censornet.

2024 UK Cyber Resilience Report

The state of UK SMBs' cybersecurity response

Contents

Welcome

The UK is unprepared for a large-scale ransomware attack and "at any moment" could be brought to a standstill. Impactful words from Parliament's Joint Committee on the National Security Strategy (JCNSS). But it's not just ransomware – the UK is grappling with additional risks.

Generative AI, for one, presents a delicate balancing act for cybersecurity leaders. On one hand, business leaders extol its virtues, seeking productivity gains. On the other, generative AI's potential for sophisticated phishing, personalised email attacks, and backdoor vulnerabilities weighs heavily.

As if that weren't daunting enough, ongoing geopolitical uncertainty is adding to the complexity, introducing fresh risks from state-affiliated cyber actors. We've seen attacks from 'the big four' – China, Russia, North Korea, and Iran – hitting enterprises, governments, and SMBs from all sides.

Encouragingly, it's clear that our national leaders aren't oblivious to the cyber risks swirling for business and society. The EU's NIS2 directive is one of several measures expected to come into force this year, alongside the digital operational resilience act, cyber resilience act, and AI Act.

So, we're at a crossroads... The challenges are unprecedented. But so too are the pioneering technologies that can help us to tackle them.

This is our third annual report, exploring how UK SMBs defended against attacks in 2023 and their strategies for 2024. Amid data loss, extortion, and ransomware havoc, there's hope: SMBs are investing in technologies to confront the generative-AI threat head-on.

Ed Macnair
CEO
Censornet

01 Cyber threats on steroids

The cyber tug of war is about to get an injection of steroids.

Data loss, extortion, and ransomware continue to wreak havoc – causing sleepless nights and interrupted holidays. And, to make matters worse, SMBs are grappling with deciphering the 'myths and realities of AI'. The challenge on their agenda is to truly understand how AI is being used in cyber attacks and defence. There are three notable areas shaping the cyber threat landscape:

Data Loss and Extortion

Nearly four-in-ten SMBs lost data to a cyber attack in 2023. The MoveIT attacks were a high-profile example of data loss. The attackers successfully leveraged a zero-day exploit in Progress Software's file transfer tool. This attack demonstrates how cyber criminals' tactics have evolved to steal and exploit sensitive data through supply chains.

The Ransomware Lotto

For a third consecutive year, around one in five SMBs fell victim to a ransomware attack. In fact, only 35% feel they have the ability to protect themselves against attacks of this nature.

Even Royal Mail was vulnerable. An attack by the LockBit affiliate left 11,500 Post Office branches unable to handle international mail or parcels for nearly six weeks. Besides the £10m cost in remediation and system resilience improvements (to date!), it's a stark reminder of ransomware's potential to shut down business operations too.

The Myths & Realities of AI in Cyber

The democratisation of AI is a game-changer for cyber attacks. The National Cyber Security Centre has warned that cyber reconnaissance, phishing, and coding[1] will all become more effective and efficient due to AI. And a community of bad actors is eager to manipulate that advantage to advance its attacks.

It's not all bad news, though. The same technology that expands the attack surface can equally protect SMBs against its risks. It makes AI a certain priority for 2024.

"The threat landscape is becoming even more complex, with AI being used as both an attack vector and an attack surface. SMBs are demanding more from their cybersecurity, looking for better ways to fortify their business and safeguard their assets."

Matt Eggleton
Alliance Manager | TET Limited

1. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

of organisations can't protect against ransomware attacks

02 A mixed cyber threat hit list

Cyber threats are commonplace for SMBs. Many are being hit by both malice and employee error. And, to make matters worse, they're being held to ransom and fined for the privilege. So, what's catching the IT department out?

1. **Malice and error hit SMBs in equal measure**
   27% of SMBs lost data last year due to disgruntled employees. And 30% lost data due to user error. So, not all risks are malfunction and malice related.
2. **Suspicious emails tempted one-in-five employees**
   Nearly one-in-five SMBs suffered from an employee opening a suspicious or malicious email that led to a serious attack.
3. **Data loss due to a cyber attack jumped 30%**
   39% of SMBs lost data due to a cyber attack in 2023. That's a 30% jump over 2021, waving a red flag that they're not doing enough to protect themselves.
4. **The ransomware threat stayed consistent**
   One-in-five SMBs fell victim to ransomware – unchanged over the last three years.
5. **One in three paid a ransom and one in five was fined**
   34% of SMBs paid out after a ransomware attack last year – that's one in three! And the costs don't end there: one in five was also subject to a regulatory fine.

So, what is causing the high rate of cyber-related incidents?

