How to future-proof your business for AI cyber threats

A guide for small and medium-sized businesses

In association with

be the business

1. Introduction

Technology is changing the world faster than ever. AI is now everywhere, accessible to everyone, for free. For business, that creates significant cyber risks – ones that didn't exist 12 or 24 months ago.

And it's not only large companies under threat. Far from it. The most vulnerable businesses are small and medium size firms, particularly those where cybersecurity has always taken a back seat. Where 'good enough' means relying on firewalls and antivirus software (because that's how it's always been).

35% of UK microbusinesses experienced a cyber attack in the 12 months to April 2025

43% of UK small businesses experienced a cyber attack in the 12 months to April 2025

£1,600 average cost of the most disruptive cyber security breach in the 12 months to April 2025

£7,960 average cost of the most disruptive cyber security breach in the 12 months to April 2025, excluding those who experienced no impact from their most disruptive breach

DSIT Cyber Security Breaches Survey, 2025

Generative AI is now extremely capable

We've probably all heard of ChatGPT, a generative AI chatbot.

Generative AI means artificial intelligence that can create new content, like text, computer code, and even audio and video (more on that later). When it launched in November 2022, it was the first chatbot to be trained on vast amounts of text and able to converse like a human on any subject.

Since then, the pace of change has accelerated very quickly. Generative AI tools like ChatGPT and rival Google Gemini are now:

- Much better at understanding and creating things
- More accessible and being used in more places
- Easier to use for consumers, businesses and developers

2. AI is a business-critical risk for SMBs' cyber security in 2025 and beyond

For small and medium-size businesses (SMBs), cybersecurity threats are increasing. Some might sound far-fetched – but the risks are very real.

39% of small businesses have no cybersecurity training in place

Be the Business, 2025

612,000 UK businesses identified a cyber breach or attack in the past year

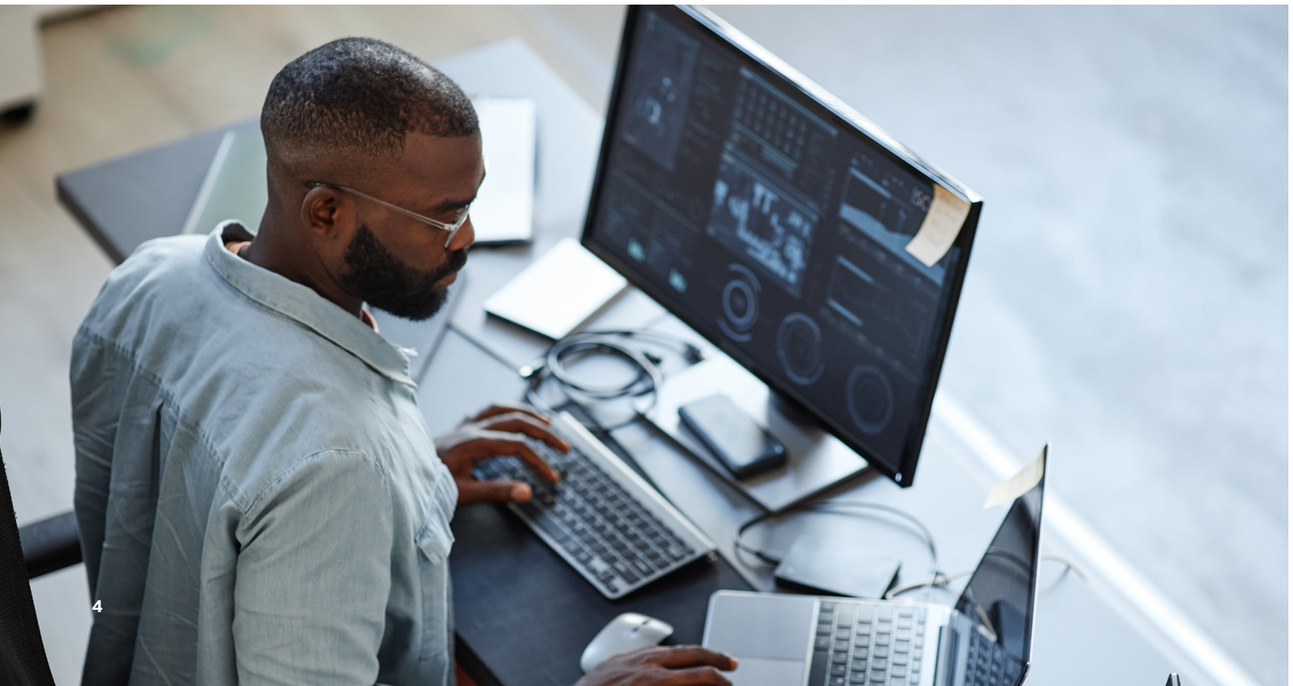
DSIT Cyber Security Breaches Survey, 2025

