
89%	Reported increase in AI-enabled adversary activity.

Breakout time measures how quickly an attacker moves from an initial foothold to another system. It is not the time needed to complete an entire attack.

Sophos's 2026 Active Adversary Report found:

3.4 hours	Median time for attackers to reach Active Directory in the investigated cases.
88.1%	Share of observed ransomware deployments occurring outside normal business hours.
78.85%	Share of observed data exfiltration occurring outside normal business hours.

These findings come from the vendors' respective datasets, not a census of every cyberattack.

Why does this matter for small businesses?

You may not have someone monitoring your systems at 2am. Your IT provider may only offer support during office hours. By the time someone notices suspicious activity, an attacker may already have compromised additional accounts or systems.

> **What you should do:** Apply security updates promptly, use phishing-resistant authentication, restrict administrator access and ask your IT provider what happens outside working hours.

> ***You can't rely on spotting an attack quickly enough. You need to prepare before it happens.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Q3. How is AI changing cyber risk for small businesses?

AI is changing both how criminals attack and how businesses can accidentally expose themselves. I think about three sources of harm:

- **Malice:** Criminals deliberately targeting your organisation.
- **Mistake:** Employees or business owners making errors, including sharing sensitive information with inappropriate AI tools.
- **Malfunction:** Technology behaving unexpectedly, including automated systems making repeated mistakes.

AI can increase the speed and impact of all three.

AI-powered impersonation and fraud

Criminals can create convincing phishing messages, cloned voices and fabricated video calls.

In 2024, engineering firm Arup confirmed that an employee in Hong Kong had been deceived into transferring approximately HK$200 million, around £20 million, following a fraudulent video conference involving deepfake impersonation, as reported by the Financial Times.

The lesson isn't that everyone must learn to recognise a deepfake. It's that financial controls must work even when a fake looks or sounds convincing.

What about employees using AI?

The NCSC has highlighted the risks of shadow AI, including employees using unapproved tools without their organisation understanding the security implications.

The government's Cyber Security Breaches Survey 2025/26 also found that only 24% of businesses using AI had practices to manage associated risks.

That creates a visibility problem.

Employees may upload confidential customer information, contracts or commercially sensitive data into tools that haven't been assessed. Others may rely on incorrect AI-generated answers.

> **What you should do:** Find out which AI tools employees actually use. Provide approved alternatives, explain what information must not be uploaded and require human checking for important outputs.

Q4. Should we share passwords, save them in browsers or use facial recognition?

Passwords remain one of the most common ways criminals gain access to business accounts. But the advice has evolved considerably.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Should employees share passwords?

Generally, no. Use individual accounts wherever possible. If multiple people need access, use delegated permissions or a business password manager with secure sharing. Avoid distributing credentials through ordinary email, WhatsApp or spreadsheets.

Are password managers a good idea?

Yes. A reputable password manager helps people create and store long, unique passwords. Choose one with strong authentication, controlled sharing and appropriate recovery arrangements.

Is it safe to write passwords down?

It can be. For someone who would otherwise reuse a weak password, writing a long, unique password on paper and keeping it securely at home can be a reasonable approach. But don't leave it on your desk, attach it to your computer or carry it with the device it unlocks! For businesses, a managed password vault is usually preferable.

Is it safe to save passwords in my web browser?

Most browsers, including Chrome, Edge, Safari and Firefox, offer to remember passwords. That's convenient, and using a browser password manager to create and store strong, unique passwords is generally safer than reusing weak passwords or keeping them in an unprotected document. But there are risks worth understanding.

Someone who gains access to your device may also gain access to your accounts.

If your laptop is stolen while unlocked, or someone gains access to your computer account, they may be able to use websites where you're already signed in. Depending on your browser and device security, they may also be able to access stored credentials.

Malware can steal information from browsers.

Some malicious software, known as infostealers, is designed to steal saved passwords, authentication cookies and session tokens. These tokens matter because they may allow criminals to hijack an existing session without knowing your password or completing a new MFA challenge.