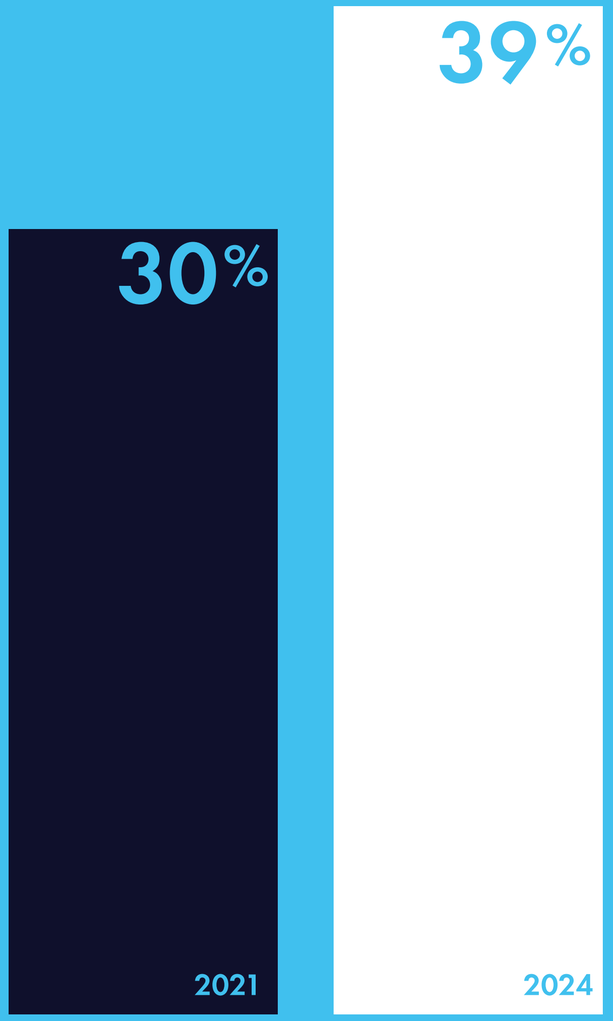
"The era when only large enterprises faced cyber attacks is long gone. SMBs should consider assessing their current cyber strategy and technology to understand how they perform against industry standards and highlight potential breach risks. Without detection, response, and remediation strategies, small and medium businesses are targeted as easy wins to opportunistic threat actors. Communicate has seen organisations falling prey to attacks that could have been avoided with things like MFA and Cyber Security Awareness Training."

David Johnson
Cyber Director | Communicate Technology

What was the #1 reason for data loss over the last 12 months?

Data loss jumps significantly in three years

Organisations who have suffered data loss because of cyber attacks

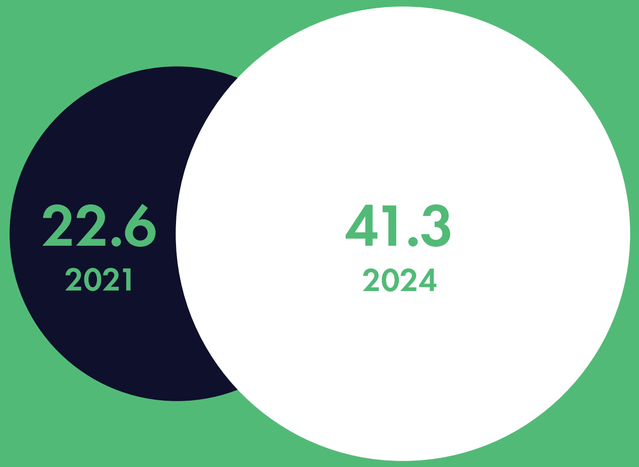


03 The overwhelming volume of alerts

The sheer number of cybersecurity alerts facing businesses each day has grown exponentially. To stay secure, each alert needs investigating. And, to make matters worse, IT teams are shrinking. Together, it's created a perfect storm.

Compare the size of the attack...

Security alerts per hour

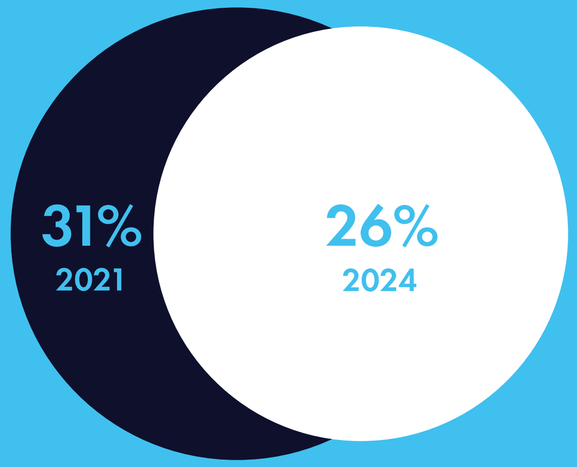


Security professionals today are handling nearly double the number of alerts compared to three years ago. Now, they receive 41.3 alerts per hour, compared to 22.6 in 2021.

One-in-six SMBs (16%) receive more than 1,000 alerts on an average day – that's more than double the number of businesses that experienced such high volumes in 2021.

...with the size of the defence.

Businesses that employs three or more people with responsibility for cybersecurity



The mean size of security teams today is 2.63 people. That's slightly down from 2.7 people in 2021.

However, only one-in-four (26%) businesses employs three or more people with responsibility for cybersecurity today. That's down from 31% only three years ago.

Who (or what) picks up the slack?

It all adds up to cybersecurity professionals taking on drastically increased workloads (and there's more on the human cost to come...).

Alarmingly, it also means that 40% of alerts simply aren't being investigated – there just isn't time in the day.

It begs the question: who (or what) is picking up the slack? If the human resource isn't available, are businesses implementing more comprehensive system-based defences instead?

The response we're seeing is uncertain at best: more than half (53%) believe their cybersecurity needs development.

It's no wonder that IT staff are suffering.

