stryke.

New Year, Same Threats

A Cyber Security Retrospective, and how it can inform 2025

New Year, Same Threats

Let’s take a look back, to inform how we look forward

The start of any New Year often brings hope and anticipation for fresh opportunities and progress. However, in the world of cybersecurity, **the threats we battled in 2024 are not disappearing—they’re evolving and growing more sophisticated.**

As UK SMB’s plan for 2025, it’s important to acknowledge that the same main threat vectors persist, demanding **vigilance and proactive** defence strategies. It’s critical that we keep an eye on the trends that will shape 2025 and beyond in the constantly changing world of Cybersecurity.

Our 2025 Cybersecurity Retrospective eBook takes a look at the threats that shaped the 2024 cybersecurity landscape and what businesses need in order to tackle the threats they will face in 2025. We highlight some key areas and solutions that will help your business in the face of today’s security challenges and demonstrate how **Stryke can play a critical role play** in defending organisations like yours against the growing array of digital threats.

50%

of businesses reported having experienced a cybersecurity breach in the last 12 months[1]

1 Official Statistics GOV.UK, Cyber security breaches survey 2024. 9 April 2024

2024's Dominant Cyber Threats

Cybercriminals have shown remarkable adaptability, constantly evolving their strategies to exploit emerging vulnerabilities and bypass traditional security measures. This ability to innovate and adapt has kept businesses, governments, and individuals under persistent threat, as attackers leverage new technologies and refine their methods to increase the success rate of their exploits.

Cyber threats in 2024 demonstrated a sophistication and scale that left organisations reeling. Attackers are no longer limited by technical barriers; instead, they have access to readily available tools, services, and global networks that make launching complex attacks easier and more efficient than ever before.

Here's a summary of some of the most dangerous threats from 2024, which will remain highly relevant in 2025:

1. Ransomeware

The digital data hostage crisis

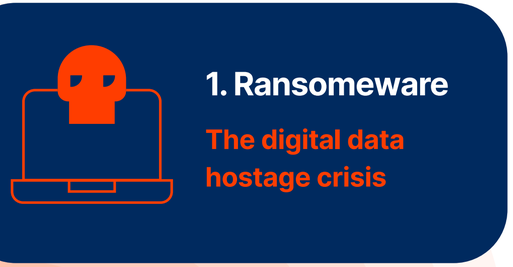
2. AI-Powered Phishing

Smarter attacks, bigger risks

3. Cloud Misconfigurations

4. Credential Theft and Account Takeovers

Here's a summary of some of the most dangerous threats from 2024, which will remain highly relevant in 2025:



Ransomware: The digital data hostage crisis

Ransomware attacks continued to make the headlines in 2024, with attackers targeting SMB businesses, governments, and even critical infrastructure. High-profile groups like LockBit and BlackCat pushed the boundaries by leveraging tactics like double-extortion methods where hackers don't just lock your files and demand money to unlock them—they also threaten to share your private or sensitive information with others unless you pay. Additionally, Ransomware-as-a-Service (RaaS) platforms have lowered the entry barrier, allowing even novice 'hobby' hackers to launch attacks with just as harmful consequences.

Even the big names can't avoid these types of attacks. A number of high-profile data breaches were believed to have been caused by the Snowflake compromise, which began in April 2024. This included a data breach of Ticketmaster's parent company Live Nation, which impacted as many as 560 million of the company's customers. A breach of banking giant Santander's customer and employee data in May was also linked to the attack on Snowflake.

Why it won't go away: Easy money. The financial success of ransomware will ensure its longevity. With many organisations still paying ransoms, attackers have little incentive to stop.