This is one reason why MFA, while essential, isn't a complete defence against account compromise.

Password synchronisation creates another dependency.

If your browser synchronises passwords between your laptop, phone and other devices, those credentials may be accessible through your browser or cloud account. Protect that account with strong authentication, preferably a passkey or security key, and review which devices are signed in.

Shared computers and browser profiles create additional risks.

If employees use the same computer account or browser profile, they may gain access to each other's saved credentials or signed-in sessions. Every employee should have their own device account and browser profile, with appropriate permissions.

Is a dedicated password manager better?

For a business, I'd generally recommend a reputable business password manager. It can provide additional capabilities that are particularly useful when several people need access to business

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

systems, including secure credential sharing, centralised access controls, audit logs and removing access when someone leaves.

However, a dedicated password manager isn't automatically immune to malware or account compromise. It still needs strong authentication, secure devices and appropriate configuration.

For a sole trader or micro-business owner, a well-protected browser password manager may be a perfectly reasonable starting point.

> **My advice:** Don't stop saving passwords in your browser only to start reusing simple passwords. That would be a step backwards. The objective is to use strong, unique credentials and protect the devices and accounts that store them.

What about passkeys?

The NCSC has published guidance on passkeys, recommending their use wherever supported. Passkeys and FIDO2 security keys are phishing-resistant. Traditional one-time codes can still be intercepted or phished.

Prioritise your email, banking, accounting, cloud administration and password manager accounts. Where stronger options aren't available, use an authenticator app or SMS verification rather than leaving accounts protected by passwords alone.

Should I use facial recognition or fingerprint authentication on my phone?

Yes. If your phone supports secure facial recognition or fingerprint authentication, I'd recommend enabling it.

Think about how much of your business you now manage through your smartphone: email, banking, payments, accounting, customer records, social media and cloud services. For many micro-business owners, their phone is effectively their office. If someone gains access to an unlocked phone, they may be able to access much of the business.

Modern biometric authentication, such as Apple's Face ID or secure fingerprint recognition on Android devices, can provide a convenient additional layer of protection, but not all facial recognition systems are equally secure. Some use dedicated hardware and stronger anti-spoofing protections, while others rely mainly on the phone's camera.

Five things I'd recommend

1. **Enable secure facial recognition or fingerprint authentication.** Choose the strongest biometric option your phone supports and use it to protect sensitive apps where available.
2. **Use a strong device passcode.** Biometrics are backed by a PIN or password, so avoid easily guessed codes such as 123456, birthdays or repeating numbers. A longer PIN or alphanumeric passcode provides stronger protection.
3. **Keep your phone updated.** Enable automatic operating system and app updates. Older phones that no longer receive security updates should be replaced or managed appropriately.
4. **Enable remote location and erasure features.** Apple's Find My and Google's device-finding services can help locate, lock or erase a lost phone. Make sure these features are configured before you need them.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

5. **Protect what appears on your lock screen.** Consider hiding the content of sensitive messages and authentication codes until the phone is unlocked. It's also worth checking which applications can access your microphone, camera, contacts, photos and location, and removing permissions they don't need.

What happens if I lose my phone?

This is something many business owners overlook. If your phone contains your passwords, passkeys and authentication app, losing it could leave you unable to access email, banking or other essential services.

Set up secure recovery methods in advance, such as a second trusted authenticator or backup security key. Keep recovery codes somewhere safe and separate from the phone. And remember that biometric authentication doesn't prevent every threat. If you unlock your phone and then fall for a phishing attack, approve a fraudulent payment or install a malicious app, facial recognition won't necessarily protect you.

> **My advice:** Treat your smartphone as a business computer, because that's exactly what it has become. Protect it with the same care as your laptop, and make sure you can regain access to critical business accounts if it's lost, stolen or damaged.

The NCSC's password guidance provides additional advice on managing credentials securely.

