Strident Cyber Risk Report 2025

December 2025
Rebecca Richards

2025 has been a landmark year in the evolution of cyber risk, marked by significant incidents and regulatory advancements that have reshaped the threat landscape for organisations across all sectors.

Strident's Cyber Risk Report 2025 provides a comprehensive overview of these developments, offering actionable insights for risk managers and cyber security professionals.

Contents

Key Events and Trends

Major Breaches:

The year witnessed high-profile cyber breaches, most notably at M&S and Jaguar. These incidents exposed critical vulnerabilities in supply chain security and data management, resulting in substantial financial and reputational damage.

The breaches have prompted organisations to reassess their cyber defence strategies and prioritise proactive risk mitigation.

Regulatory Change:

The introduction of the Data (Use and Access) Act 2025 represents a pivotal shift in data governance. This new legislation sets new standards for how organisations collect, use, and share personal and sensitive data.

Compliance requirements have intensified, with greater emphasis on transparency, accountability, and user consent. The Act is expected to drive widespread changes in data handling practices and elevate the importance of robust compliance frameworks.

Evolving Threat Landscape:

Beyond media highlighted breaches, 2025 has seen a surge in sophisticated cyber-attacks targeting critical infrastructure, financial systems, and healthcare providers.

Threat actors are leveraging advanced techniques, including AI-driven exploits and ransomware-as-a-service, making it imperative for organisations to stay ahead of emerging risks.

Geopolitical Threats: The Russian Cyber Risk

The cyber threat from Russia remains a significant and persistent risk to the safety and security of the UK. Russian state-sponsored actors and affiliated cybercriminal groups have been linked to a range of hostile activities, including targeted attacks on critical national infrastructure, government agencies, and private sector organisations.

These campaigns often aim to disrupt essential services, steal sensitive data, and undermine public trust. The evolving tactics of Russian threat actors—such as the use of advanced persistent threats (APTs), disinformation campaigns, and supply chain compromises—underscore the need for heightened vigilance and coordinated national defence strategies.

The UK government and security agencies continue to issue warnings and guidance to help organisations defend against these sophisticated threats, emphasising the importance of robust cyber resilience and international cooperation.

Strident Cyber Risk Report 2025

2025 Threat Overview

85% of business and 86% of charities who reported a data breach up to April 2025, recorded that phishing was the cause of the breach. This means that 85% of reported breaches were preventable.

Phishing attacks were responsible for an estimated **7.78 million cybercrimes** against businesses, globally.

Although phishing is the number one reason for data breach, it relies on human error to be successful. The ICO have noted that **23.2% of breaches which were not phishing attacks, were caused by human error** - although broader industry percentages suggest a much higher total human element, where all breach types are considered – potentially this figure could rise to 95%.

Additionally, the ICO have reported that health, education, and finance sectors were among those with the highest amount of breach reports.

Top 10 Cyber Threats

There are a number of vectors that attackers use, sometimes in combination.

Here are the top 10 and what you can do to protect your business.

1. Phishing
2. Ransomware / Malware
3. Spoofing
4. Distributed Denial of Service
5. Insider Threat
6. Man-in-the-Middle
7. Code Injection
8. Supply Chain Attack
9. DNS Tunnelling
10. Brute–Force Attack

1. Phishing

What is it?

Phishing attacks may reach you by email, telephone, text messaging or via messaging apps. These are fake messages designed to steal data or obtain funds, the messages are designed to trick staff into performing actions outside of normal procedure.

How do we protect ourselves?

Ensure that staff accounts are created on the “least privilege” principle (minimum access rights) and ensure that staff do not browse online using administrator accounts. Use multifactor authentication and ensure your staff are subject to regularly refreshed cyber security training which includes how to spot and avoid phishing attempts.

The training should also include normal procedures staff are expected to follow how to identify and report when they are being asked to act outside of the norm. The more staff know, the lower the risk to your organisation. Report all phishing emails / messages / calls to the NCSC on **report@phishing.gov.uk**

strident

Strident Cyber Risk Report 2025

2. Ransomware / Malware

What is it?

Malware: Malicious software designed to disrupt or damage a network, device, or system, or gain unauthorised access to data.