61,000 UK charities identified a cyber breach or attack in the past year

DSIT Cyber Security Breaches Survey, 2025

74% of cybersecurity experts think AI-Powered cyber threats are a major risk for their organisation

Darktrace, 2025



A poll of almost 1,000 Chief Internal Auditors across 20 European countries, conducted by the Chartered Institute of Internal Auditors, found the risks presented by AI are rising faster than any other business-critical issue.

83% of auditors cited Cyber Security as the top risk

ECIIA, Risk in Focus 2025: Hot topics for internal auditors, 2024

52% identified human capital, diversity, talent management and retention as a top five risk (ranked second)

DSIT Cyber Security Breaches Survey, 2025

46% cited changes in laws and regulations (ranked third)

Chartered IIA study, 2024

Threat 1: Badly implemented generative AI

Generative AI tools hold huge promise for business. They can help you be more efficient, reduce your costs and grow faster. But although they seem easy to use, the underlying technology is extremely complex.

Just like how a driving license doesn't give you the skills to race a Formula 1 car, IT know-how alone isn't enough to implement generative AI safely. It requires advanced, specialist expertise and qualifications.

AI systems, especially those used for security (like spotting unusual activity on your network), learn from data. If these technologies are not set up correctly, you risk 'data poisoning'. This is an attack where malicious actors subtly feed bad data into the AI's learning process.

Over time, this can corrupt the AI's understanding, teaching it to ignore real threats or see legitimate activity as malicious.

Solution: Choose technology partners with proven expertise in secure AI implementation, not just general IT skills.

- Carefully check their qualifications in managing AI-specific threats like data poisoning, their track record with secure AI deployments, and their specific processes for protecting your business data within AI systems.
- Make sure you have strong contracts in place.
- Create clear policies for your employees on how to use generative tools safely and what's acceptable. This should include banning staff from putting sensitive company or customer information into these tools unless there are clear safety measures.

Threat 2: Smart devices and the ‘internet of things’

In the past, a business intranet (internal network) and the internet were mostly separate entities. Now, that distinction is no longer true. Assuming that everything ‘inside’ your network is safe makes your business highly vulnerable.

Because networks, devices and the internet are all interconnected, everything connected to your system must be secure. This includes work-from-home laptops, smart devices like networked printers or security cameras, and mobile devices like work phones.

Smart devices, often known as IoT (internet of things), are particularly vulnerable to cyber attacks. As of 2024, there were over 16 billion connected IoT devices. Many of them have significant processing power, which means they can do more damage if malicious actors take control of them.

When hackers infect poorly secured IoT devices with malware, these compromised devices can form a “botnet” – a network controlled by the attacker. On command, all the devices simultaneously flood a target (e.g. an ecommerce website) with internet traffic. The volume of traffic overwhelms the target, knocking it offline.

Even though manufacturers claim IoT products comply with security standards and certifications, their security protections are often inadequate. As these devices become more integrated into business operations, the associated risks increase.

Solution: Adopt a Zero Trust approach to security

- Zero trust means no device or user is inherently trusted, even if they’re already connected to your network. In future, this could potentially involve giving access with methods like continuous biometric verification, where a user’s identity is verified by monitoring their unique biological or behavioural traits (like their fingerprint, face or movements), throughout an entire active session rather than just at login.
- Apply the ‘principle of least privilege.’ An IoT security camera, for example, should only communicate with its designated secure server and never with other systems like finance.
- Make a complete list of all your connected smart devices and immediately change all default passwords to strong, unique ones.
- Ask your tech partner to put these devices on their own separate network section if possible. Keep your devices updated with the latest software, and use basic network monitoring to spot and block any suspicious activity.

How to future-proof your business for AI cyber threats

Threat 3: Attacks using quantum computers

Looking to the future, the risk of quantum attacks is increasing. Quantum attacks are cyber attacks conducted by extremely powerful computers – powerful enough to crack the code that encrypts (protects) our information in systems like email and messaging.

Just like the other threats, any business of any size could be under threat. It may feel like a future problem, but “harvest now, decrypt later” means the threat from quantum is very real even today. Hackers may hold onto encrypted data, knowing that in the future they may be able to use quantum to exploit it.