Here's a summary of some of the most dangerous threats from 2024, which will remain highly relevant in 2025:

2. AI-Powered Phishing

Smarter attacks, bigger risks

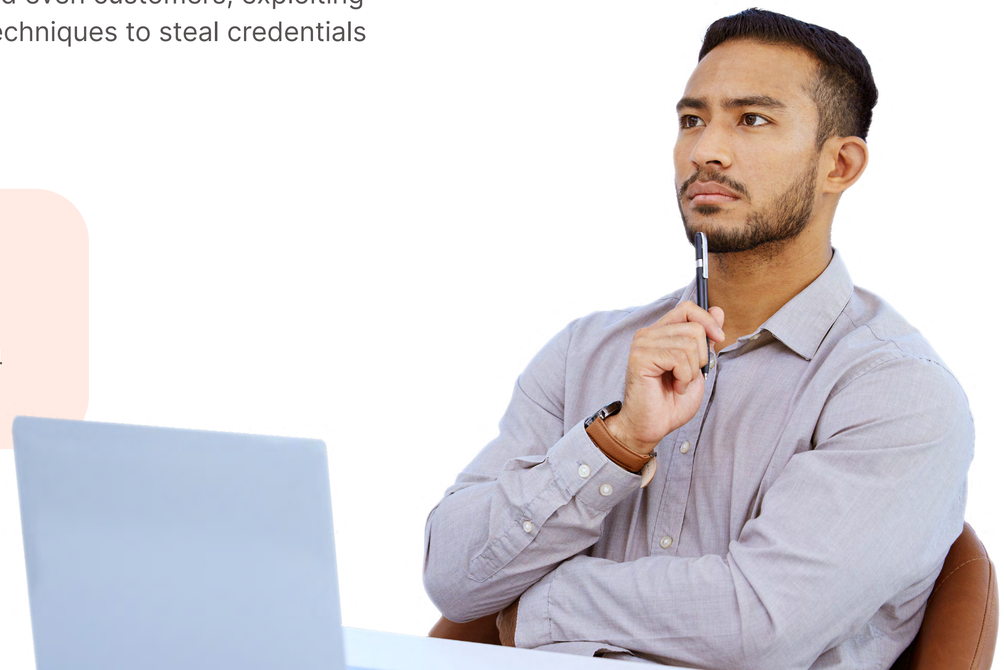
AI-Powered Phishing: Smarter attacks, bigger risks

In 2024, the integration of artificial intelligence allowed cybercriminals to craft hyper-personalised phishing emails that were almost indistinguishable from legitimate communications. Credential phishing emails increased 703% in the second half of 2024 (SlashNext, 2024). These AI-generated scams targeted company executives, employees, and even customers, exploiting trust and using social engineering techniques to steal credentials and deploy malware among others.

Why it won't go away: As AI becomes increasingly commonplace and accessible, attackers will continue to use it to outpace traditional email protection solutions.

703%

Increase in credential phishing emails in the second half of 2024 (SlashNext, 2024)



Here's a summary of some of the most dangerous threats from 2024, which will remain highly relevant in 2025:

3. Cloud Misconfigurations

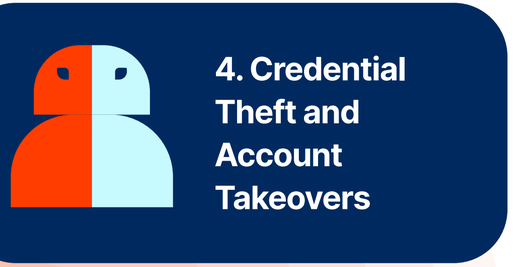
Cloud Misconfigurations

As businesses embraced cloud technologies in 2024 to support remote work, digital transformation, and scalability, cloud misconfigurations emerged as a leading cause of data breaches. These missteps often resulted from human error, lack of expertise, or insufficient automation in securing cloud environments. Misconfigurations primarily involved improperly secured storage buckets, weak access controls, and exposed cloud services.

These attacks were not just about espionage but also about disruption, as seen in ransomware-like tactics employed by politically motivated groups.

Why it won't go away: The growing complexity of multi-cloud environments makes it challenging for organisations to maintain consistent security configurations, leaving gaps that attackers can exploit.

Here's a summary of some of the most dangerous threats from 2024, which will remain highly relevant in 2025:



Credential Theft and Account Takeovers

In 2024, stolen credentials were the root cause of a significant number of breaches. Cyberattacks using stolen credentials alone have increased 71% year-over-year (IDM X-Force, 2024),

Attackers exploited weak passwords, reused credentials, and gaps in multifactor authentication (MFA) implementation to gain unauthorized access. Credential theft is like a thief copying your keys to access your digital accounts, enabling them to steal data, impersonate you, or spread attacks.

