Cyber Threats 2026: AI, Identity, and Resilience in an Accelerated Threat Landscape

An evidence-based risk outlook for IT, cybersecurity and business leaders

Red Helix

CONTENTS

Executive Summary

Organisations are entering 2026 facing the fastest-moving cyber threat landscape on record. Adversaries are leveraging generative AI to automate attacks, increase speed, and create highly convincing social-engineering campaigns, while the expansion of cloud and third-party ecosystems has multiplied exposure. At the same time, regulatory expectations around resilience, governance and identity protection are increasing, leaving leadership teams under growing scrutiny.

Generative AI, while offering productivity gains, also introduces new classes of risk. Many organisations may unknowingly expose sensitive or regulated information to public AI tools, while threat actors' experiment with novel attack methods such as prompt injection, model manipulation, and AI-enabled social engineering. As businesses embed AI more deeply into critical processes, misconfigurations and lack of oversight can lead to unauthorised AI actions or unintended data leakage.

Ransomware continues to be the most disruptive and persistent threat. The 2025 edition of the CrowdStrike European Threat Landscape Report shows that European organisations accounted for **approximately 22% of global ransomware and extortion victims**. North America was the only region with more ransomware attacks.

Identity compromise, supply-chain vulnerabilities, and cloud misconfigurations remain primary attack vectors, while regulatory pressure increases in parallel with rising awareness of cyber risk. Organisations that invest in identity-centric security, AI governance, supply-chain assurance, and robust detection & response are the ones most likely to maintain resilience in 2026.

This report outlines key trends, the evolving threat landscape, and actionable recommendations for leadership, security teams and board-level stakeholders.

"At Red Helix, we see a clear pattern emerging. Identity has become the new perimeter, AI has become both a tool and a target, and resilience has become the measure by which organisations are judged. Our role is to support with expertise, visibility and assurance so that our customers can face 2026 with confidence."

- Marion Stewart, CEO

1. The Impact of AI on Cybersecurity

AI Powered Attacks

Attackers are using AI to automate reconnaissance, refine phishing campaigns and generate highly convincing synthetic media. Currently, **48% of organisations surveyed cited AI-automated attack chains as their greatest ransomware threat**, while **85% expressed concern that traditional detection tools are becoming inadequate against AI-enhanced attacks**.

Attackers are experimenting with prompt injection, model manipulation and context aware phishing generated by large language models. Deepfake audio, video and documents allow impersonation of colleagues, suppliers or executives with unprecedented realism. Combined with compromised credentials, these techniques bypass both technical controls and human verification.

The expansion of AI agents in enterprise workflows introduces additional exposure. Poorly configured or overly permissive agents can be manipulated to perform unintended actions, interact with sensitive systems or trigger automation at scale. This new class of AI driven operational risk blends human error with machine autonomy, creating vulnerabilities that did not previously exist.

AI Powered Defence

Despite its misuse, AI remains a powerful defensive force. Security teams are increasingly relying on behavioural analytics, anomaly detection and AI assisted threat intelligence to counter rapidly evolving threats. Modern detection platforms correlate endpoint, identity, cloud and network signals to identify malicious activity earlier in the kill chain.

Research into behavioural and graph-based analysis demonstrates significant improvements in detecting novel ransomware and polymorphic malware. Runtime analysis, unsupervised learning and temporal correlation provide additional capability beyond traditional approaches.

In 2026, the organisations that succeed will be those that combine AI enhanced detection with skilled human expertise. An agent assisted SOC, built on rapid correlation and automated triage, provides defenders with a speed advantage that adversaries cannot easily overcome.

Security of AI Systems

As AI becomes embedded in business operations, organisations must treat it as part of their security critical estate. Poor governance, weak access controls or unmonitored usage can lead to data leakage, unauthorised automation or unpredictable agent behaviour.

Secure adoption requires clear policies for data inputs, strict controls over who can use specific AI tools, continuous monitoring of AI agent behaviour and comprehensive logging to support incident investigation. Without this discipline, AI introduces systemic vulnerabilities that attackers can exploit with growing ease.

"We're witnessing a fundamental shift in security culture as AI becomes embedded in every tool we use. The new priority is building AI-specific security awareness, ensuring people understand not just how to use AI, but how to use it safely to protect themselves and their organisations."

- Jason Price, Pre-Sales Engineer

2. The Human Factor, Security Culture and the Cyber Skills Gap

Even before AI became ubiquitous, human error was consistently the most common root cause in data breaches. Now, with AI agents, generative tools, and automation embedded in everyday workflows, human risk converges with AI risk, creating a hybrid vulnerability that can be exploited at multiple layers. AI powered social engineering exploits cognitive bias, trust and routine behaviours more effectively than ever. Deepfake enabled impersonation, false invoice fraud and AI generated phishing have become highly scalable and convincing.

Misuse of AI tools by employees, accidental data sharing and overreliance on AI generated outputs all contribute to breach risk. At the same time, organisations continue to face a significant shortage of skilled security professionals, placing additional pressure on SOC teams and increasing the risk of configuration errors or delayed detection.

3. Identity, Credential, and Access Threats

Identity remains the primary gateway for attackers, reflecting a shift from traditional perimeter-focused attacks to identity-centric exploitation. According to the 2025 Verizon Data Breach Investigations Report, **credential theft accounted for approximately 61% of breaches in organisations with cloud-first architectures**.

Identity and Access

Threat actors increasingly exploit valid accounts through phishing, session hijacking, multi-factor authentication fatigue attacks, token-based intrusions, and targeted attacks against Active Directory itself. These attacks leverage both human error and insufficient controls within identity and access management systems. Remote work and widespread cloud adoption have amplified exposure, making consolidated identity governance and continuous behavioural monitoring essential.