"Our own Security Operations Centre is monitoring more and more alerts. We're now processing thousands of high-level incidents a month for our clients. The bottom line for SecOps is to keep your Mean Time To Detect and Respond as low as possible, regardless of the quantities of alerts – and you can only do that with the right team, process and technology."

David Smart
CEO | Softwerx

04 Cyber professionals are suffering

So, what about the impact on people? How are cybersecurity professionals expected to 'square the circle' of the rising number of threats with their shrinking resources?

We found three areas where the pressure is really taking hold:

Annual leave interrupted

- Security professionals are regularly working out of hours. 38% have been called in the middle of the night to investigate an incident.
- Many can't get away even when they try; a third have had their annual leave interrupted by security alerts.

Sleep deprivation is rife

- There's been a big jump in the number of security professionals experiencing sleep deprivation. On average, security professionals get just over five-and-a-half hours' sleep a night – hardly a healthy routine.
- Nearly a third feel unable to cope and have experienced prolonged periods of work-related stress and burnout.

Career progression has slowed

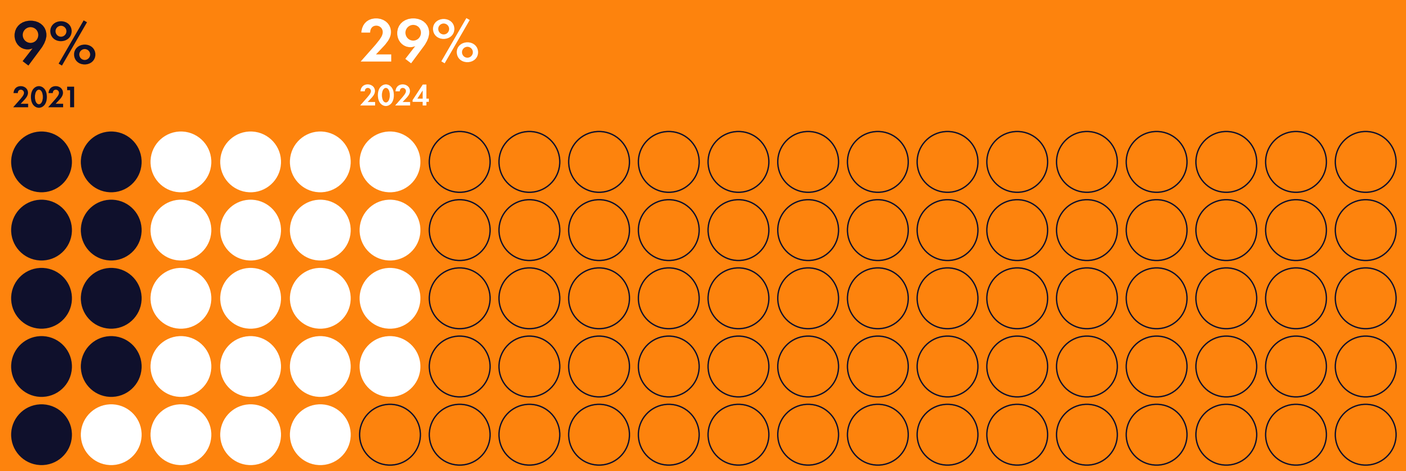
- The number who feel their career prospects have been negatively impacted because of a cyber attack has jumped from 18% to 29% over the last three years.

All signs indicate problems – not only today but also in the future. In addition to the imbalance between cyber risk and cyber defence, security estates for SMBs are becoming increasingly complex. With people's health, lifestyle, and professional reputation in the balance, are we doing enough as an industry to help?

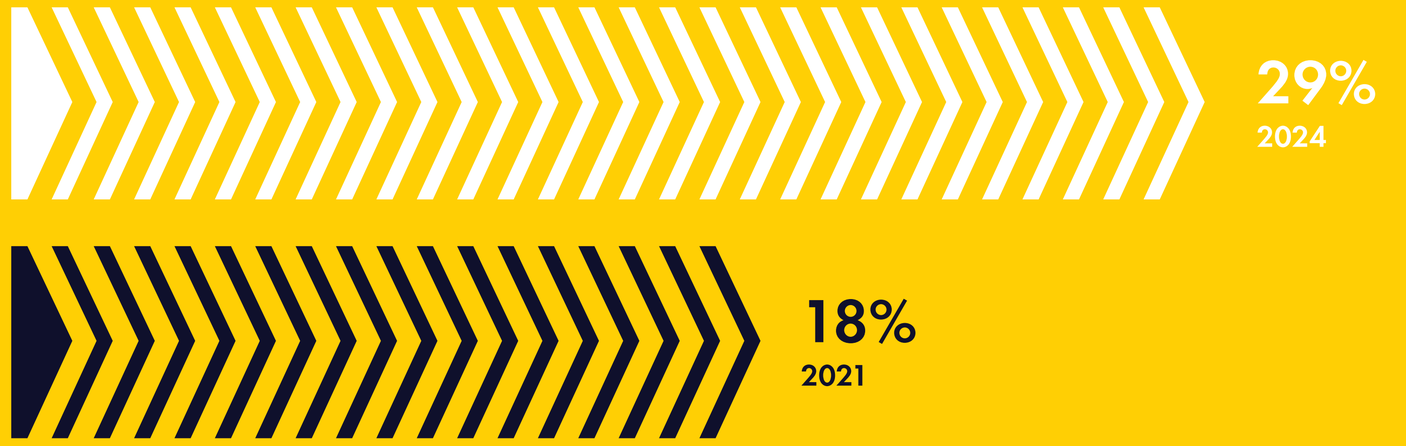
"We need to better look after the people charged with protecting our organisations' security. Reducing the cyber noise and finding a more robust way to respond and remediate threats plays a big part here."