Why it won't go away: As businesses continue to transition to hybrid work models, securing identities and access remains a top challenge.

Organisations are increasingly finding themselves in a high-stakes game of cat and mouse, trying to predict and mitigate threats that continue to escalate in frequency and impact.

71%

Year-over-year increase in cyberattacks using stolen credentials

Predictions on the Primary Threat Vectors in 2025

Let's move to the primary threat vectors that we believe will be prominent in 2025. A threat vector refers to a path by which a cyber threat or attack is delivered to target systems or individuals - the route that a hacker takes to exploit vulnerabilities and compromise the security of a system. Threat vectors can take various forms, and understanding them is crucial when developing an effective cyber security strategy.

1. Regulatory Compliance Will Strain Security Teams

- New regulations, such as the EU's NIS2 Directive and DORA (Digital Organisational Resilience Act) will intensify the focus on compliance, stretching already overburdened cybersecurity teams.
- To balance compliance and security, organisations will turn to smart software tools that automate regulatory adherence.
- Maintaining a focus on adaptive and proactive cybersecurity will become crucial in order to keep up with an ever changing landscape.

2. Deepfake Technology in Social Engineering

- Deepfake audio and video will be weaponised for more convincing social engineering attacks, such as impersonating executives to authorize fraudulent payments or gain access to secure systems.
- Companies will need to invest in order to combat these increasingly sophisticated scams; these threats can be mitigated with education, awareness training and more stringent verification protocols.

Predictions on the Primary Threat Vectors in 2025

3. Ransomware Will Evolve Further

- Ransomware attacks will incorporate triple-extortion tactics, targeting not only victims and their customers but also external stakeholders, such as regulatory bodies or competitors.
- Ransomware-as-a-Service (RaaS) will continue to expand, enabling less skilled attackers to launch sophisticated hacking campaigns. This lower barrier to entry for hackers will increase both the volume and frequency of attacks.

4. AI Will Supercharge Both Attackers and Defenders

- Attackers: Cybercriminals will leverage advanced AI to automate and personalise attacks, such as creating hyper-realistic phishing campaigns and deploying AI-powered malware that adapts in real-time.
- Defenders: Security tools will increasingly rely on autonomous AI to detect, respond to, and mitigate threats without human intervention, marking a shift toward agentic AI models for proactive defense.

Looking Ahead

Keep your business alive in 25’

The threats from 2024 are not going anywhere, but organisations can and must take proactive steps to mitigate risk. Here are a few areas to consider:

1. Implement Zero Trust Architecture

A Zero Trust model operates under the principle of “never trust, always verify.” By continuously authenticating users and devices before granting access, organisations can reduce the risk of credential-based attacks.

2. Leverage AI for Defence

As attackers use AI to enhance their tactics, defenders must adopt AI-driven tools for threat detection, response, and analysis. AI can help identify anomalies in real-time and prevent breaches before they escalate. Fight like for like!

3. Adopt a Known Security Framework

Frameworks like ISO/IEC 27001:2022 help establish a robust ISMS to protect your organisation’s data, systems, and operations. This globally recognised standard enhances security, ensures regulatory compliance, and builds customer trust through systematic risk management.

4. Enhance Employee Training

Cybersecurity is everyone’s responsibility. Enhance employee training by using AI tools for personalised learning. Use real-world simulations. Look at human risk management tools to identify and address high-risk behaviours, and automated phishing campaigns to test and improve awareness.

5. Focus on Incident Response

With enough motivation, no system is immune to hackers. Organisations must have robust incident response plans that outline clear steps to contain and recover from cyber-attacks.

6. Partner with Styke

Work with our leading Compliance and Security experts to help you tackle the landscape of ‘must haves’ and ‘should haves’ so you make the right choices for your business, employees and customers.

Final Thoughts

2025 may be a new year, but the cyber threats we face are continuously developing. Attackers are becoming more sophisticated, leveraging advanced tools and exploiting any vulnerability they can find. The right cyber security strategy will provide peace of mind and the adaptability needed to keep you two steps ahead.

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.

Get in touch today to see how we can help

Let's have a chat