The likely target is information transmitted over your business networks. The reality is: nothing digital can be fully trusted. Even the security tools you adopt might have the potential to be turned against you, unless they are provided and configured by well-trained professionals who understand these complex, interwoven dangers.

Solution: Prioritise expertise for quantum and interconnected threats

- Using standard security software without expert set-up is becoming a bigger risk. Your approach to security needs to factor in these advanced, interconnected threats.
- When you review any new tech, especially AI-driven tools or services that will handle sensitive data, carefully check how they’re protected against these new threats. Start to observe if suppliers are talking about readiness for quantum threats and where possible, start to ask pointed questions about their readiness.
- Remember: any tool is only as secure as how it’s set up. It’s very important to make sure your security tools are provided and configured by well-trained professionals.
- This means investing in partners or staff with a genuine understanding of these changing risks. They can help you choose the right tools, ensure they’re set up correctly, and update your protections as the threat landscape changes.

> “Even the security tools you adopt might have the potential to be turned against you, unless they are provided and configured by well-trained professionals.”

Attacks usually begin with AI-enabled social engineering

AI cybersecurity threats are not hypothetical. It's happening now, and malicious actors could target any business. Even tech-savvy, well-protected firms can still be vulnerable to threats.

The recent attack on a UK retailer, for example, is believed to have originated from a contractor in its supply chain. It took the form of a social engineering attack – where criminals convince a human to give them access to a network by impersonating someone else.

Reports suggest a hacker first called the company's outsourced IT service desk, impersonating internal staff with a request to reset passwords and disable security precautions. This allowed the hackers to bypass the company's usual cybersecurity defences entirely; they were then able to deploy ransomware (malicious software) in their systems. The attack is believed to have cost the company around £300m as of June 2025, and its impact is ongoing.

Such attacks are extremely common. In 2024, the National Cyber Security Centre predicted a 'significant uplift' in social engineering by hackers-for-hire, opportunistic cyber criminals and hacktivists (activist hackers) by the end of 2025.

That prediction was correct: research suggests 98% of cyber attacks now involve this technique. And it's not only large corporations under threat; the average business faces over 700 attempted social engineering attacks annually. Fake audio and videos created by generative AI ('deepfakes') have also made these attacks much more convincing and much easier to perform, increasing the risk.

How a deepfake social engineering attack cost $25 million

In early 2024, a global engineering firm fell victim to an extremely sophisticated AI-driven scam.

In early 2024, a global engineering firm fell victim to an extremely sophisticated AI-driven scam. A finance employee in their Hong Kong office was tricked into transferring approximately $25 million to fraudsters after attending a video conference where AI-generated deepfakes convincingly impersonated their Chief Financial Officer and other senior executives.

The criminals used AI to create realistic video and voice clones of these individuals, making the group video call, with multiple supposed executives participating and giving instructions, appear entirely genuine.