Annie Miller
Marketing Manager | NGS

Suffered from sleep deprivation due to cybersecurity concerns



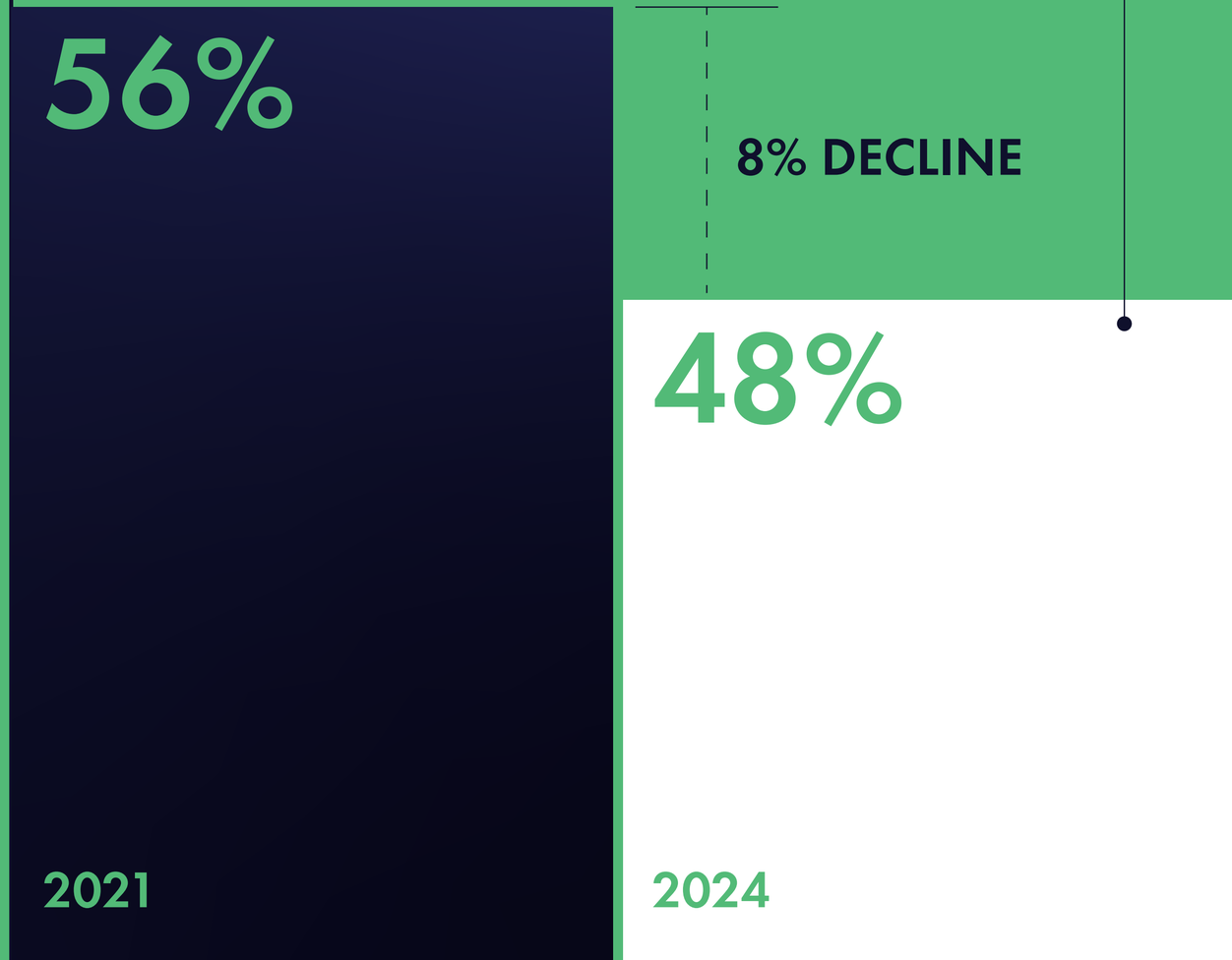
Feeling a cyber attack has negatively impacted personal career prospects.



53%

think cybersecurity needs development

But only 48% believe their cybersecurity is fully future-proofed.



↘ CYBER READINESS IN DECLINE

05 Less is more in the cyber future

Concerns about cybersecurity defences are largely fuelled by the breadth and depth of products that SMBs rely on.

In fact, almost seven-in-ten (67%) professionals list 'the number of point products they need to protect their data' as their biggest challenge in 2024.

SMBs are increasingly adopting cloud-based cybersecurity products. The rationale behind this shift lies in the ease of setup, management, and lower maintenance associated with cloud-based cyber applications. They hope the cloud will help them reduce their point challenge. It's why six in ten (62%) are managing cybersecurity products via the cloud in 2024, up from 57% in 2023.