> ***Protecting your password doesn't necessarily protect an already authenticated session. And protecting your device is only half the job; you must also be able to recover access when something goes wrong.***

Q5. Should I connect ChatGPT or another AI assistant to my business email?

Proceed cautiously.

There's a significant difference between asking an AI assistant to draft an email and giving it access to your entire mailbox, customer records and business systems. Depending on the product and permissions, an AI assistant may be able to read confidential information, modify records or send messages.

What is prompt injection?

Imagine an attacker sends an email containing malicious instructions intended for an AI assistant. The assistant should treat the email as information to process, not as instructions to obey, but the attacker may attempt to manipulate it into searching for confidential records or forwarding information elsewhere.

This is called prompt injection. The NCSC has explained why prompt injection is a distinct security challenge.

Whether such an attack succeeds depends on the system's design and safeguards, but it demonstrates why broad permissions can be dangerous.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Before connecting an AI assistant, ask:

- What information does it genuinely need?
- Can access be limited to particular tasks or records?
- Can it send, delete or forward information?
- Does a human approve consequential actions?
- Are actions logged?
- Can access be revoked immediately?
- What happens if the AI is manipulated, makes a mistake or malfunctions?

Start with low-risk tasks, such as drafting content for human review. Avoid autonomously delegating payment transfers, changes to bank details, confidential disclosures or access approvals. Use an appropriately governed business AI service rather than connecting personal AI accounts to corporate systems without approval.

The NCSC also provides guidance on thinking carefully before adopting agentic AI.

> ***Protecting the login is only the beginning. You must also control what people, applications and AI agents can do once they're inside.***

Q6. How can we protect ourselves against fake invoices, cloned voices and payment fraud?

Don't depend on recognising a convincing fake. Build verification into your processes. According to UK Finance's 2026 Annual Fraud Report, approximately £1.28 billion was lost to fraud during 2025, including £576.4 million in authorised push payment fraud.

The government's Cyber Security Breaches Survey 2025/26 also estimated that around 43,000 businesses experienced fraud originating from a cyber breach.

Five practical rules

1. Never change supplier bank details solely because of an email.
2. Call the supplier using a number already held in your records.
3. Require two people to authorise significant or unusual payments.
4. Treat urgency, secrecy and pressure as warning signs.
5. Make it safe for employees to question instructions, even those apparently coming from senior leaders.

If someone claims to be calling from your bank, hang up and call the bank using a verified number. In the UK, dialling 159 connects callers to participating banks' fraud teams.

Eligible consumers, micro-enterprises and small charities may qualify for reimbursement of certain authorised push payment scams, subject to the applicable rules and limits. Do not assume every fraud loss is covered.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Protect your business email domain

Ask your IT provider about SPF, DKIM and DMARC, which help prevent certain forms of email impersonation. You can check your domain using the free NCSC Email Security Check and find additional guidance in the Global Cyber Alliance Small Business Toolkit.

> ***A legitimate payment can survive a five-minute verification check.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

PART 2

Technology, suppliers and resilience

Q7. If our IT provider says we're protected, isn't that enough?

No. Ask for evidence. Your IT provider may manage your computers, email, backups and cloud services, but you still need to understand what you're paying for and whether it works.

Verizon's 2026 Data Breach Investigations Report identifies third-party involvement as a major feature of the breaches in its dataset.

The government's Cyber Security Breaches Survey 2025/26 found that only 15% of businesses reviewed the cybersecurity risks associated with their immediate suppliers.

Ask your provider:

- Who has administrator access to our systems?
- Is MFA enforced on critical accounts?
- Are important security updates being installed?
- When were our backups last successfully restored?
- How quickly would you detect and respond to an incident?
- Is out-of-hours response included?
- What happens if your own business is compromised?
- Could we continue operating without your services?

Request a simple monthly report covering access, patching, backups, incidents and outstanding risks.

> ***Don't ask whether you have backups. Ask when they were last successfully restored.***

Q8. Is older technology dangerous if it still works?

