stryke.

The Threats Haven’t Changed. The Stakes Have.

A Cyber Security Retrospective and Outlook for 2026

A Cyber Security Retrospective and Outlook for 2026

A new year brings fresh momentum for most businesses. Cyber threats, however, don't reset with the calendar. The risks UK organisations faced in 2025 have evolved, becoming more commercialised, more automated, and often easier to exploit.

For UK SMBs, the story of 2025 was clear. Attackers continued to focus on the fastest route to money: people, passwords, and payments. They increasingly combined traditional tactics such as phishing and impersonation with modern tooling, including artificial intelligence, infostealers, and stolen session tokens.

The UK Government's latest national research found that 43% of UK businesses reported experiencing a cyber security breach or attack in the previous 12 months.[1] For those organisations, phishing remained the most prevalent and disruptive type of incident.

Our 2026 Cybersecurity Retrospective looks back at the threats that shaped 2025 and outlines what UK SMBs should prioritise to stay protected in 2026, without overcomplicating security or overbuying technology.

43%

of UK businesses reported experiencing a cyber security breach or attack in the previous 12 months[1]

1 UK Government Cybersecurity breach survey

2025's Dominant Cyber Threats

Cybercriminals continued to professionalise throughout 2025, operating less like opportunistic hackers and more like structured, profit-driven organisations. Attacks are no longer limited to highly technical individuals working in isolation. Instead, a mature criminal economy now exists where malware, phishing kits, stolen credentials, and access to compromised systems can be bought and sold with ease. In many cases, these services are accompanied by user guides, regular updates, and even customer support.

This growing marketplace has significantly lowered the barrier to entry for attackers. Individuals with limited technical ability can now launch sophisticated campaigns by combining readily available tools with proven social engineering techniques.

For UK SMBs, this has resulted in a noticeable increase in both the volume and quality of attacks, with criminals able to move faster, scale more easily, and adapt their methods with minimal effort.

Throughout 2025, attackers increasingly blended familiar techniques such as phishing, impersonation, and credential theft with modern tooling, including artificial intelligence, automated malware, and identity-focused attack methods. **Rather than exploiting complex technical vulnerabilities, many incidents relied on manipulating people, abusing trusted access, and exploiting gaps in basic security controls.**

What we continue to see at Stryke across the UK SMB market is a worryingly high number of organisations that lack some of these fundamental controls. In many cases, the measures missing are basic but highly effective, and when implemented correctly, can significantly reduce exposure to common cyber attacks. Through our day-to-day work supporting businesses to become more secure and resilient, we have learned (and seen first-hand) that attackers show no conscience or discretion when choosing their targets. **Regardless of the type of business you operate, your employee headcount, or your turnover, you are still a target.**

At the same time, we have seen a notable increase in the adoption of managed cyber security services across the UK SMB market. For many organisations, this reflects a recognition of the cyber skills gap and the challenge of maintaining effective security controls alongside day-to-day IT responsibilities. Managed services help address this gap by providing continuous protection and expertise, while freeing internal IT teams to focus on supporting the business in a more proactive, strategic, and innovative way.

Alongside this shift, it has become increasingly clear that the days of relying on isolated point solutions are coming to an end. Layering multiple disconnected tools often introduces unnecessary complexity, increases the operational burden on IT teams, and ultimately creates larger security gaps rather than closing them. **A more integrated, managed approach is now essential to reduce complexity, improve visibility, and deliver meaningful cyber resilience.**

As a result, organisations increasingly find themselves in an ongoing cycle of prediction and response, attempting to stay ahead of threats that continue to evolve in speed, frequency, and impact. The trends observed during 2025 reinforce a clear message: while the tools and tactics may change, attackers will consistently pursue the simplest and most reliable path to financial gain. To counter this, organisations must adopt security strategies that are adaptive, resilient, and grounded in real-world risk.

Here's a recap of some of the top threats that we have seen in 2025, which will remain highly relevant in 2026:

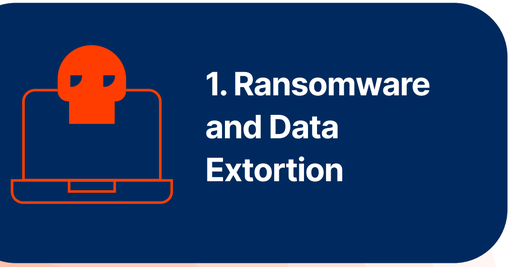
1. Ransomware and Data Extortion

3. Credential Theft, Infostealers and Session Token Abuse

2. Phishing, Impersionation, and Business Email Compromise (BEC)

4. AI Enabled Social Engineering and Deepfake Fraud

Threats likely to continue into 2026:



Ransomware and Data Extortion

Ransomware remained one of the most damaging cyber threats in 2025, but with a clear and important evolution in how attacks are carried out. While traditional ransomware relied on encrypting systems to cause disruption, many criminal groups now prioritise stealing sensitive data and extorting victims without necessarily encrypting systems at all. This shift allows attackers to operate more quietly, reduce the risk of early detection, and apply pressure through the threat of data exposure rather than system downtime. For victims, this often results in complex legal, regulatory, and reputational consequences, even when core systems remain operational.