But it's the volume play that's hurting

The cloud isn't a magic bullet. SMBs are still reliant on 22 individual cyber point products. This is costly, complex, and frustrating. And it's an issue that can be solved with better technology. Four in ten are calling for cybersecurity innovation that's offered to enterprises to be made available to them too. Here, they can access more comprehensive suites of products that tie together technologies to reduce the volume headache.

It's a problem that's unfortunately been around for years, with the average number of point products staying roughly the same since 2021. This is despite organisations' best efforts to change that status quo.

And it's a problem that's felt more profoundly by public sector organisations: 61% are now taking steps to reduce their number of cybersecurity vendors, alongside 51% of their private sector counterparts.

Clearly, consolidation is an important element of security policy in 2024. Given the pressures outlined in earlier chapters, security teams scarcely have the time to manage a vast and complicated stable of vendors and platforms. Accessing critical functions through a single vendor can go a long way to reducing stress and improving cybersecurity performance.

But how else can we tighten our cybersecurity defences?

"Are your IT operations capable of managing rapid growth and expansion plans? As organisations grow, the volume of technology solutions can escalate, causing a complexity of systems that's hard to manage."

James McKee
Cyber Security Consultant | Qual

67%

list the number of cybersecurity point products needed to protect against the entire threat spectrum as their biggest challenge in 2024

06 Is protection on the decline?

Consolidation alone won't close the cyber gap. We need to tighten our defences and protect our data with today's latest technology. But SMBs are lagging in preparedness against some very common and prevalent attack vectors — even more so than expected. And that's a concern, given that the intricacy and persistence of cyber attacks is rising fast. Here are some significant examples of concern:

Only one in two has file sharing visibility

Unauthorised access and accidental disclosure are big concerns. It's likely due to just one-in-two SMBs having visibility over file content that staff share externally. And only 47% have data loss prevention (DLP) solutions in place, leaving half vulnerable to major data loss.

Cross-channel attack defences are crumbling

In 2021, 37% of businesses told us they were protected against cross-channel attacks (specifically those that start with email).

In 2024, that number plummeted to 29.5%.

We see a similar, albeit less dramatic drop in the ability to block dangerous attachments from reaching the inbox, alongside a fall in the ability to quarantine suspicious or malicious emails.

Just half can manage the risk of new cloud apps

- Only half of businesses can manage cloud application usage.
- Just one in two can track data leaving the business.
- Under a quarter can continuously audit cloud objects – such as storage buckets – to ensure they comply with security policies.

When you consider the plethora of cloud applications we rely on for our 'everyday', this is a real concern. Think Hubspot or Salesforce for acquiring new customers, Dropbox for file sharing, or ChatGPT to enhance productivity. Every day, we are met with better ways to make us more efficient and grow our businesses. And AI is piling up the options for us.

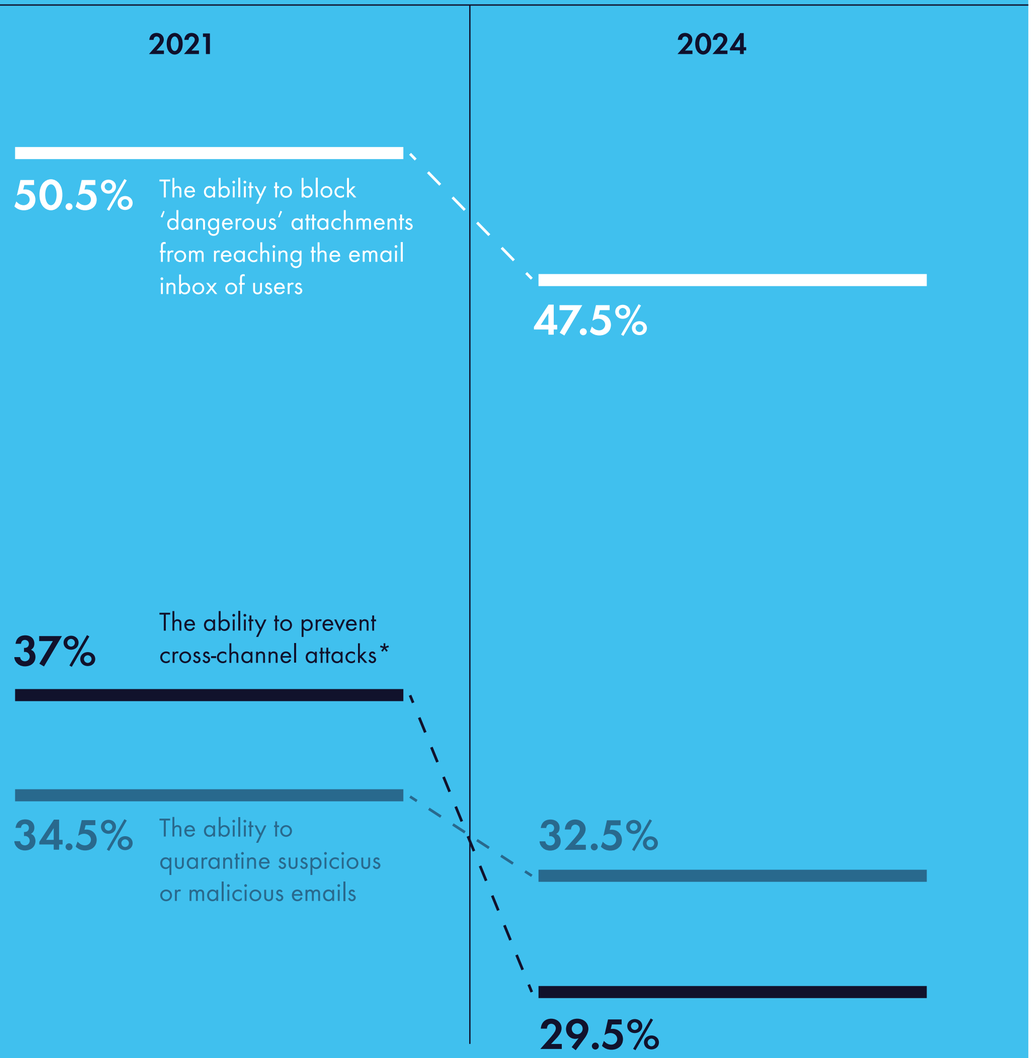
But the lack of security policies to say what's okay and what's not is getting SMBs into hot water. It either adds more unnecessary risk into the organisation, or prevents users from being productive.

