TUDORVALE

Risk Report

The ESET 2026 SMB Cyber Risk Report

Smaller Businesses, Same Threats

SEPTEMBER 2026

Cybersecurity
Progress. Protected.

If organisations can't plug simpler security gaps before they are caught up in this brave new world of AI-powered, nation state-backed attacks, threat actors have an open invitation to breach UK SMBs and grind the nation to a halt.

Executive summary

UK SMBs are on the brink of a security shake up

Matt Knell, UK Country Manager, ESET

The British cybersecurity landscape could soon be unrecognisable for companies of every size. The NCSC is already warning UK Small and Medium-Sized Businesses (SMBs) could be caught in the crossfire of geopolitically-charged cyber threats, while powerful AI models can help threat actors to spot and exploit software vulnerabilities at scale, putting firms at greater risk of an incident.

Despite these looming threats, our study of 500 UK SMBs finds many are still struggling to lock down the basics. Half of them faced security incidents in the past 12 months, typically caused by simple tactics like phishing, known exploits, and weak passwords.

At the same time, a cyber skills crunch is making it harder for SMBs to recruit the talent they need – a problem that's feeling harder to address each year.

If organisations can't plug simpler security gaps before they are caught up in this brave new world of AI-powered, nation state-backed attacks, threat actors have an open invitation to breach UK SMBs and grind the nation to a halt.

The good news is British businesses have the means to fight back. With rising security budgets, robust cyber insurance offerings, and a wealth of MDR and MSP services available to help SMBs to stay secure, they have a golden opportunity to rethink their security strategy and bring in support before it's too late.

Key findings

AT LEAST 49% OF UK SMBS EXPERIENCED A CYBER INCIDENT LAST YEAR

55% EXPECT THEIR CYBERSECURITY BUDGETS TO INCREASE NEXT YEAR

86% OF UK SMBS DON'T OUTSOURCE AT LEAST PART OF THEIR CYBERSECURITY RESPONSIBILITIES VIA MDR OR AN MSP/MSSP

81% SAY CYBER WARFARE AND GLOBAL CONFLICTS ARE A VERY REAL CYBER THREAT THAT CAN IMPACT THEIR BUSINESS

THE MOST COMMON CAUSES OF AN INCIDENT WERE:

- Phishing
- Unpatched vulnerabilities
- Weak passwords
- A lack of monitoring

THE TOP CYBERSECURITY CHALLENGES SMBS FACE ARE:

- Keeping up with cybersecurity threats
- Keeping up with new technologies like AI
- Vulnerability and patch management
- A lack of skills

UK SMBs are a multi-trillion-pound target

Accounting for more than half of UK turnover in the UK private sector, or £2.8 trillion, SMBs are a pillar of the British economy, but also a prime target for threat actors. Increasingly, cybercriminals attempt to breach SMBs, gain access to systems, siphon off sensitive data, hold companies to ransom, and ultimately turn a profit.

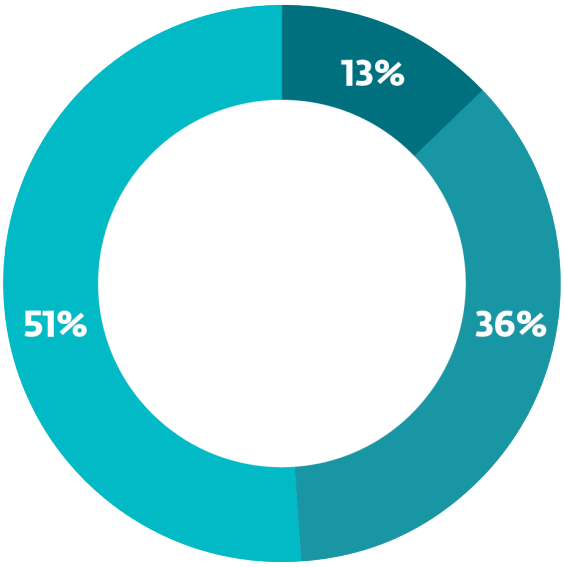
Unfortunately, many are succeeding.

Of those who experienced a security incident, 13% of respondents experienced several. This figure is higher for companies with higher endpoint counts, and those working in critical infrastructure.

The most common cause for an incident was phishing, followed by unpatched vulnerabilities, weak passwords, and lack of monitoring. This shows that simple attack techniques and a lack of basic security hygiene are still behind most SMB breaches. SMBs recognise this, as more than two-thirds (68%) say they are more vulnerable to attacks than larger enterprises.

While breaches are prevalent and caused by simple methods, SMB response time is in line with enterprise counterparts. On average, it took UK SMBs **just over four weeks** to identify and recover from a breach. Just 22% of respondents say it took over six weeks.