Ransomware: Malicious software used to extract money from an organisation, usually by encrypting or blocking access to files or systems until a ransom is paid.

How do we protect ourselves?

Malware: Ensure a robust antivirus is installed and is kept up to date. Use network and device firewalls to control traffic and block unauthorised access. Scan removable media, use web filtering to block access to dangerous sites. Use pop up blockers and avoid fake security warnings.

Ransomware: Maintain secure, offline backups which are physically separated from your network. Test the backups regularly to ensure they restore data. Keep all software up to date. Install a robust anti-virus which blocks known Ransomware.

Educate your staff to look out for phishing emails so they know to avoid clicking on links or attachments. Avoid enabling Macros in email attachments as these can be used to execute malicious code. Use strong authentication controls including long passwords, passkeys, and MFA.

3. Spoofing - Part 1

What is it?

Email: A fake email sent to look like it is from a known sender

Call spoofing (call/ text): changes the displayed phone number or send to appear legitimate.

Website spoofing: fake websites which mimic real ones to steal access credentials

How do we protect ourselves?

Email: implement a sender policy framework and DomainKeys identified Mail. Implement domain – based message authentication, reporting & conformance. Use email filters and up to date antivirus. Make sure staff are trained to be continually suspicious and to inspect emails carefully. Use secure email services and configurations.

Call / Text: Do not answer unknown numbers, if the call is legitimate, the caller will leave a voicemail. Verify callers independently – if someone calls claiming to be from a bank, HMRC or other agency, hang up the call and call back on the phone number available via the organisation's official website. Set a voicemail password to prevent hackers accessing it if they spoof YOUR number.

Website Spoofing: Be wary of unexpected emails which contain links and check the security certificate and URL to ensure you can see a padlock and that the address starts with HTTPS. Look for bad spelling and grammar or variations on logos, colours or contact details. Avoid public networks.

3. Spoofing - Part 2

What is it?	**GPS spoofing:** faking location data to mislead GPS – led systems. **MAC / ARP Spoofing:** Links a malicious MAC address to the legit IP to intercept data on a local network.
How do we protect ourselves?	**GPS Spoofing:** Use receivers that can process signals from multiple Global Navigation Satellite Systems (GNSS) like Galileo, GLONASS, and BeiDou, in addition to GPS. Install dedicated hardware like a «GPS firewall» between the antenna and receiver to monitor the signal for anomalies. Hide or obscure GPS antennas from public view to prevent physical access to place a local spoofing transmitter. **MAC / ARP Spoofing:** Configure network switches to validate ARP inspection, for infrastructure devices like servers and gateways, manually define static ARP entries. Segment VLANS. Enable port security on network switches to restrict the number of MAC addresses allowed per port, or limit access to a single, known MAC address. Deploy firewalls or packet filtering to identify and block malicious ARP packets.

4. Distributed Denial of Service (DDoS)

What is it?	An overload of information sent to a server, service, or network, making it unavailable to legitimate users.
How do we protect ourselves?	Deploy firewalls and Web Application Firewalls (WAFs) to filter malicious traffic. Minimise the attack surface by closing unused network ports and disable unnecessary services. Understand your traffic – establish a baseline for normal network traffic to help identify anomalies. Keep systems and software up to date with the latest patches. Leverage cloud-based protection with 24/7 monitoring & alerts. Increase bandwidth as this can help absorb traffic spikes. Ensure sufficient redundancies and monitoring. Have a failover system in place!

5. Insider Threat

What is it?	This threat is the PEOPLE. Either on purpose or by mistake, someone within your organisation will break security rules and potentially cause a breach.
How do we protect ourselves?	Ensure you have security policies and procedures in place and educate your staff on security requirements. Ensure that staff contracts, and those used for temporary staff and contractors, include confidentiality, protection of Intellectual Property and compliance with company policy & procedure. Ensure that staff know how to identify security incidents, how to report them and who to report to. Have cyber insurance.