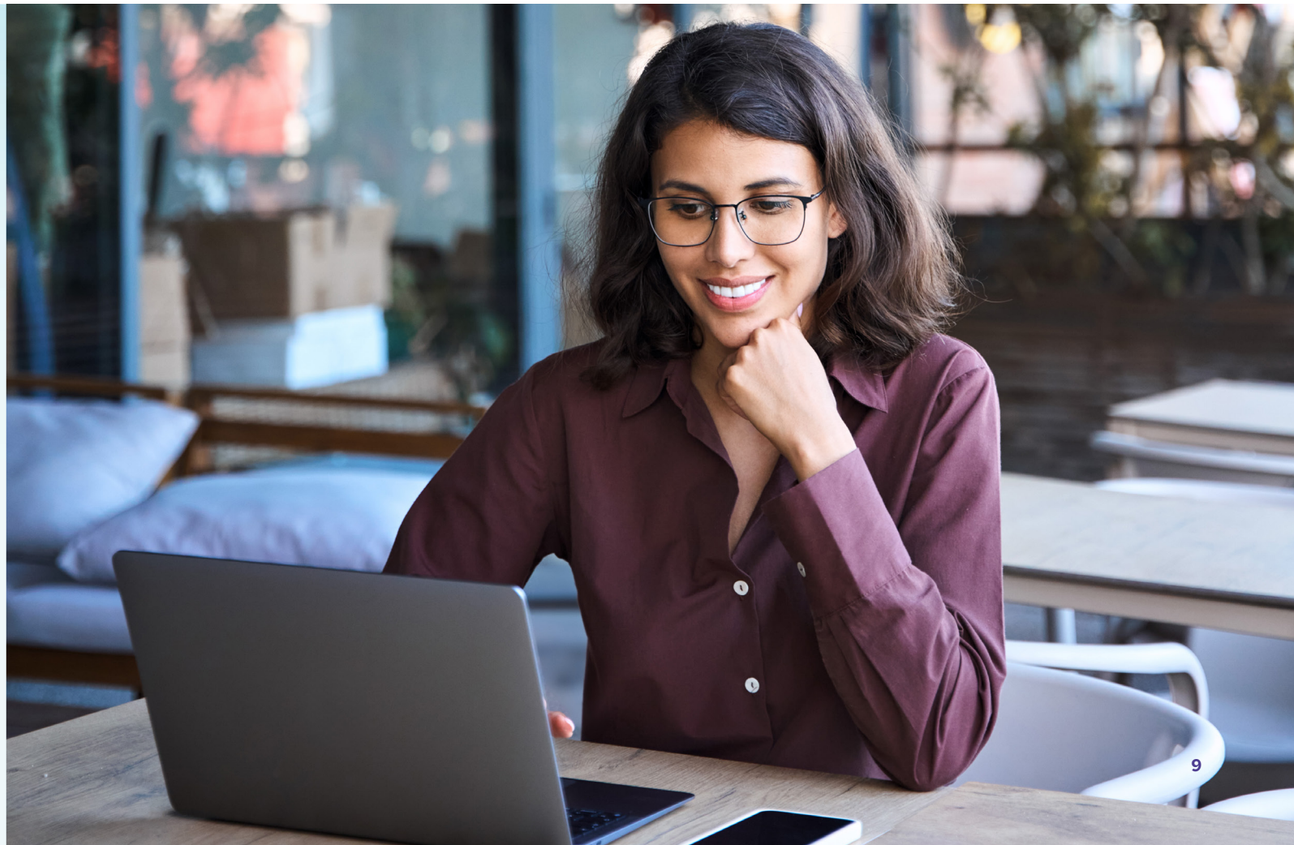
How North Korean hackers defrauded blue-chip U.S. firms out of $6.8 million

Another example is a series of high-profile attacks in 2024. North Korean hackers posing as U.S. IT workers successfully infiltrated dozens of Fortune 500 companies by securing remote jobs, including a Silicon Valley tech company, a U.S. car maker and a luxury retail store among many others.

The hackers used generative AI to create remarkably convincing fake online personas and highly personalised messages on LinkedIn. To maintain their U.S. presence, company-issued laptops, shipped to the supposedly American hires, were actually managed by a local intermediary. This allowed the foreign-based hackers to remotely access these trusted devices from abroad.

Their activity then appeared as legitimate U.S. employee traffic, effectively bypassing geographical security checks and using 'safe' company hardware to infiltrate internal networks and access data.

The hackers fraudulently received over $6.8m in wages, and in some cases, downloaded sensitive company data before sending a ransom demand.



£175m or 4% of turnover

maximum potential fine issued by Information Commissioner's Office (ICO) for breach of customer data

ICO, 2025

The human factor

These events show how the weakest link in a cyber security system is often the human – and why a zero trust approach is business critical.

Malicious actors using generative AI are often able to convince employees to click a malicious link or open an infected document.

That single click can be enough to deploy malware onto the SMB's systems; the danger then rapidly escalates through supply chains.

Supply chain threats have ripple effects

Once an SMB is compromised, attackers can exploit its trusted status and systems to target clients, customers, and partners, using the SMB as an unwitting launchpad for wider attacks.

This is precisely what happened in 2018, when an admin password stored in a text file in a business contractor's infrastructure allowed hackers to 'break out' of their system, access their customer's own internal systems, and steal over 380,000 customers' card data. The breach resulted in a record £20 million fine.

The lesson is clear: every vendor you work with can increase your vulnerability to attacks and if you work with a large business, you're even more likely to be targeted. And seemingly minor mistakes – like storing a password in unprotected, easily accessible text files – can have catastrophic consequences. It's essential both you and your entire supply chain conduct regular cybersecurity audits to find any weak links and mitigate your risk.

How to future-proof your business for AI cyber threats

How one click created a supply chain ripple effect for Laura's accounting firm

When an invoice for her client landed in Laura Day-Henderson's inbox, it looked just like any other. She's a self-employed accountant handling the books for over 50 businesses – and there were never enough hours in the day.

Under heavy time pressure, she clicked the Dropbox link to open the invoice.