So, is AI a lifeline? Or is it the crack that breaks the dam?

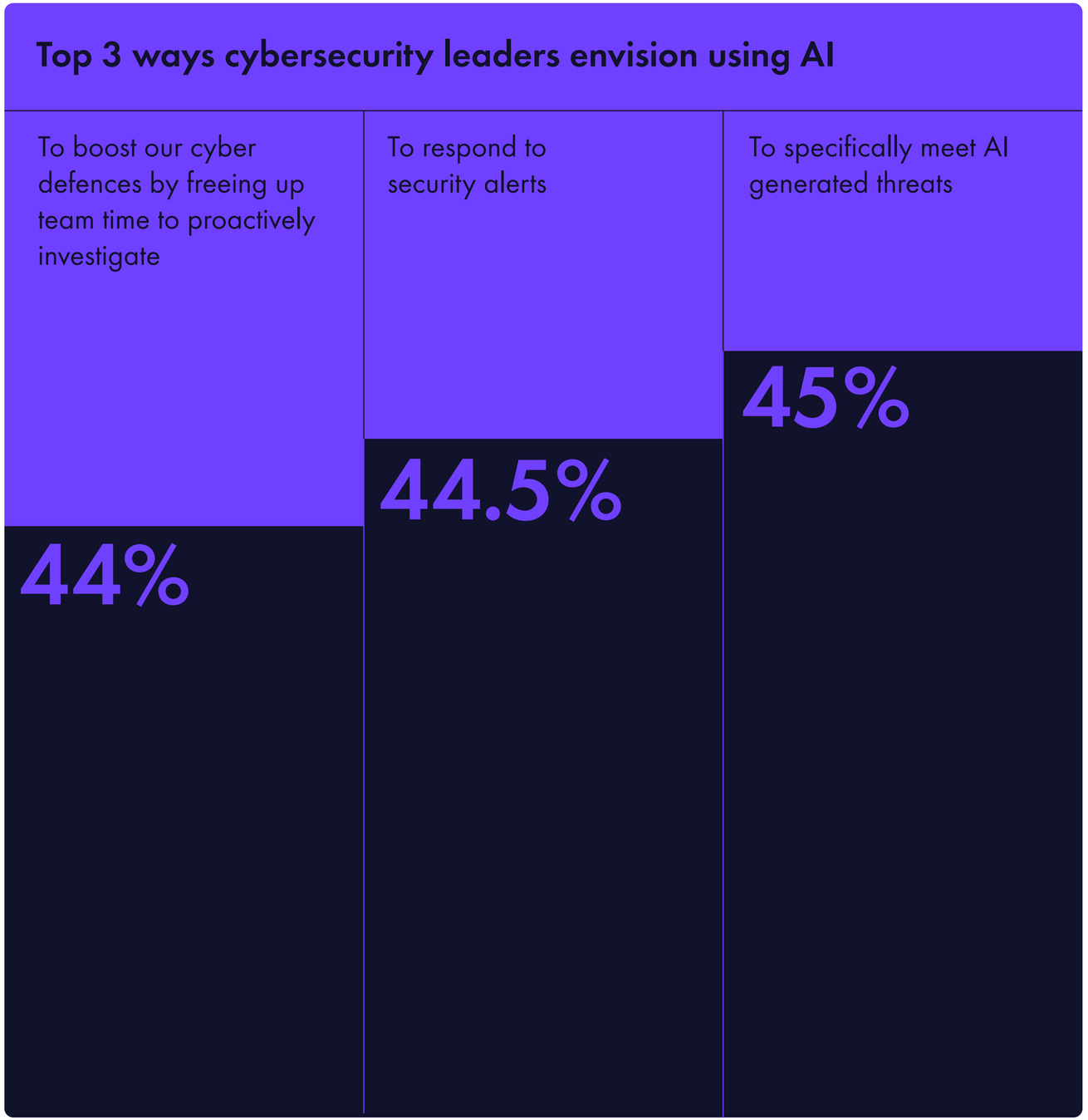
"Human error has the potential to undermine even the strongest defences. That's why education and training on best practices are crucial. Equipping your team with the skills needed to identify and prevent cyber attacks and data loss is essential for any business handling private and personal data."