Potentially, especially when it's unsupported, internet-connected or remotely accessible.

In October 2026, French authorities reported disruption involving remotely managed refrigeration equipment across approximately 700 supermarkets. Reports described significant temperature manipulation, spoiled stock and equipment damage. Manufacturers indicated that many affected units were older devices without ongoing security updates. The exact initial access route had not been confirmed when this guide was prepared.

The lesson is relevant to businesses using older tills, routers, CCTV equipment, building controls or specialist machinery. Working and secure are not the same thing.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

What should you do?

Maintain a list of your equipment and identify which devices no longer receive security updates. Prioritise systems accessible from the internet or by external suppliers. Apply security updates promptly and restrict unnecessary remote access.

The government's Cyber Essentials scheme requires relevant high-risk and critical updates to be installed within 14 days.

Windows 10 reached the end of standard support in October 2025. Businesses still using it should check whether they have appropriate extended security coverage or need to migrate.

The NCSC Small Business Guide provides further advice on protecting business devices and systems.

Q9. What about routers, printers, laptops and other devices connected to my network? Are they a cybersecurity risk?

Yes, and they're often overlooked.

When business owners think about cybersecurity, they usually think about laptops, passwords and antivirus software, but almost everything connected to your network can introduce risk. That includes broadband routers, Wi-Fi access points, printers, scanners, CCTV cameras, smart televisions, tills, card terminals and building controls.

Some of these devices have their own operating systems, administrator accounts, remote access features and security vulnerabilities, and many are installed once and then forgotten.

Why does the router matter?

Your broadband router connects your business network to the internet. If it's poorly configured, vulnerable or compromised, an attacker may be able to interfere with network traffic, change DNS settings, access exposed management services or use it as a foothold for further attacks.

So check:

- Is the router still supported by its manufacturer or provider?
- Does it receive security updates automatically?
- Has the default administrator password been changed, where applicable?
- Is remote administration disabled unless necessary?
- Is Wi-Fi protected with WPA3 or WPA2-AES?
- Is there a separate guest network for visitors?
- Are unnecessary services such as UPnP disabled where practical?

If you're unsure, ask your broadband provider to explain the settings and whether they manage updates.

What about printers?

Modern printers are computers in their own right. Many store documents temporarily, connect to cloud services, have administrator interfaces and support remote management. An insecure printer could expose sensitive documents or provide another route into your network.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Check that your printer receives firmware updates, uses a strong administrator password and isn't unnecessarily accessible from the internet. Disable features you don't need, such as unused network protocols or remote printing services. Where practical, restrict which devices can access it.

Are newer laptops and routers more secure?

Often, yes, although age alone doesn't determine security.

Modern laptops may include hardware-backed security features such as TPM chips, Secure Boot, device encryption and biometric authentication. These can make it harder for criminals to steal information or tamper with a device. Modern operating systems also provide built-in security protections, including firewalls, malware protection and automatic updates.

Newer routers may support WPA3 encryption, automatic firmware updates, improved isolation between networks and built-in threat-blocking features, but the important questions are whether those protections exist, are enabled and are maintained.

Buying newer technology doesn't automatically make you secure. But supported devices with modern security features can significantly improve your starting position.

Should I use the security services offered by my broadband or telecoms provider?

They're worth investigating. Some UK business broadband and telecoms providers offer additional security services, including malicious website blocking, network-level threat protection, managed routers, secure Wi-Fi and technical support.

For a micro-business without dedicated IT staff, these services may provide a useful extra layer of protection, but don't assume every package includes them or that they're automatically enabled.

Ask:

- What security protections are included?
- Are they enabled by default?
- Does the provider update and manage the router?
- Can the service block known malicious websites or threats?
- Will I receive alerts if something suspicious is detected?
- Is help available outside normal business hours?
- What protection do I still need on my laptops, phones and cloud accounts?