"I'm quite tech savvy and mindful of what's going on, but working as an accountant/bookkeeper for a lot of different businesses, we don't necessarily know the individual suppliers that each business is working with. So when a link to access an invoice came through the client's inbox, we presumed it needed to be processed," she says.

It wasn't an invoice. It was malware, which immediately re-sent a similar email to everybody in the client's inbox. The impact was immediate.

"Suddenly we've got all these phone calls coming in saying, oh, I've just opened an email from you. Is that legitimate? Because I wasn't expecting an invoice from you."

Everybody who opened the link were now themselves under attack. The effects were snowballing.

"We had to send an email to everyone to make them aware of what had happened, tell them not to open the link if they haven't already," Laura says. "Or if they have, advise them to get somebody who actually knows what they are doing to investigate it. And of course just apologise for what happened.

"We had people asking for compensation because they've had to get somebody in to make sure there's no issues. And we're wondering: are we paying that out? Is it worth going through insurance? Is it actually our responsibility?

"But at the same time, you don't want to have a bad business relationship. These are people you work with, you want to continue working with, so you have to keep people happy as well.

"The client did pay out – about £500 per disgruntled contact. Unfortunately they couldn't claim through their insurance as their insurance policy didn't cover cyber attacks. They then put a claim in against the accounting firm and ultimately a claim on myself.

In the end, Laura didn't have to cover the costs because the attack didn't originate from her. But it was a lesson learnt the hard way.

"It was embarrassing, more than anything, because as an accountant, you want to protect a client's financial and personal data as much as possible. You need to be very careful with things, you need to be very diligent. And it reflects badly on your ability to do that sort of thing."

> "It's a lot better to think twice and take an extra second than it is to have a massive headache to deal with afterwards."

"The biggest lesson learnt, though, is to make sure you've already got a plan of who to turn to if something goes wrong – because if you don't have something in place, you're going to be spending hours, if not days or weeks, researching who to contact. And the longer it's not dealt with, the more damage can potentially be caused."

How one vulnerability cascaded into multiple client attacks for Balbinder's website business

For Balbinder, owner of a UK web design and development business, managing over 100 client websites on a single physical server was initially a practical solution. But it became a critical vulnerability.

The first sign of trouble was subtle: some client sites began sending out unwanted "spam" emails.

This led to his mail server – the system responsible for sending and receiving emails – being "blacklisted." Other email systems would then automatically reject emails coming from his server, severely impacting his clients' ability to communicate.

Balbinder quickly separated the mail server, thinking he'd contained the issue.

But the problem persisted – and began to escalate.

"I realised there had been some sort of MySQL injection on the database," he explains. Hackers had exploited a weakness to insert malicious code into the website's data storage, which holds vital information like user details or website content.

He checked the activity logs, showing who was doing what within the website's backend (behind the scenes).

Tracing a suspicious IP address (unique web address) from Thailand, he could see the hacker moving from one client's site to another, extracting data.

"It felt daunting. Scary." he says. "I was thinking: have I got the skill set to deal with this?".

Clients were asking why their website wasn't working, their email wasn't working, or they were getting spam. Some said they were losing money and threatened to leave.

The solution was a drastic one: a complete overhaul, through the night, of every client's site. Balbinder moved each one to new, separate cloud servers – which can be more secure – with up-to-date security fixes and better activity logging.