FIGURE 1: HAS YOUR ORGANISATION EXPERIENCED A CYBERSECURITY INCIDENT IN THE LAST 12 MONTHS?



Yes, more than one | Yes | Not that I know of

49%

Of UK SMBs experienced at least one cybersecurity incident last year

51%

Were not aware of an incident

The state of UK SMB security

With so many SMBs successfully hit by elementary attack methods, it's important to understand why these simple tactics are still working. The biggest cybersecurity challenges SMBs face (Fig. 2) are keeping up with the latest cybersecurity threats, keeping up with the latest cybersecurity technologies, vulnerability management, and a lack of cybersecurity skills and expertise.

Security posture still has room for improvement, as 54% of SMBs don't have advanced protection measures in place – namely a combination of endpoint protection, secure access for critical apps, security management tools and regular software updates. More than one-in-ten (11%) UK SMBs still rely on basic antivirus and built-in OS firewalls, which are frequently bypassed by modern malware strains.

Just over one-in-five (21%) UK SMBs have an internal Security Operations Centre (SOC) team, while 33% have a single dedicated cybersecurity specialist. For 32%, cybersecurity is part of an IT specialist's broader role.

Despite limited security headcount, skills shortages, and struggles to keep pace, **just 14% are outsourcing their security** via Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), or Managed Detection and Response (MDR) solutions. 11% partially outsource cybersecurity responsibilities to a third party, while 3% outsource all the responsibility.

FIGURE 2: WITHIN YOUR IT DEPARTMENT, WHAT DO YOU SEE AS THE THREE BIGGEST CHALLENGES WHEN IT COMES TO CYBERSECURITY?

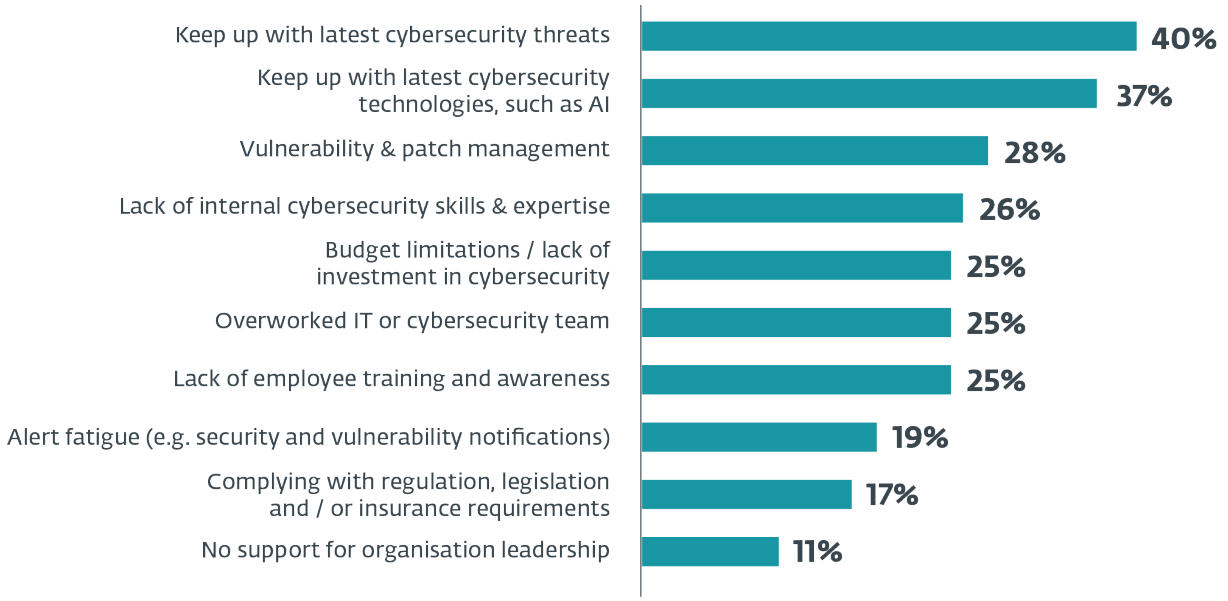
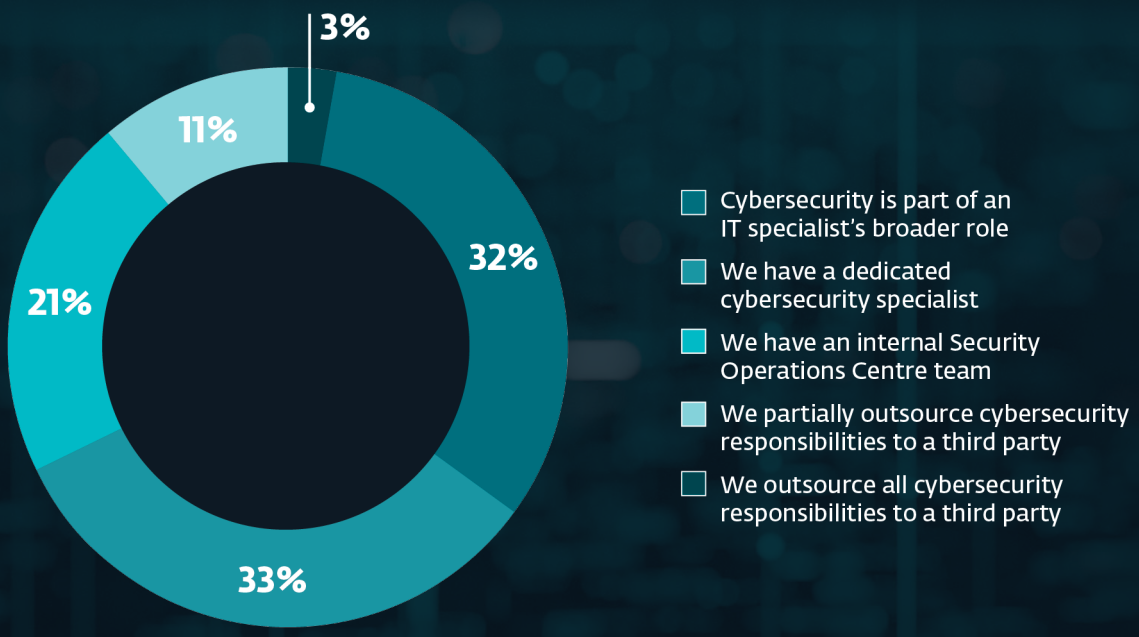


