TRANSCRYPT

The State of UK SME Cybersecurity 2025

Annual Report · Threat Landscape, Compliance & Resilience

A data-driven analysis of the cyber threats, vulnerabilities and compliance challenges facing the United Kingdom's 5.5 million small and medium-sized enterprises — with practical guidance for building genuine resilience in 2025 and beyond.

Published: February 2025 · Version 1.0
transcrypt.xyz

Contents

01 Executive Summary

The cyber threat landscape facing the United Kingdom's small and medium-sized enterprises has never been more challenging. In the twelve months covered by this report, 43% of UK businesses reported experiencing some form of cyber breach or attack — equating to approximately 612,000 organisations. For medium-sized firms, the figure climbed to 70%, and for large enterprises, 74%.

Phishing remains the dominant attack vector, responsible for 85% of business breaches, while ransomware incidents doubled year-on-year, with approximately 19,000 businesses now affected. The NCSC handled 204 nationally significant incidents in its 2024–25 reporting period — a 130% increase over the previous year — and described the widening gap between threats and national defences as the defining challenge of this era.

Encouragingly, small businesses are beginning to respond. Cyber insurance uptake among SMEs rose to 62% (from 49% the prior year), risk assessments increased to 48% (from 41%), and formal security policies are becoming more commonplace. Yet critical gaps persist: only 27% of businesses have board-level ownership of cybersecurity (down from 38% in 2021), only 14% review the risks posed by their immediate suppliers, and fewer than 1% of the UK's 5.5 million businesses hold Cyber Essentials certification.

This report examines the key threats, emerging trends, compliance shifts and practical measures that every SME leader needs to understand in 2025. The message is clear: cybersecurity is no longer an IT problem. It is a matter of business survival.

43%
of UK businesses experienced a cybe
2024

85%
of breaches involved phishing attacks

2x
increase in ransomware incidents year-on-year

612K
businesses reported cyber incidents

<1%
of UK businesses hold Cyber Essentia

204
nationally significant NCSC incidents handled

02 The UK SME Landscape: Scale and Significance

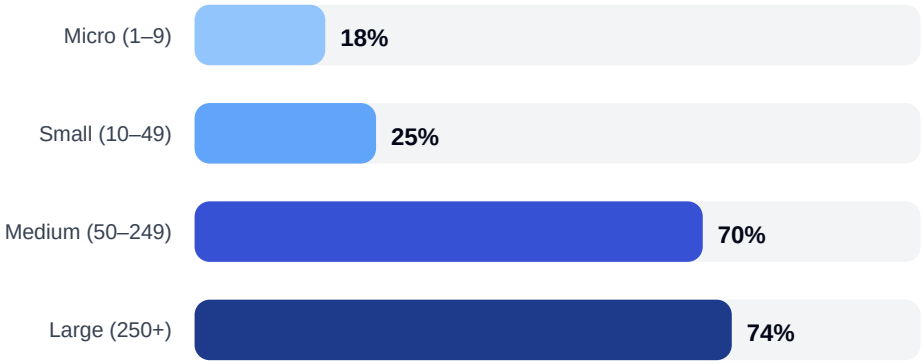
Small and medium-sized enterprises are the backbone of the British economy. The UK is home to approximately 5.5 million businesses, and the overwhelming majority — over 99% — are classified as SMEs (fewer than 250 employees). They collectively employ around 16.7 million people and generate roughly half of private sector turnover.

The digital transformation of these businesses has accelerated markedly since 2020. Cloud adoption, remote and hybrid working, and reliance on digital supply chains have become standard operating practice. Yet the security infrastructure underpinning this transformation has not kept pace. Most SMEs lack dedicated cybersecurity personnel, operating instead with general IT support or, in many micro-businesses, with no formal IT function at all.

This mismatch — increasing digital exposure combined with limited security resources — is precisely what makes SMEs attractive targets. Cybercriminals are rational actors: they seek maximum return for minimum effort.

> *"81% of all UK cybersecurity attacks and data breaches happen to SMEs. Yet 97% of those attacks could have been prevented with modern, comprehensive cybersecurity measures in place."*

Breach Rate by Business Size



Source: DSIT / Home Office Cyber Security Breaches Survey 2025.

03 Threat Landscape Overview

The NCSC's Annual Review 2025 described the UK's cyber threat environment in stark terms: four nationally significant attacks per week, a 130% year-on-year increase in the most severe incidents, and a growing gap between the capabilities of threat actors and the defences of most organisations.