Network-level protection can complement endpoint security, but it doesn't replace MFA, software updates, backups or safe business processes.

Should everything be connected to the same network?

Ideally, no.

If your business has customer Wi-Fi, CCTV, smart equipment, printers and office computers, consider separating devices according to their purpose and risk. For example, customers shouldn't be able to access the same network resources as your accounting computer or business server.

Some modern business routers and managed Wi-Fi systems make this easier through guest networks and network segmentation.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

If you're unsure how to configure this, ask a competent provider rather than experimenting with settings that could interrupt your business.

A quick check you can do today

Look around your business and identify everything connected to your network. You may discover devices you've forgotten about.

For each one, ask:

- Do we still need it?
- Is it supported?
- Does it receive updates?
- Who can access it?
- Does it need internet access?
- What would happen if it were compromised or stopped working?

The NCSC Cyber Action Toolkit and Cyber Essentials guidance provide useful starting points for securing business equipment.

> ***You can't protect what you don't know is connected.***

Q10. How do we know our backups will actually work?

A backup is only useful if you can restore from it. Ransomware attackers may try to compromise backup systems before encrypting production data.

A useful starting point is the 3-2-1 approach:

3	Keep three copies of important data.
2	Use two different storage types or systems.
1	Keep one copy offline or otherwise protected from modification or deletion.

Immutable backups can provide additional protection by preventing changes or deletion for a defined period. But the most important question is whether you've tested recovery. Ask your provider to demonstrate a successful restoration and explain how long recovering critical services would take. Remember that backing up files isn't always the same as being able to restore a working business application.

The NCSC Small Business Guide explains the importance of maintaining and testing backups.

> ***A backup you've never restored from is an assumption, not a recovery plan.***

Q11. What happens if our main supplier or cloud service goes down?

You can suffer serious disruption without being directly attacked. The Jaguar Land Rover incident demonstrated the potential impact of disruption spreading through a supply chain.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Cloud outages can have similar consequences even when no malicious activity is involved. This is why every business should understand its dependencies.

Create your minimum viable business

Identify the essential services you need to keep operating. Think in terms of recovery priorities:

Minutes	Protect people, stop fraudulent transactions, establish decision-making and contain the incident.
Hours	Restore essential communications, customer contact and priority operations.
Days	Recover payments, orders, essential records and core services.
Weeks	Address backlogs, restore less critical systems and rebuild normal operating capacity.

Then consider the additional workload created by disruption. Can your employees manage manual processes? How will customers contact you? What happens if recovery takes twice as long as expected?

> ***Restoring technology is not necessarily the same as restoring business operations.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

PART 3

Responding when something goes wrong

Q12. What should I do in the first hour of a cyberattack?

The first hour is about containment, coordination and preserving your options.

First-hour action checklist

1. **Contact your IT or cybersecurity provider.** Establish who is leading the response.
2. **Isolate affected devices.** If a computer appears infected, disconnect its network cable and disable Wi-Fi. Don't wipe or reset it. Where safe, keep it powered on pending incident-response advice because valuable evidence may be lost if it's switched off.
3. **Secure affected accounts.** Ask your provider to revoke suspicious sessions, disable compromised access and investigate malicious forwarding rules.
4. **Contact your bank immediately if money is involved.**
5. **Inform employees.** Explain what they should do and how to communicate safely if email may be compromised.
6. **Contact your cyber insurer.** Follow its notification requirements.
7. **Preserve evidence.** Record what happened, when it was discovered and the actions taken.
8. **Assess reporting requirements.** Certain personal data breaches must be reported to the ICO within 72 hours of becoming aware of them. The Information Commissioner's Office provides guidance on reporting obligations.

Don't automatically unplug every device or switch off the entire network. Wider containment should follow specialist advice and the circumstances of the incident. If you've experienced fraud, contact your bank and report it through Report Fraud. You can also report a cybersecurity incident to the NCSC.

> ***Don't wait until you know exactly what happened before getting help.***

Q13. How should we communicate with customers after a cyber incident?