Adam Hopper
Senior Account Manager | Focus Group

In the last 12 months, were you able to protect your organisation with the following?



*attacks that start via email, but continue over the web or cloud application channels if a user clicks on a link in the email message



07 AI's lifeline for the overwhelmed

It's time to address the elephant in the room: generative AI — seen by many as a magic pill.

The reality, of course, is slightly different. It's generative AI's cousin, AI, that continues to chart the direction of SMB security postures, both on the offensive and defensive fronts.

Here are the top three ways businesses expect to use AI in cybersecurity:

1. **AI-fuelled attacks and response**
   It's a classic double-edged sword: AI promises to give cybersecurity professionals breathing room, while it simultaneously arms attackers with next-gen tools to target them.

   It's a threat that is being felt most keenly in the private sector, where 56% said they expect to use AI in their response against new threats. In the public sector, only a quarter (26%) said the same.

2. **The AI-on-AI security alert warfare**
   The industry is already embracing AI in building cybersecurity defences and automating critical yet repetitive processes. It's music to the ears of the overwhelmed security professionals who face over 41 threat alerts each hour. 45% of them hope that they can use AI to respond to AI-generated security alerts in the future.

3. **Spare time to investigate and save costs**
   This use case is likely to manifest more over time, as AI-enabled defences become more widely available and more intelligent.

   44% of SMBs envisage that AI will be used in their cybersecurity defences to free up time to proactively investigate threats, and to help them prioritise the most dangerous-looking threats. But just 29% expect AI to help them reduce headcount and save money.

So, with high hopes for AI, how do we integrate the technology so it doesn't become another challenging pain point?

"Let's hope we have reached peak AI hype and can now move the conversation forwards to focus on tangible use cases such as AI's ability to revolutionise threat detection and response strategies."

Laurence Bentley
Head of Cyber Security | Core to Cloud

08 The AI Integration Puzzle

The prevalence of AI should mean that SMBs are prioritising the integration piece. After all, it is a topic that's been weighing heavy on their mind for some time. Yes, we are referring to the 22 cyber products each SMB typically needs to manage.

AI in cyber has already taken hold. 94% of businesses deployed more AI-powered cybersecurity technologies in the last 12 months, with 78% of security leaders feeling more secure knowing that AI-powered cybersecurity is defending their business against attacks.

The 'bulletproof' to the 'reasonably reassured'

Despite their relative caution in predicting future uses of AI, public sector respondents are more confident in the abilities of AI as a whole. 82% say they either have bulletproof confidence in it, or are reasonably reassured by it. In the private sector, this figure drops to 70%.

But when it comes to integration, over half of respondents have experienced issues integrating AI-powered cybersecurity technologies into their business. A lack of knowledge, issues with compatibility, and technical challenges are cited as the most common issues, especially as cybersecurity grows ever more complex.

In other words, the will is there but the reality is yet to catch up. We're dealing with bleeding-edge technology, and it's hard for both human skills and existing infrastructure to keep up with the speed of innovation – particularly given that AI has a habit of improving exponentially.

So, businesses will need to adopt a 'constant innovation' mindset in the coming years – committing to a continual cyber learning curve; the forever challenge of updating and improving their systems at a more rapid pace than ever before.

More crucially, they will need to solve the integration piece.

Simpler architecture, less complexity, and fewer point products is the future.

"Employees need to trust that their work environment is secured, wherever they operate. Reducing complexity, doubling down on simple architecture and harnessing AI-powered cybersecurity solutions is a core way to build a more human-centric cybersecurity experience – for both the IT team and employees across the organisation."

Dave Landreth
CTO - Network & Security | HybrIT Services

Top issues integrating AI-powered cybersecurity technologies

A lack of knowledge / trust of AI

28%

Compatibility and technical challenges with our existing products

28%

Integration is still in the planning stages

14.5%

INVESTMENT IN INTEGRATION

78%

plan to invest in an autonomous cloud-based security platform that allows security products to autonomously share security event and state data.

09 2024 outlook

The top challenges facing SMBs in the year ahead are twofold:

1. **The sheer number of cybersecurity point products they feel they need.**
2. **The cost and complexity of implementing all the technologies required.**

Reflecting this, SMBs' top wish is to bring automation and integration to cybersecurity, so they can benefit from round-the-clock protection. They are also increasingly calling for security vendors to open up traditionally closed point products to enable an automated response to cyber threats and attacks.

It's not hard to see why: in the last three years, the number of professionals who want to find a cybersecurity solution that means they don't need to worry about their organisation's security when they're trying to sleep has doubled.

It's why SMBs are considering how they can implement a consolidated security platform that's broad, comprehensive, autonomous, and deeply integrated. This is the direction of travel. And it's why 78% plan to invest in an autonomous cloud-based security platform in the next year.

Of course, it all comes at a cost. And cost prioritisation is paramount. For those looking to what their peers are doing: the top capabilities SMBs are investing in include data loss prevention, web, email, and cloud application protection. And their cybersecurity spending remains resilient – 85% of budgets are staying the same or increasing.