This evolution also reflects a maturing cybercrime economy. Data theft and extortion can be faster to execute, easier to scale, and just as profitable as traditional ransomware campaigns. In some cases, attackers combine both methods, encrypting systems and simultaneously threatening to publish stolen data if demands are not met. For UK organisations, particularly SMBs with limited internal security resources, this creates a broader, more persistent risk extending beyond simple system recovery.

The UK National Cyber Security Centre continues to describe ransomware as one of the most acute and pervasive threats facing UK organisations, highlighting its ongoing impact across both the public and private sectors. The NCSC consistently advises that organisations of all sizes remain at risk and should prioritise preventative controls, resilience, and recovery planning to reduce the likelihood and impact of an attack.[2]

Why it won't go away: It still works. Criminals only need a single weak point, such as a compromised account, exposed remote access, a vulnerable supplier, or one clicked link, to create operational disruption and financial pressure.

2 UK National Cyber Security Centre, Annual Review and ransomware guidance

2. Phishing, Impersionation, and Business Email Compromise (BEC)

Phishing, Impersionation, and Business Email Compromise (BEC)

Phishing remained the most common cyber security issue affecting UK organisations in 2025, and it is no longer limited to obviously suspicious emails. Attacks increasingly involve impersonation, invoice fraud, and supplier or payment deception, delivered via email, Microsoft Teams, WhatsApp, and phone calls.

A growing number of these incidents involve the compromise of legitimate business email accounts. Once attackers gain access to a trusted mailbox, they can impersonate employees or suppliers, monitor conversations, and insert fraudulent payment instructions at precisely the right moment, making detection far more difficult.

The UK Government's 2025 Cyber Security Breaches Survey that we mention at the start of this publication found that, among organisations that experienced a breach or attack, phishing was the most prevalent and disruptive type of incident, affecting the majority of victims.

Why it won't go away: Phishing and impersonation targets and exploits human behaviour rather than technical weaknesses. They are cheap to run, easy to scale, and highly effective in fast-paced, trust-based working environments. As long as approval processes remain informal and decisions are made under pressure, these attacks will continue to succeed.

3. Credential Theft, Infostealers and Session Token Abuse

Credential Theft, Infostealers and Session Token Abuse

Attackers are not always breaking in, they are logging in. A defining feature of 2025 was the growth of identity driven attacks. A common attack chain now involves tricking a user, stealing credentials or session tokens, accessing Microsoft 365 or other cloud applications, moving quietly within the environment, and monetising access through fraud, extortion, or data theft.

Microsoft's Digital Defense Report highlights the rise of token theft, where attackers steal authentication tokens to access accounts without needing a password, and the growing role of infostealers in harvesting credentials and session data for resale in the cybercrime economy.[3]

For UK SMBs, the impact of this type of compromise can be severe. A single mailbox takeover can lead to invoice diversion. Access to SharePoint or OneDrive can result in large scale data theft, and a compromised administrator account can expose the entire Microsoft 365 tenant.

Why it won't go away: Cloud adoption is now universal and identities have become the primary entry point. Attackers will continue to invest where the return is highest, and that return is access.

3 Microsoft's Digital Defense Report

4. AI Enabled Social Engineering and Deepfake Fraud

AI Enabled Social Engineering and Deepfake Fraud

When "it looks and sounds right" is no longer full proof. During 2025, AI-driven impersonation moved from a theoretical risk to a practical and increasingly effective attack method. Deepfake audio and video, combined with highly convincing written impersonation, were used to support fraud attempts that closely mimicked legitimate business interactions. These attacks were particularly effective against finance teams and senior decision-makers, where authority, urgency, and trust play a critical role in day-to-day operations.

A widely reported example involved UK engineering firm Arup, where criminals used deepfake impersonation during a video call to persuade an employee to transfer significant sums of money. The incident demonstrated how attackers can convincingly replicate the appearance and voice of trusted individuals, bypassing traditional red flags that staff might otherwise rely on.

The UK Government's cyber security survey also notes growing awareness that advanced techniques, including AI based impersonation, are becoming more mainstream.

Why it won't go away: AI significantly reduces the cost and effort required to produce convincing deception. In this environment, the most effective defences are strong processes and verification controls, not instinct or familiarity.

Predictions on the Primary Threat Vectors in 2026

What is a Threat Vector? This refers to a path by which a cyber threat or attack is delivered to target systems or individuals. Essentially, a route that a hacker takes to exploit vulnerabilities and compromise the security of a system. Threat vectors take various forms and understanding them is crucial to developing effective cyber security strategies.