Communication is part of your response. Attackers may contact customers, suppliers or journalists directly to increase pressure on a victim.

The October 2026 ASOS incident and the 2025 Kido nursery attack illustrate why organisations cannot assume they will control when affected individuals first hear about an incident.

Tell people three things

1. **What you know**, without speculation.
2. **What it means for them** and whether they need to act.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

3. **What you're doing** and when they'll receive another update.

Avoid minimising an incident before the facts are known. Warn customers about follow-on phishing or impersonation attempts. Have an alternative communication channel ready if your email, website or social media account is compromised. Prepare a short holding statement in advance.

> ***Trust isn't determined only by whether something goes wrong. It's also shaped by how you respond.***

Q14. Doesn't cyber insurance mean we're covered?

Cyber insurance can help with response costs, investigations, legal advice and certain financial losses, but it doesn't prevent an attack or guarantee recovery. Policies may contain exclusions, limits, excesses and security requirements. Some forms of invoice fraud and social engineering may have restricted coverage.

Check what you declared when purchasing your policy, what controls must remain in place and which response providers you must contact.

The NCSC's Cyber Insurance Guidance explains the questions businesses should ask before purchasing cover.

> ***Insurance is a financial backstop, not a cybersecurity control.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

PART 4

Getting started

Q15. Where should an overwhelmed business owner start tomorrow morning?

Start with an inventory. Write down your devices, accounts, software, cloud services, important information and suppliers. Identify who has access to each. Then prioritise:

- **Protect access:** Use passkeys or strong MFA, starting with email and administrator accounts.
- **Protect data:** Establish protected backups and test restoring them.
- **Update technology:** Apply security updates and replace unsupported systems where possible.
- **Protect payments:** Introduce independent verification for changes to bank details and unusual transfers.
- **Manage AI:** Establish approved tools, data-sharing rules and human approval requirements.
- **Prepare people:** Make it easy to report mistakes and suspicious activity without blame.

The NCSC's free Cyber Action Toolkit provides personalised guidance for sole traders and small businesses. Consider working towards Cyber Essentials as a recognised baseline.

Q16. I'm a micro-business with fewer than ten employees. What cybersecurity protection do I really need, and where can I get help?

This is a question I particularly want to address because I think micro-businesses are often poorly served by the cybersecurity industry. And I say that not only as someone who has worked in cybersecurity for almost 30 years, but also as a micro-business owner myself.

In my own experience, finding good, affordable cybersecurity support for a very small company can be surprisingly difficult.

I've encountered providers whose services are designed for larger organisations, sometimes with minimum employee thresholds of 15, 25 or more people, or budgets that simply aren't realistic for a sole trader or micro-business.

I've also encountered advice that wasn't appropriate for the business concerned, or that confused general IT support with specialist cybersecurity expertise.

These are observations from my own experience, not findings from a formal industry-wide survey. There are excellent providers serving small businesses, but finding the right one isn't always easy.

And when you're running a business with only a handful of employees, you're not necessarily equipped to judge whether the cybersecurity advice you're receiving is sound.

That's a problem, because micro-businesses face many of the same threats as larger organisations, often without the resources to manage them.

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

The good news: there are things you can do yourself

You don't need an expensive cybersecurity team to make meaningful improvements.