6. Man–in–the–Middle

What is it?	Where a malicious actor intercepts and relays communications between two parties, whilst making them think they are talking to each other. It is used to steal data, alter messages and often uses unsecure wi-fi or vulnerability exploitation.
How do we protect ourselves?	Avoid the use of public wi-fi, use a VPN, only visit websites which use the “https” protocol. Keep software up to date and use strong passwords supported by other controls such as MFA and location locking. Implement continuous network monitoring and educate staff on the risks.

7. Code Injection

What is it?	Where malicious code is inserted into a vulnerable application, which tricks it into executing the attackers’ commands instead of it has intended functions.
How do we protect ourselves?	Validate and sanitise all user input and use “allow lists” to define what is acceptable. Apply the least privilege principle. Avoid dangerous functions that allow for the for the interpretation of strings in code. Web application firewalls (WAF) shall be applied. Vulnerability scans / penetration testing which is underpinned by a documented patch management strategy should also be in place. .

8. Supply Chain Attack

What is it?	Where attackers exploit the trust placed with third parties and targets less secure organisations within a supply chain, to gain access to systems and data or may use the supply chain to introduce malicious code.
How do we protect ourselves?	Vet suppliers for security controls, risk assess all suppliers. Ensure that clear contracts and agreements are in place and address incident reporting requirements. Limit vendor access to internal systems and services – apply the least privilege principle. If you are a developer, have a Software Development Life Cycle in place which includes security testing and validation activities. Control endpoints and patch systems. Maintain an asset inventory of all software and hardware assets, including third party. Adopt a zero – trust approach and underpin with employee training.

9. DNS Tunnelling

What is it?	A covert attack which hides DNS data inside normal looking DNS queries and responses. It uses DNS trusted traffic flow to bypass firewalls and security systems. Attackers encode data into subdomains or DNS records sent to an attacker-controlled server, creating a hidden channel for communication with infected devices.
How do we protect ourselves?	Configure firewalls to block all outbound DNS requests to external DNS servers. Implement query restrictions and use DNS security extensions. Encrypt internal DNS traffic. Regularly update and patch systems.

10. Brute–Force Attack

What is it?	A trial-and-error hacking method which uses automated software to guess passwords, encryption keys or log in credentials by systematically trying all possible combinations.
How do we protect ourselves?	Ensure that accounts lock out after a set amount of incorrect password attempts. Use strong (long) passwords and support with MFA and location locking. Regularly monitor access.

ENSURE A MULTI-LAYERED APPROACH TO SECURITY

Ensuring a multi-layered approach to security is crucial in protecting against known security threats. Starting with a security - based risk assessment is the ideal place to start.

Underpin all threat protections with a breach response and business continuity plan, which is practiced regularly.

Strident Cyber Risk Report 2025

Maturity Scorecard

Use the Strident POPT Scorecard to help you identify the level of maturity in place at your organisation:

Capability	Level 1	Level 2	Level 3
People	Annual learning	Annual learning & testing	Documented incident response plan, quarterly desk top simulations
Organisational	High level InfoSec policies / compliance with legal requirements	InfoSec reviewed as part of board governance	Infosec policies & procedures, control of staff & temps
Premises	Door locks / locks for physical files	Physical security & emergency procedures	Physical access control
Technology	AV + Firewall(s)	MDM, MFA, strict access controls, enforced PW policies.	EDR, WAF, Macro blocking, VLAN segmentation

Capability	Level 4	Level 5
People	Role mapped runbooks, semi annual drills	Live reporting rehearsals, test participation & lessons learned
Organisational	Threat intelligence / modelling	Infosec supply chain assessments & audit. Continual monitoring.
Premises	Physical monitoring / access reviews	Continual monitoring, review, and improvement.
Technology	Network IDS / IPS, backup schedule, encryption for data at rest and in transit, immutable backups.	Zero – trust enforcement, vulnerability scanning & penetration testing & patching.

Strident Cyber Risk Report 2025

Legal Changes in 2026

The Cyber Security and Resilience Bill (expected in 2026):

Looking ahead, the UK government is set to introduce the Cyber Security and Resilience Bill in 2026, representing a major overhaul of the nation's cyber regulatory framework.

This new law will significantly expand the scope of existing regulations, bringing a wider range of organisations under direct oversight—including not only operators of essential services (such as healthcare, energy, water, transport, and digital infrastructure), but also medium and large managed service providers, data centres, and critical suppliers within digital supply chains.