Commoditisation of Cybercrime

Ransomware-as-a-Service (RaaS) has lowered the barrier to entry for aspiring cybercriminals. Platforms offering ready-made ransomware kits, complete with customer support and revenue-sharing models, mean that technically unsophisticated actors can now mount devastating attacks. The RaaS market is estimated at $2.5 billion globally in 2025. The DragonForce attacks on M&S and the Co-op illustrate how these criminal enterprises operate at scale.

State-Sponsored and Geopolitical Threats

The NCSC identified persistent activity from state-backed actors linked to China (Flax Typhoon), Russia (Authentic Antics malware), Iran (critical infrastructure attacks), and North Korea (fake IT worker scams). While primarily targeting government and defence, their techniques cascade to criminal groups targeting SMEs in connected supply chains.

Figure 1: UK Cyber Threat Severity Matrix. Bubble size indicates relative severity; position shows prevalence (x-axis) versus business impact (y-axis).

04 Phishing: The Persistent Frontline

Phishing remains the single most prevalent cyber threat facing UK businesses, responsible for 85% of all breaches and 93% of all cyber crimes against businesses. It is the attack method that causes the most operational disruption — not because individual emails are necessarily devastating, but because of the sheer volume and the investigative effort each incident demands.

Why Phishing Works Against SMEs

Phishing exploits human psychology, not technical vulnerabilities. Staff are often wearing multiple hats and working under time pressure. Only 34% of small businesses reported providing any cybersecurity awareness training in the past twelve months. Attackers impersonate trusted contacts, create artificial urgency, and leverage social engineering to coax employees into clicking malicious links or entering credentials on spoofed pages.

Business Email Compromise (BEC)

A particularly damaging variant where attackers impersonate a CEO, supplier or financial contact to request fraudulent payments. Common scenarios include fake invoice redirections and supplier bank detail changes. These bypass technical controls because the email contains no malware — just a convincing request. UK SMEs collectively lose an estimated £3.4 billion per year to inadequate cybersecurity, with BEC contributing a significant share.

> *"Phishing persists as the top threat because people are often the first line of defence. No security tool can perfectly filter out every convincing phishing email."*

What Effective Defence Looks Like

Organisations that conduct monthly cybersecurity training see a 70% decrease in employee errors. 41% of SMEs now use simulated phishing tests. The most effective approach combines technical controls (email filtering, DMARC) with regular staff awareness training and clear escalation procedures.

05 Ransomware: An Escalating Menace

Ransomware remains one of the most acute threats to UK organisations. The proportion of businesses reporting a ransom demand doubled — from under 0.5% to 1%, translating to approximately 19,000 affected organisations. The NCSC managed 20 significant ransomware incidents, with 13 classified as nationally significant — a threefold increase.

The retail attacks by DragonForce on Marks & Spencer, the Co-op and Harrods brought ransomware into public consciousness, with empty shelves serving as a stark reminder of operational impact. For every high-profile case, hundreds of SME incidents go unreported.

The Double and Triple Extortion Model

Modern ransomware attacks go beyond encryption. Attackers exfiltrate data before encrypting, threatening publication if unpaid (double extortion). Some contact victims' customers directly (triple extortion). For SMEs handling client data — legal firms, accountants, healthcare providers — reputational damage can exceed direct financial cost.

Government Response

In July 2025, the UK Government signalled intent to ban ransom payments for public sector bodies and CNI operators, alongside broader incident reporting requirements. For SMEs in public sector supply chains, demonstrable resilience is becoming a contractual necessity.

19K
UK businesses affected by ransomwa

70%
year-on-year increase in ransomware

£10K
average cost of cyber-facilitated fraud

06 AI-Powered Threats and Defences

Artificial intelligence is reshaping cybersecurity on both sides. For attackers: more convincing phishing, deepfake audio/video for impersonation, and automated vulnerability scanning at scale. For defenders: enterprise-grade capabilities — automated threat detection, anomaly analysis, behavioural monitoring — becoming accessible to smaller organisations.

The Threat Dimension

35% of UK SMEs now consider AI-generated attacks their top cybersecurity concern. 69% of cybersecurity professionals globally report AI-enhanced attacks as their primary worry. AI tools can generate phishing emails virtually indistinguishable from legitimate communications, create realistic voice clones, and automate exploitation of known vulnerabilities far faster than human attackers.