1. **Protect your important accounts.** Enable MFA on your email, banking, accounting, cloud storage and other critical services. Use passkeys wherever possible. Introduce a reputable password manager and stop reusing passwords.
2. **Check your backups.** Find out what's being backed up and where the copies are stored. Then try restoring a file. Keep a protected copy of important business information that an attacker cannot easily delete or encrypt.
3. **Keep your technology updated.** Switch on automatic updates for laptops, phones, browsers, operating systems and business applications. Don't forget your website, including its plugins, themes and underlying software, such as PHP. If someone else manages your website, ask who's responsible for applying critical security updates and how quickly they're deployed. And remember your router and printer too.
4. **Protect yourself against scams.** Verify unusual payment requests using a trusted telephone number. Use Ask Silver from Get Safe Online to help assess suspicious messages. You can submit a screenshot of a suspected scam for assessment. Avoid sharing sensitive personal or business information, and don't treat a result as a guarantee that a message is safe.
5. **Check your broadband router and Wi-Fi.** Make sure your router receives updates, uses a strong administrator password and isn't exposing unnecessary management services to the internet. Use modern Wi-Fi encryption and provide a separate guest network if visitors need internet access.
6. **Protect your smartphone.** For many micro-business owners, their phone is effectively their office. Enable secure facial recognition or fingerprint authentication, backed by a strong passcode. Keep the operating system and apps updated, enable remote locking and erasure, and review which applications can access sensitive information. Make sure you have a secure way to recover important business accounts if your phone is lost or stolen.
7. **Make sure your business can operate if you lose access to a platform.** If your business relies on Instagram, Facebook, WhatsApp, an online marketplace or a single cloud provider, consider what happens if you lose access. Keep appropriate copies of customer information, own your domain name and have alternative communication arrangements.

How can you check whether your cybersecurity is working?

Don't simply accept reassurance. Ask yourself or your IT provider:

- Can I demonstrate that MFA is enabled on my critical accounts?
- Can I successfully restore a file from backup?
- Are my devices and software still receiving security updates?
- Do I know who has access to my business accounts?
- Is my business phone protected with secure biometrics, a strong passcode, automatic updates and remote-locking capabilities?
- If someone stole my laptop or compromised my browser account, could they access my business email, banking, customer records or other important services?
- Would I know who to contact if my email were compromised tonight?

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

- Could I continue trading if my main online platform became unavailable?

If you can't answer those questions, you've identified where to start.

Where can micro-businesses get help?

- **NCSC Cyber Action Toolkit:** a free, personalised tool designed for sole traders and small businesses.
- **NCSC Small Business Guide:** practical advice on essential cybersecurity measures.
- **Regional Cyber Resilience Centres:** police-supported organisations offering guidance and access to services for smaller businesses.
- **Global Cyber Alliance Small Business Toolkit:** free resources covering email security, phishing and other common risks.
- **Cyber Essentials:** a government-backed cybersecurity baseline.

What about security services from broadband and telecoms providers?

They're worth investigating. Some UK business broadband and telecoms providers offer services such as malicious website blocking, network-level threat protection, managed routers, secure Wi-Fi and technical support.

For a micro-business without dedicated IT staff, these may be useful additional layers of protection. But ask what is included, whether it is enabled, who maintains it and what risks remain outside its scope. A service marketed as secure broadband doesn't mean your entire business is protected.

> **My advice:** If you can only do three things this week, make them these: protect your email with strong MFA, check that you can restore your backups, and complete the NCSC's free Cyber Action Toolkit.

Then work through the other improvements. You don't need to solve everything immediately, but you do need to start.

> ***Cybersecurity shouldn't be a privilege reserved for businesses large enough to afford a dedicated team.***

Q17. What's the single most useful thing I can do in the next 30 days?

Rehearse a bad day. Set aside one hour with the people who would need to respond. Imagine your email is unavailable, customer records are locked and you can't take payments. Ask:

- Who is in charge?
- Who do we contact?
- How will we communicate?
- Can we still serve customers?
- How long can we operate?
- What must be restored first?
- When did we last test recovery?

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Run scenarios involving malice, mistake and malfunction. The NCSC's free Exercise in a Box provides ready-made exercises. At the end, identify three improvements, assign owners and set deadlines.

> ***Don't wait for an attack to discover whether your recovery plan works.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Small Business Cybersecurity Checklist

Use this page to track your progress. Each item links back to the relevant question in the guide.