1. Extortion Without Encryption Will Increase

- More cyber attacks will focus on extortion rather than disruption; attackers are increasingly stealing sensitive data and applying pressure behind the scenes. This can include threats to publish confidential information, notify customers or suppliers, or triggers regulatory scrutiny, all designed to force a rapid payment.
- This type of attack is more damaging than traditional ransomware. Even when systems remain operational, the risk of data exposure creates consequences that are difficult to quantify and harder to manage. Encryption is no longer a requirement for leverage - business pressure is.
- Extortion without encryption is quieter, faster, and often just as profitable. It means that strong backups alone are no longer enough. Preventing unauthorised access and detecting data theft early is as critical as recovery planning.

2. Token Theft & MFA Bypass Techniques Will Become More Common

- As multi-factor authentication becomes more widely adopted, attackers are shifting their focus away from passwords and towards methods that allow them to bypass MFA altogether. They are finding ways to work around it by stealing session tokens, abusing legitimate sign-in flows, or positioning themselves between users and trusted services.
- Attackers do not need to defeat MFA. They reuse valid authentication tokens to access accounts as if they were legitimate users. This creates a false sense of security where MFA is enabled but accounts are still silently compromised. Protecting identities will require visibility, monitoring, and controls beyond switching MFA on.

Predictions on the Primary Threat Vectors in 2026

3. Deepfake and Business Email Compromise Will Converge

- In 2026, deepfake technology will increasingly be used to strengthen traditional Business Email Compromise attacks. Rather than relying on a single message, attackers will combine a convincing email with a quick Teams or WhatsApp message and a short voice call that sounds exactly like a trusted colleague or senior leader.
- This multi-channel approach is highly effective in fast-moving business environments, where staff are accustomed to informal communication and urgent requests. Where approval processes are weak or verification steps are unclear, AI does not need to be perfect. It only needs to be convincing enough to push someone to act.

4. Stolen Credentials Will Continue to Drive the Majority of Initial Access

- For most SMBs, the fastest and most reliable route into systems remains stolen credentials. Rather than exploiting complex technical vulnerabilities, attackers focus on obtaining legitimate login details and using them to access email, cloud applications, and business systems without triggering immediate alarms.
- Verizon's 2025 SMB breach analysis shows that a significant proportion of incidents continue to involve the use of compromised credentials. As long as single accounts can grant broad access, and monitoring remains limited, stolen credentials will remain one of the most effective tools in the attacker's arsenal.

Looking Ahead

Keep your business secure in 2026

The threats are not going anywhere, but organisations can and must take proactive steps to mitigate risk. Here are a few areas to start thinking about:

1. Put Identity First

Organisations should enforce strong multi factor authentication across all systems, particularly for administrative accounts. Administrator access should be separated from daily user accounts, standing privileges should be reduced, and unusual sign ins or mailbox rule changes should be monitored closely. For most Microsoft 365 based SMBs, this delivers the greatest security improvement for the least effort.

2. Ensure Backups Are Truly Recoverable

Backups should not be permanently connected to the same environment they protect. Backup access must be secured with separate credentials and MFA, and restores should be tested regularly. A backup that cannot be restored is not a backup.

3. Treat Payments as a High Risk Security Process

Mandatory call back verification should be used for bank detail changes, using known contact details rather than email threads. Dual approval should be required for higher risk payments, and there should be a clear escalation process for urgent requests. These controls directly reduce the risk of BEC and impersonation fraud.

4. Train Staff for Today's Attacks

Security awareness training in 2026 must address impersonation and invoice fraud, suspicious login prompts and MFA fatigue, fake IT support requests, and deepfake voice or video impersonation.

5. Maintain a Simple Incident Response Plan

Even a short, clearly defined incident response plan can significantly reduce disruption. Organisations should know who makes decisions, who to contact for support, what systems to isolate first, what evidence to preserve, and how and when to communicate during an incident.

6. Reduce Supplier and IT Provider Risk

Most UK SMBs rely on third parties. Organisations should prioritise access control and MFA for supplier access, enforce least privilege, maintain logging and visibility, and set clear expectations for incident notification and support. UK Government research shows that formal supply chain reviews remain relatively uncommon among smaller organisations, creating opportunity for attackers.

Final Thoughts

2026 may be a new year, but cyber threats continue to evolve. Attackers are becoming more efficient, better equipped, and increasingly focused on identity, email, and payment processes.

The good news is that UK SMBs do not need to do everything to materially improve security. Strong fundamentals, including identity protection, resilient backups, effective staff training, and robust verification processes, will prevent the majority of real world attacks.

Cybersecurity is no longer just an IT issue – it's business critical. Stryke is your trusted Cybersecurity and Compliance partner who will help you navigate this complex landscape. Let's commit to learning from the past and preparing for the future. While the threats may remain the same, our defences can and must evolve.

Stryke are well positioned to provide the right Cybersecurity and Compliance solutions to meet your organisation's unique needs, helping you stay protected, compliant, and resilient in the new year ahead.

Kyle Tackley – CTO & Co-Founder

kyle@stryke.co.uk

Get in touch, let's have a chat

Speak to Stryke