The Defence Opportunity

Defensive AI is becoming practical for SMEs, typically through managed services or integrated platforms. Key applications include automated email threat analysis, behavioural monitoring for unusual patterns, intelligent vulnerability prioritisation, and AI-assisted policy generation that translates complex compliance requirements into actionable tasks.

> *"AI is a double-edged sword. The key for SMEs is ensuring AI works as an assistant — removing toil and spotting gaps — not as a replacement for deterministic security checks."*

07 Supply Chain Vulnerabilities

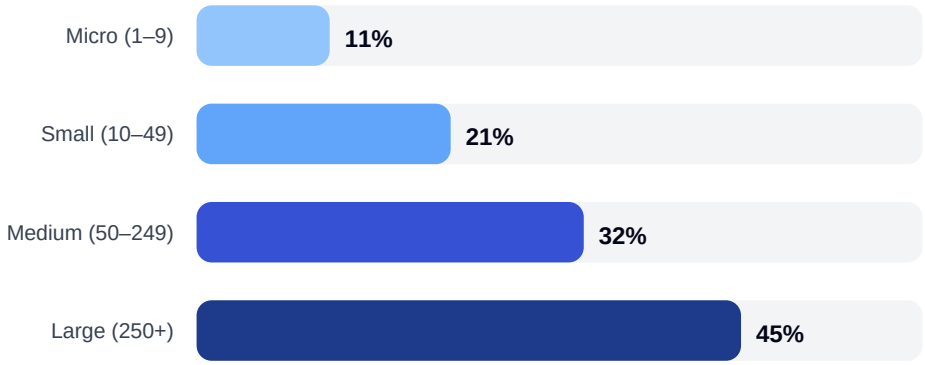
Supply chain attacks represent one of the fastest-growing threat categories. In 2025, an estimated 62% of cyber intrusions originated from third-party suppliers, and over half of organisations reported a supplier-related breach. In financial services, over 50% reported at least one supply chain attack in 2024.

Despite this, formal supply chain risk management remains rare. Only 14% of businesses review the risks posed by their immediate suppliers, and just 7% assess their wider supply chain. The NCSC's 2025 Annual Review explicitly called on large organisations to encourage suppliers to achieve Cyber Essentials.

Why SMEs Are the Weak Link

Modern supply chains are deeply interconnected. A vulnerability in one small supplier can cascade through an entire network. The Synnovis ransomware attack on the NHS demonstrated how a single supplier compromise can disrupt critical services across a sector.

Supply Chain Risk Review by Business Size



Source: DSIT Cyber Security Breaches Survey 2025.

08 The Cost of a Breach

Quantifying cyber incident costs is complex, as many impacts are indirect or delayed. The DSIT Breaches Survey 2025 provides the most authoritative UK-specific data.

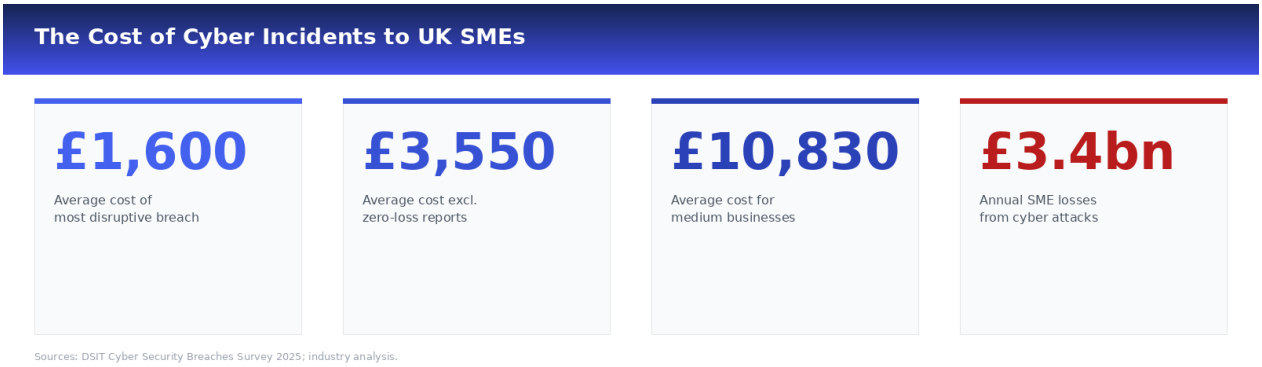


Figure 2: The cost of cyber incidents to UK SMEs across different measurement approaches.