FIGURE 3: HOW IS CYBERSECURITY MANAGED IN YOUR ORGANISATION?



OF THE UK SMBS THAT OUTSOURCE AT LEAST SOME OF THEIR CYBERSECURITY RESPONSIBILITIES:

57%
Outsource security via an MSP/MSSP company

21%
Also use their Managed Service Provider for MDR

27%
Outsource security via a cyber insurer offering MDR

16%
Outsource security via a vendor offering MDR

When selecting a partner for outsourced security, SMB's key priorities are strong services support and consulting (44%), followed by product functionality & performance (43%). Also, as concerns around sovereignty mount, UK organisations strongly prefer UK or European-based providers and server locations.

Approaching a cyber cliff edge

In a quickly evolving cyber threat lansdcape, two-thirds (67%) of UK SMBs fear a cyberattack in the next year. This figure is even higher for SMBs who have experienced a breach, those in the critical infrastructure sector, and those with more endpoints.

If breached, firms fear data loss (48%), financial loss (42%), operational disruption (40%), and a loss of customer confidence and trust (40%).

SMBs acknowledge that nation-state backed attacks are now aimed at disrupting businesses of all sizes. 81% of security decision makers say cyber warfare and global conflicts are a very real cyber threat that can impact their business.

When asked about the specific security threats they worry about, respondents are most concerned about AI-powered malware (32%), ransomware and malware (28%), and cloud computing threats (26%).

As worries around AI and cybersecurity grow – SMBs are having to adapt quickly. More than four-in-five UK SMBs (83%) say they are integrating AI applications into their organisations, while seven-in-ten (69%) admit that AI introduces new risks.

In response to security and privacy risks, 69% of UK SMBs have an AI policy in place to restrict the use of AI applications outside of approved processes or platforms. When it comes to integrating AI into cybersecurity strategies, the primary goals involve using AI to anticipate threats and improve attack mitigation.

IF BREACHED, FIRMS FEAR:

48%
Data loss

42%
Financial loss

40%
Operational disruption

40%
Loss of customer confidence and trust

Healthy budgets put towards employee training and cloud security

Despite rising security risks and skills shortages, 88% of UK SMBs find budgets adequate or more than sufficient. There is also good news on the horizon, as 55% expect a budget increase in the next year – which will help to plug security gaps and address emerging threats.

The top investment priority for UK SMBs this year is employee training & awareness (48%).

Virtually all (94%) UK SMBs consider training critically or very important. They are focusing on phishing simulations (46%) and comprehensive awareness training (36%) for their employees. SMBs who have experienced incidents in the past are more likely to carry out security training.