To comply, organisations must reassess their risk management frameworks, invest in staff training, strengthen supplier oversight, and ensure that incident detection and reporting processes are well-rehearsed and documented.

Early planning and initiative-taking adaptation will be essential, as the Bill is expected to be phased in over time, with detailed operational rules set out in secondary legislation following further government consultation.

How AI is supercharging Cybercrime

Access to Generative AI tools has heightened cyber risk, enabling attackers with minimal technical skill to launch sophisticated attacks.

Automated malware builders, deepfake generators, and AI-driven phishing kits allow even "kiddie scribblers" to execute attacks that previously required advanced expertise.

AI-powered threats can adapt in real time, analysing security measures and modifying their tactics to bypass defences.

Polymorphic malware now mutates its code dynamically, evading signature-based detection and increasing the probability of successful breaches.

Deepfakes and Identity Fraud AI enables the creation of highly convincing deepfake audio and video, allowing attackers to impersonate executives, government officials, or even friends and family members.

These tactics have led to high-profile financial frauds and espionage campaigns, with deepfake incidents increasing by over 2,000% since 2022.

Automated Vulnerability Discovery AI systems can scan massive codebases and networks for vulnerabilities at machine speed, accelerating the timeline for zero-day exploit discovery and deployment.

This capability has led to a dramatic rise in credential theft, ransomware, and supply chain attacks.

Global Impact and Real-World Consequences:

- **Critical Infrastructure Under Siege**: State-sponsored actors have weaponised AI to target essential systems—water treatment, power grids, transport networks—raising the stakes from digital disruption to physical harm.
- **Economic Toll:** The global cost of cybercrime is expected to reach $24 trillion by 2027, with AI-driven attacks representing a growing share of this loss.
- **Rapid Attack Cycles:** The average detection time for AI-assisted breaches has dropped to just 11 minutes, overwhelming traditional security teams and response protocols.
- **Legal and Regulatory Challenges:** The rise of autonomous, AI-orchestrated attacks is outpacing existing legal frameworks, prompting urgent calls for new international treaties and governance strategies.

Strident Cyber Risk Report 2025

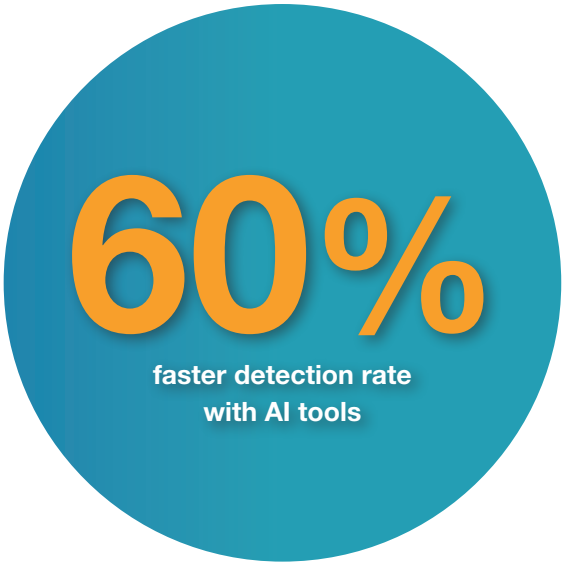
The AI Arms Race: Defence and Resilience

While AI amplifies the threat, it also powers new defences. Organisations using AI-driven security tools report a 60% faster threat detection rate and save an average of $1.9 million per breach.

However, the vulnerability paradox remains: the same technology that promises efficiency also expands the attack surface, requiring continuous vigilance, robust governance, and global cooperation.

As organisations adapt to these challenges, the lessons of 2025 underscore the need for continuous vigilance, investment in cybersecurity, and a culture of compliance.

Strident's report aims to equip stakeholders with the knowledge and strategies required to navigate the complexities of the modern cyber risk environment.



Create a plan by speaking to Strident

Speak to Strident about creating a security action plan, improving your security controls and compliance stance, we can help you initiate and implement a robust and tested cyber – security program to suit your organisations.