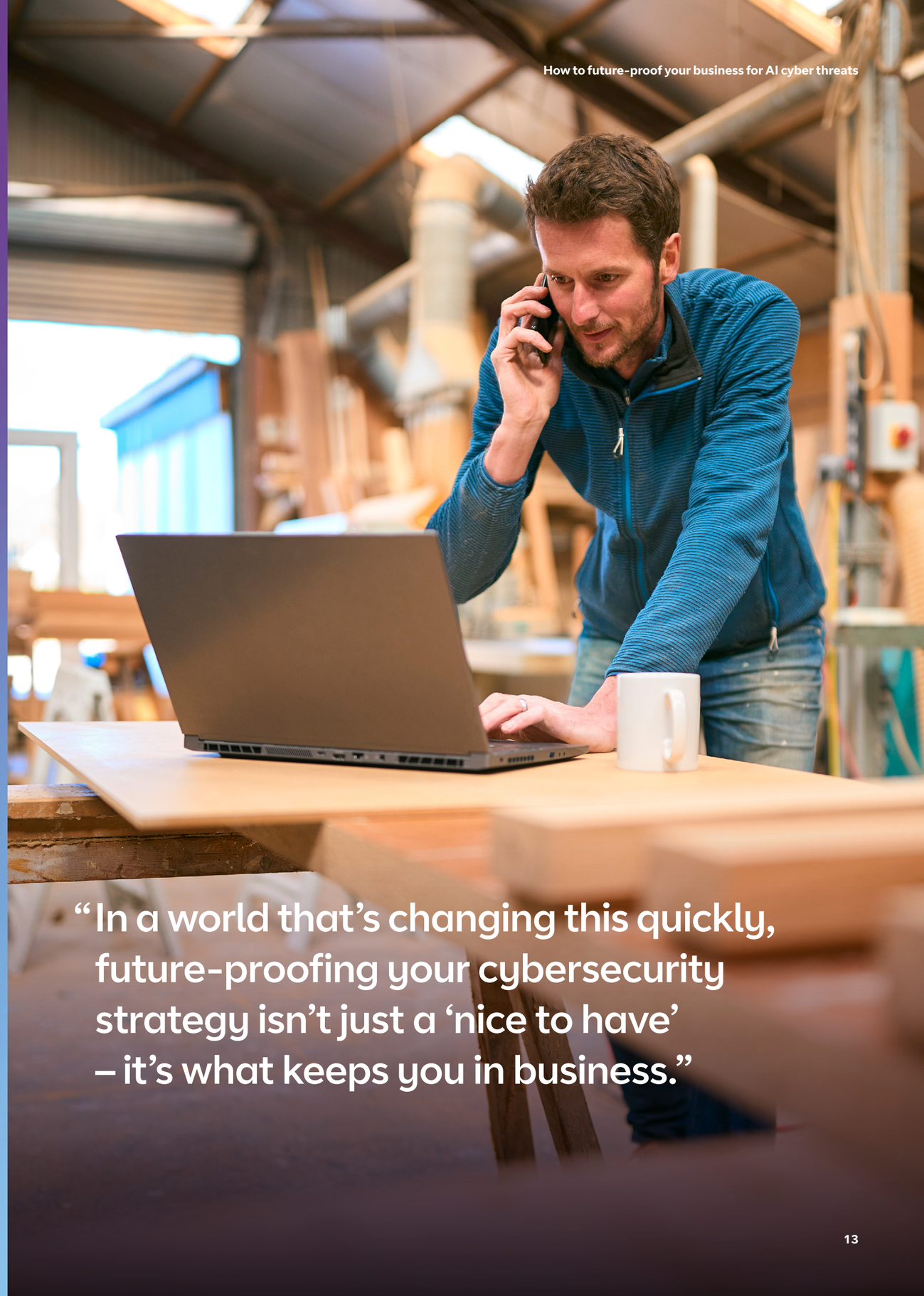
And the root cause? It was a malicious piece of add-on website software (a "plugin") from a dodgy developer who later became known for creating backdoors to steal data.

Balbinder's key lesson is the need for ongoing investment in cybersecurity.

> "Keep on top of your software and when it goes out of date – especially software that can't be upgraded any more."

"Ultimately, it may seem like a bit of a cost to invest in software updates but the cost of not doing it is potentially a lot higher. Non-technical businesses need expert help – and remember: anything on the web can be exposed."

How to future-proof your business for AI cyber threats



"In a world that's changing this quickly, future-proofing your cybersecurity strategy isn't just a 'nice to have' – it's what keeps you in business."

3. Don’t go it alone

Technologies like AI, expanding IoT networks and quantum computing are more complex and fast-moving than ever before. The risks are increasing – and SMBs need to prepare now.

To do that, you need more than just basic IT support. You need a security partner equipped with proactive threat intelligence to help you anticipate and mitigate risks before it’s too late.

This means collaborating with a team that’s always on alert for what’s next, understands the sophisticated tactics of modern cybercriminals, and translates that knowledge into practical protection for your business.

BT is uniquely well positioned to help

We’re ranked eighth in Europe and 24th in the world for filing cybersecurity patents. And we’re one of the only cybersecurity providers with a dedicated internal innovation team, anticipating future threats and developing the next generation of protective solutions. So we can protect you from threats that others don’t see coming.

Because in a world that’s changing this quickly, future-proofing your cybersecurity strategy isn’t just a ‘nice to have’ – it’s what keeps you in business.

Need help protecting your business from cyber threats?

Talk to a BT Business cyber expert:
business.bt.com/security/small-business-cyber-security

For general cybersecurity guidance, visit the UK government’s National Cyber Security Centre website:
ncsc.gov.uk/cyberessentials/overview

In association with

be the business