"The rapid growth of AI, the increasing complexity of cloud environments and the expanding potential attack surface creates additional openings for security vulnerabilities, misconfigurations, and exploits. Adopting a cybersecurity perspective that emphasises controls rather than merely tools will be essential for effectively managing technology estates."

Neil Langridge
Marketing & Alliances Director | e92plus

What are your biggest cybersecurity wishes for 2024?

10 Partnering with the best

As a 100% channel-led business, we have the pleasure of working with some of the best partners in the cyber industry.

Throughout this report, we have collaborated with industry leaders across our extensive partner network to share their insights on the challenges faced by security leaders in the UK. Find out a little more about the partners in this report:

"Partnerships are at the core of our business, and we proudly work with the best in the industry. The collaboration in this report makes clear the standard of thought leaders we partner with.

The rapid expansion of our partner programme clearly demonstrates the need for partner-friendly, affordable, integrated security. Demand for our autonomous platform has intensified and we're thrilled we can work with our partner network to help their customers to navigate the increasingly powerful threat landscape, taking the stress away from their overstretched staff. "

Charlie Milton
VP of Strategic Alliances | Censornet

TeT Limited

TET is a fast-growing IT reseller and service provider based in central London, providing solutions and services spanning Cybersecurity, Hybrid Infrastructure and Digital Transformation.

We partner with the best IT vendors to transform and simplify business operations by delivering game-changing insights and cutting-edge technology for private, public and governmental organisations.

Communicate

We are IT, telecoms and cyber-security specialists, keeping over 500 businesses and 50,000 users connected and secure across the UK.

Since 2011, we've been connecting organisations of all shapes and sizes; fast becoming one of the industry's leading internet service and managed security providers.

Our adaptable approach means clients can quickly and seamlessly add new services and users, offering flexibility to scale and integrate as you grow. From start-ups of two or three people to large corporate organisations and beyond, we've got you covered.

softwerx

With over 20 years' experience, Softwerx is one of the leading Microsoft Security Specialists in the UK. Our mission is to help Midmarket organisations throughout the UK and Europe better understand and leverage their existing Microsoft investment.

We do this by providing expert professional advice, consultancy and support on Microsoft infrastructure, security and licensing. Softwerx also operates a 24×7 'eyes-on' UK-based SOC, and our flagship MDR solution, secure365, is trusted by a number of well-known brands.

NGS

Award-winning NGS (UK) Ltd are independent, Next Generation Security trusted advisors, providing all-encompassing solutions from the perimeter to the endpoint.

NGS are recognised as thought leaders in the Next Generation Security marketplace and constantly research the threat landscape and how to protect their client's critical assets.

Delivering our managed, technical and professional services, our in-house experts work around the clock to do more, for less, better.

Qual
Empowering Technology

At Qual we offer a comprehensive range of IT Services to help our clients get the best from their technology stack.

We provide services to satisfy any organisations challenging IT decisions by listening and understanding their specific requirements and culture.

We provide an advisory and independent service founded on Cyber Security, Storage, Support and Procurement that is aligned to ensue any organisations expectations are exceeded.

focus
group

Our teams are experts in their field; passionate about finding the right solutions for you and committed to ensuring your business runs like clockwork.

We're by your side to keep your IT optimised, your business phone system at the top of its game, your data secure, your teams connected and your customers happy. At all times.

Whether you're an SME or global enterprise business; in the public sector, private sector or a charity...whatever your size, shape or service, we'll take the time to get to know your business and deliver the technology to fit the bill.

CORE TO CLOUD™

Core to Cloud is a multi-award-winning innovator in cutting-edge cybersecurity solutions and services. They support 200+ organisations, including over 50 NHS Trusts, GFK, and UCL.

Their mission is to protect their clients, not just by using security solutions but also through education and information. With a dedicated technical team and customer success, they can offer a holistic approach to Cyber Security.

They offer a consultative approach, identifying the gaps, implementing appropriate solutions, and offering ongoing and proactive support for their customers. Core to Cloud is delighted to work in partnership with Censornet.

hybrIT
services

HybrIT's team of IT experts share a passion for all things technology, delivering the best solutions, advice and outcomes for our customers.

We are made up of more than 100 seasoned professionals that are always moving forward, learning new skills and delivering cutting edge technologies.

The business is lead by a leadership team that hold a combined 125+ years experience in the industry, focusing on helping our staff thrive and love what they do.

e92plus

e92plus are the home of cybersecurity for the UK partner channel. Working with a range of industry leading technology vendors, we support a community of resellers, MSPs and specialist consultancies to help them protect their customers from the latest cyber attacks.

Providing a range of technical, commercial and enablement services, we help our partners grow their business and empower organisations to build, implement and optimise their cybersecurity strategy. From Application Security to Zero Trust, we're here for every cybersecurity journey.

About this report

The goal of our 2024 UK Cyber Resilience Report is to lay bare how SMBs' cyber readiness has been impacted by the events of the last three years. It sets out how SMBs fared under attacks in the last 12 months. And why IT leaders desire sophisticated and integrated security solutions.

The results represent the opinions of 200 IT leaders working in SMBs across the UK.

The research was conducted in partnership with market research specialist, 3Gem between 10th – 17th January 2024.

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Its AI-powered cloud security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed.

censornet.

www.censornet.com