When it comes to frequency, three-in-five (59%) train several times a year, and a further one-in-five (21%) at least once a year. Training was most frequent in SMBs working in the critical infrastructure sector and in SMBs who had experienced a breach.

To maximise the impact of cyber awareness training, organisations should build a Human Risk Management (HRM) programme focusing on engagement, context and reinforcement. This should feature real-life scenario simulations and gamification to educate employees, bolster resilience, and ensure compliance with cyber insurance requirements. Find out more about ESET's approach to Cybersecurity Awareness Training here.

The second highest investment priority is cloud security (43%), as threat actors go beyond email threats to target business cloud solutions such as OneDrive or SharePoint.

Organisations can't rely on email and web security alone. In 2025, on top of native protection in Microsoft 365 and Google Workspace, ESET Cloud Office Security detected and blocked threats that other solutions missed, providing an extra layer of defence against sophisticated and evasive attacks.

- 1,300,000 email threats detected
- 3,000,000 phishing emails blocked
- 200,000,000 spam emails captured
- 600,000 non-email threats originated from OneDrive, SharePoint, Teams, and Google Drive

Insurance – a growing influence on SMB security

When dealing with risk and compliance, cyber insurers are playing a more important role than ever in UK SMB cybersecurity. After experiencing an incident, 95% of UK SMBs report their breaches – but more than half (52%) are reporting them to their insurer while just 36% reported to a regulator.

82% of UK SMBs now carry cyber insurance – a figure which rises to 90% of larger SMBs (companies with 500-1000 endpoints). Unsurprisingly, adoption is even higher for firms that have already experienced an attack, rising to 92% for SMBs who experienced an incident in the past 12 months, and 94% for those who experienced multiple incidents.

Insurers are also working with cybersecurity vendors to offer tailored protection to customers through solutions like Managed Detection and Response programmes while reducing the risk of a breach.

> "Good cybersecurity and effective cyber insurance should work hand in hand. Organisations are increasingly looking at cyber risk as a business issue rather than simply an IT issue, and that requires a combination of prevention, resilience and specialist insurance support."

Tim Wiltshire, Director, Acrisure UK

From a prime target to a prevention-first SMB

SMBs can't think of cybersecurity as an afterthought when they are constantly targeted by ransomware, phishing, zero-day threats and targeted attacks.

But, as security budgets are set to rise, now is the perfect time for SMBs to revisit security fundamentals and nail the basics, bolstering against common attacks while preparing for the future.

This means taking the time to accurately assess their security posture and build a plan to improve resilience and build prevention-first security based on their needs.

HERE ARE FIVE STEPS TO KICK OFF THE PROCESS:

STOP AND TAKE STOCK

Too many businesses are still being hit by phishing, known vulnerability exploits, and weak passwords – when was the last time security practices and cyber awareness training was reviewed?

SEEK EXPERT GUIDANCE

Speak to security experts to better understand incoming threats such as AI-powered malware and nation-state backed attacks

GET BUY-IN FROM LEADERSHIP

Talk to your business leaders and educate them on the growing importance of cyber resilience as the chances of a breach continue to rise

HARNESS AI WHILE BALANCING FINITE RESOURCES

Build AI into cybersecurity without breaking the bank, selecting best in class SMB security tooling that balances AI with human expertise, offering effortless supervised cybersecurity

BUILD IN 24/7 PROTECTION

Bolster the businesses' protection against a constant barrage of cyber threats without maintaining in-house security specialists through outsourcing via MDR or via MSPs

Always On.
Always Protected.

ESET offers proactive cybersecurity for endpoints, email, and cloud that defends your organisation against ransomware, phishing, and zero-day attacks.

SECURE YOUR BUSINESS NOW:

GET A QUOTE

BUY ONLINE (UP TO 99 DEVICES)

LEARN HOW ESET'S MANAGED DETECTION & RESPONSE OFFERING HAS BEEN A SECURITY LIFELINE TO BOURNEMOUTH AFC BELOW:

"Having access to ESET's 24x7x365 monitoring and expertise gives us an extra layer of confidence without the significant investment and operational overhead that comes with building and staffing an around-the-clock security capability ourselves. It allows our team to focus on supporting the business while knowing our endpoints are continuously monitored."

Stefan Du Plooy, Head of IT at AFC Bournemouth

METHODOLOGY:

This research was commissioned by ESET and carried out by Go4insight, surveying cybersecurity decision makers at 500 UK SMBs (organisations with 25-1000 endpoints) in February 2026.

TUDORVALE

For more information please contact,
Andrew Jones
CEO
Tudorvale Limited
Phone: +447802287738
Email: aj@tudorvale.com

Cybersecurity
Progress. Protected.