Beyond the Immediate Financial Impact

67% of small businesses experiencing a cyber attack reported financial difficulties within six months. Businesses reported a significant increase in temporary loss of access to files or networks (7%, up from 4%). For many SMEs, reputational damage — lost client trust, damaged supplier relationships, regulatory scrutiny — can exceed direct financial cost.

The Insurance Gap

Cyber insurance uptake among small businesses has risen to 62%, up from 49%. However, 38% of small businesses still have no coverage. Insurers increasingly recognise Cyber Essentials as a positive risk signal, with some offering reduced premiums for certified organisations.

09 The State of SME Cyber Hygiene

One of the more encouraging findings is measurable improvement in basic cyber hygiene among UK small businesses. While significant gaps remain, the direction of travel is positive.

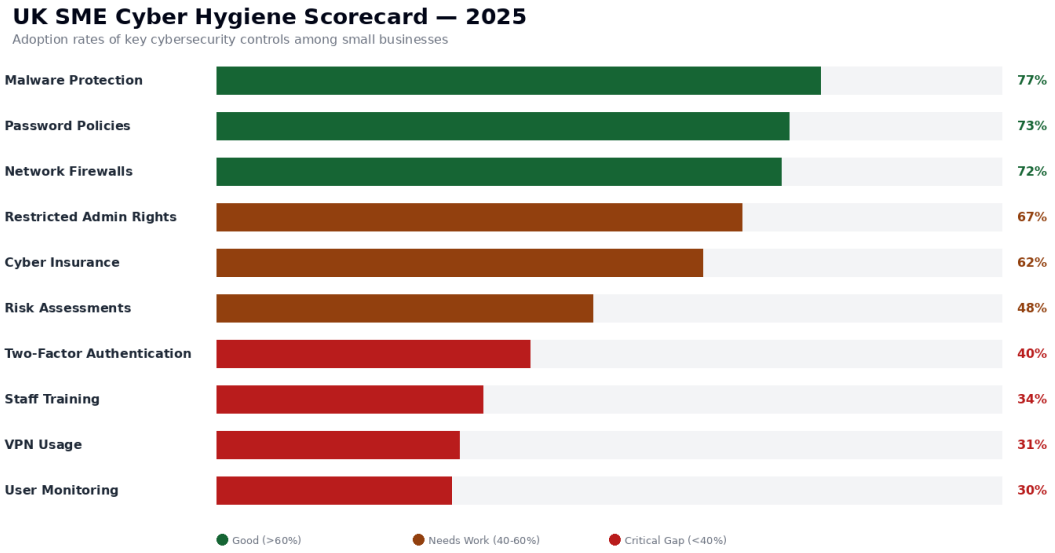


Figure 3: UK SME Cyber Hygiene Scorecard showing adoption rates of key controls. Green = good adoption (>60%), amber = needs work (40–60%), red = critical gap (<40%).

Key Year-on-Year Improvements

Cyber insurance uptake: 62%, up from 49% — a 13 percentage point increase

Risk assessments: 48%, up from 41% — a 7 percentage point increase

Formal security policies: Significant year-on-year increase reported

Business continuity planning: Growing adoption noted

Persistent Weaknesses

Two-factor authentication is deployed by only 40% of businesses. Staff training by just 34%. Board-level responsibility has declined to 27%. These are precisely the controls that Cyber Essentials is designed to address.

10 Cyber Essentials: Progress and the Gap

Cyber Essentials is the UK Government's flagship cybersecurity certification, focusing on five core technical controls: firewalls, secure configuration, access control, malware protection, and security update management.

Figure 4: The Cyber Essentials certification gap — visualising the scale of the challenge.

Evidence That It Works

A UK Government report in October 2024 confirmed that Cyber Essentials has demonstrably positive impact. The NCSC describes it as "an evidence-based intervention that we know can make organisations more resilient." It protects against up to 80% of common threats, and certified organisations consistently report fewer incidents and improved stakeholder confidence.

The April 2025 Update

Requirements version 3.2 tightened MFA expectations, mandated high/critical vulnerability fixes within 14 days, and required removal of end-of-life software. These changes ensure Cyber Essentials remains a meaningful baseline.

11 Regulatory Horizon: What's Coming

The UK's regulatory approach is shifting from guidance-led to enforcement-led. Several significant policy developments in 2025 signal a new era of accountability.