PROTECT ACCESS

- ☐ MFA or passkeys enabled on email, banking, accounting and cloud accounts (Q4, Q16)
- ☐ A reputable password manager in use, with no reused passwords (Q4)
- ☐ Individual accounts for every person; no shared logins (Q4)
- ☐ Administrator access restricted and reviewed (Q2, Q7)

PROTECT DATA

- ☐ Backups follow the 3-2-1 approach, with one protected copy (Q10)
- ☐ A file restore has been tested successfully, and the date recorded (Q10, Q16)

KEEP TECHNOLOGY UPDATED

- ☐ Automatic updates switched on for laptops, phones, browsers and apps (Q16)
- ☐ Unsupported devices identified and replaced or isolated (Q8, Q9)
- ☐ Website plugins, themes and underlying software confirmed as supported and patched (Q16)
- ☐ Router supported, updated, default password changed, guest Wi-Fi separate (Q9)

PROTECT PAYMENTS

- ☐ Bank detail changes verified by phone using a number already on file (Q6)
- ☐ Two people authorise significant or unusual payments (Q6)
- ☐ SPF, DKIM and DMARC checked with the NCSC Email Security Check (Q6)

MANAGE SUPPLIERS AND AI

- ☐ IT provider has answered the Q7 questions and provides a monthly report (Q7)
- ☐ Approved AI tools and data-sharing rules agreed (Q3, Q5)

BE READY

- ☐ Phone secured with biometrics, strong passcode and remote erase (Q4)
- ☐ Account recovery codes stored safely away from the phone (Q4)
- ☐ Cyber insurance requirements and contacts checked (Q14)
- ☐ A "bad day" exercise has been run in the last 12 months (Q17)
- ☐ NCSC Cyber Action Toolkit completed (Q15, Q16)

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

First-Hour Incident Response Checklist

Keep a printed copy somewhere you can reach it if your systems are unavailable.

- ☐ Contact your IT or cybersecurity provider and agree who is leading the response.
- ☐ Isolate affected devices: disconnect the network cable and disable Wi-Fi. Don't wipe or reset them; where safe, keep them powered on.
- ☐ Secure affected accounts: revoke suspicious sessions, disable compromised access and check for malicious forwarding rules.
- ☐ Contact your bank immediately if money is involved. Call 159 to reach participating banks' fraud teams.
- ☐ Tell employees what to do and how to communicate safely if email may be compromised.
- ☐ Contact your cyber insurer and follow its notification requirements.
- ☐ Preserve evidence: record what happened, when it was discovered and every action taken.
- ☐ Assess reporting requirements: certain personal data breaches must be reported to the ICO within 72 hours.
- ☐ Report fraud through Report Fraud, and report the cybersecurity incident to the NCSC.
- ☐ Prepare a holding statement for customers: what you know, what it means for them, what you're doing.

KEY CONTACTS (FILL IN BEFORE YOU NEED THEM)

IT / cybersecurity provider .....

Bank fraud team .....

Cyber insurer and policy number .....

Person leading the response .....

Alternative communication channel .....

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0

Final thought: Are you protected, or are you prepared?

Many businesses understand that cyber risk exists but still struggle to take action. Sometimes they underestimate the likelihood of an attack. Sometimes they assume their IT provider, security software or insurance policy has everything covered. Sometimes there are simply too many competing priorities.

And for micro-businesses, there can be another challenge: finding appropriate, affordable and trustworthy advice in the first place.

But cybersecurity isn't just about preventing bad things from happening. It's about protecting your ability to continue operating when they do.

The disruption may come from malice, mistake or malfunction. Your organisation may be attacked directly, or it may suffer because a supplier fails. Your security controls may work exactly as designed and still leave your business unable to deliver what customers need.

That's why I believe businesses must think beyond cybersecurity controls towards cyber survivability.

Know what matters most. Understand your dependencies. Test your assumptions. Preserve your options, because ultimately, the question isn't simply whether you can stop an attack.

> ***It's whether your business can survive one.***

© 2026 KnewStart. All rights reserved. | October 2026 | Edition 1.0