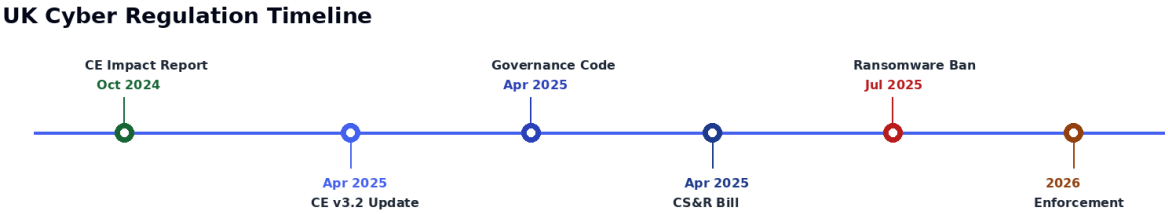


Figure 5: Key regulatory milestones shaping the UK cyber landscape from 2024 to 2026.

Cyber Security and Resilience Bill

Introduced in 2025, aligned with the EU's Cyber Resilience Act, setting minimum cybersecurity requirements for digital products, software and connected services. For SMEs, clients and partners will increasingly require demonstrable security maturity as a condition of doing business.

Cyber Governance Code of Practice

Published April 2025, establishing board-level expectations for cybersecurity governance. Encourages a named board-level individual responsible for cyber risk, structured frameworks, and regular senior reporting.

Ransomware Payment Restrictions

The July 2025 proposals signal a ban on ransom payments for public sector and CNI operators, plus broader reporting requirements. For SMEs in public supply chains: if you cannot pay a ransom and lack tested backups, a ransomware attack could be business-ending.

12 Building Resilience: Practical Recommendations

Cybersecurity for SMEs does not require an enterprise budget. Getting the basics right prevents the overwhelming majority of attacks.

01 Achieve Cyber Essentials Certification

The single most impactful step. Establishes a baseline of five core controls protecting against up to 80% of common threats. Consider upgrading to CE Plus for independent verification.

02 Implement Multi-Factor Authentication Everywhere

MFA dramatically reduces credential-based attacks. Deploy across email, cloud services, remote access and any system holding sensitive data. Prefer passwordless where available.

03 Train Your People — Regularly

Monthly training reduces employee errors by 70%. Simulated phishing exercises build muscle memory. Make security everyone's responsibility.

04 Patch Within 14 Days

Apply high/critical vulnerability fixes within 14 days, per CE v3.2. Remove end-of-life software. Automate patching where possible.

05 Back Up and Test Your Backups

Maintain offline or immutable backups. Test restoration regularly — an untested backup is not a backup. Your last line of defence against ransomware.

06 Review Your Supply Chain

Ask suppliers about their cybersecurity. Consider requiring Cyber Essentials from key suppliers. You are only as secure as your weakest link.

07 Get Cyber Insurance

With uptake at 62% among small businesses, it's becoming standard. Provides financial protection and access to incident response expertise.

08 Assign Board-Level Responsibility

Nominate a senior leader accountable for cybersecurity. Use the Cyber Governance Code of Practice. Schedule quarterly reporting. What gets measured gets managed.

13 Methodology and Sources

This report synthesises data from multiple authoritative sources. No proprietary Transcrypt customer data is included.

Primary Sources

• DSIT / Home Office Cyber Security Breaches Survey 2025 — quantitative data from ~2,180 businesses, gathered August–December 2024.

• NCSC Annual Review 2025 — threat assessment covering September 2024 to August 2025.

• NCSC / IASME Cyber Essentials Statistics — quarterly certification data, including 2024–25 annual figures.

• UK Government Ransomware Proposals Response (July 2025) and Cyber Governance Code of Practice (April 2025).

• Cyber Security and Resilience Bill (2025).

Supplementary Sources

• Verizon 2025 Data Breach Investigations Report (DBIR)

• IBM 2025 Cost of a Data Breach Report

• Bionic SME Insights Report 2025 (500 UK SME owners)

• Industry analysis from ramsac, CyberSmart, Focus Group, ANSecurity

Limitations

Survey-based data is subject to self-reporting bias and variation in detection capability. Cost figures should be treated as indicative. Where sources conflict, we have prioritised DSIT data as the most methodologically rigorous UK-specific dataset.

This report was compiled by Transcrypt, a UK-based cybersecurity and compliance platform built specifically for SMEs. Transcrypt automates the process of achieving Cyber Essentials and other security standards — translating complex frameworks into plain-English tasks.

transcrypt.xyz