Credential Threats

Living-off-the-land attacks using stolen credentials are becoming more common. Once attackers obtain legitimate user credentials, they can re-enter environments repeatedly, increasing operational risk and complicating incident response. Hackers are no longer breaking in, they can simply log on. Identity and Access Management (IAM) and Privileged Access Management (PAM) are therefore no longer optional: they must be centralised, continuously monitored, and integrated with zero-trust frameworks.

4. Rapidly Expanding Attack Surface

The attack surface continues to grow as organisations adopt cloud services, IoT devices, and complex third-party supply chains. Each new system component or connected device introduces potential vulnerabilities that attackers can exploit.

Internet of Things (IoT)

IoT adoption has expanded the number of endpoints and created additional vectors for intrusion. Misconfigured devices or insecure integrations can provide attackers with persistent footholds, enabling lateral movement and escalation.

Cloud

Misconfigurations in cloud environments remain a major contributor to breaches. Teams must manage distributed identities, ephemeral workloads, and automated CI/CD pipelines, all of which increase visibility challenges and amplify the risk of configuration errors.

Supply Chain

Complex supply chains, which integrate third-party vendors, SaaS applications, and open-source dependencies, introduce systemic risk. Attackers increasingly target these indirect pathways to compromise multiple organisations simultaneously. Recent ENISA reporting underscores the **growing number of supply-chain-related incidents**, highlighting the need for third-party risk management and continuous assurance.

5. The Commercialisation of Cybercrime

Ransomware-as-a-Service (RaaS)

Ransomware continues to operate as a structured, commercialised ecosystem. RaaS enables fewer technical actors to execute attacks by purchasing access, tools, and infrastructure, while developers maintain profit-sharing arrangements. CrowdStrike and Check Point both report that RaaS activity has reached record levels in 2025, with **at least 85 active extortion groups globally.**

Multi-Phase Extortion

Double-extortion attacks (an attack involving data theft and system encryption) are now the baseline. Emerging tactics, sometimes referred to as “quadruple extortion,” combine data theft, encryption, leaks, and additional coercive actions. These strategies place significant operational and financial pressure on victims.

Access Brokers and Anonymity

Access brokers act as intermediaries, selling compromised credentials or network access to the highest bidder. This professionalisation of cyber crime complicates attribution, enforcement, and recovery. Coupled with increasingly anonymous cryptocurrency transactions, tracking and prosecuting offenders has become even more difficult.

Ethical and Strategic Implications for Victims

Regulatory and moral questions arise when considering ransom payments. Organisations face difficult choices as paying may restore operations, but it could also be funding illicit activity, while non-payment may increase operational exposure. Board-level discussions must include both technical and ethical considerations so organisations can pick the best course of action.

“The most worrying trend, for me, is the gamification of ransomware. This has made attacks far less predictable as isolated, unskilled groups get involved. These offshoot actors often seek attention as much as financial gain, fuelling attacks that are increasingly unpredictable and chaotic.”

- Patrick Okolie, Cyber Security Product Specialist

6. Regulatory Frameworks

The regulatory landscape is tightening globally. Organisations must comply with frameworks such as GDPR, NIS2, the EU AI Act, ISO 42001, and emerging sector-specific guidance for financial services and healthcare. For example, the FCA Consumer Duty requires financial institutions to evidence strong operational resilience, responsible data use and robust oversight of suppliers. Similarly, NHS-linked bodies must use the Data Security and Protection Toolkit (DSPT), which requires clear identity access controls, privileged-account governance and breach-response readiness.

Data Privacy

Enforcement is intensifying. The message from the ICO in October 2025 was clear: "Maintaining good cybersecurity is fundamental to economic growth and security. With so many cyber attacks in the headlines, our message is clear: every organisation, no matter how large, must take proactive steps to keep people's data secure. Cyber criminals don't wait, so businesses can't afford to wait either". In 2025, Capita were issued a fine of £14m for failing to ensure the security of personal data related to a breach and Guernsey's Office of the Data Protection Authority (ODPA) fined a medical group £100,000 after patient data was stolen due to poor patching and delayed threat detection.

AI Governance

The release of ISO 42001 and growing AI regulatory frameworks highlight the need for organisations to monitor AI usage, enforce data access controls, and maintain auditability of AI-driven processes. Organisations that fail to establish clear AI governance risk not only operational disruption but also regulatory penalties.

"Following high-profile breaches affecting organisations like M&S and Jaguar Land Rover, we've seen the UK government take a far more active role in cybersecurity. New regulations and cyber-focused legislation signal a growing recognition of cyber risk as a national priority. We will continue to see this shaping policy and practice throughout 2026 and beyond."

- Tom Exelby, Head of Cyber Security

7. The Next Frontier of Cyber Threats

Agentic AI

Agentic AI is generative; it uses large language models to come up with answers which don't physically exist at the moment. Its use is growing rapidly, with new advancements being made weekly. Gartner predicts that **by 2026, 40% of enterprise applications will integrate task-specific AI agents**, and Goldman Sachs estimates that **agentic AI will account for roughly 60% of software market value by 2030**.

While these systems promise efficiency gains, they also introduce additional attack surfaces and governance challenges. It is embedded in office tools such as Microsoft and Google, so it has become an organisational issue, if there are no governance and controls on what it's used it for.

Quantum Threats

Forward-looking organisations are beginning to assess quantum-resistant encryption. Quantum computing may, in the medium term, compromise traditional cryptographic systems, necessitating early migration and auditing of cryptographic assets to mitigate future risk.

"Right now, IT professionals are locked in a constant cat-and-mouse battle with cyber criminals, and that dynamic isn't going away. As we move into 2026, this contest will only intensify, becoming a full-scale technology race as agentic AI and quantum capabilities reshape both attack and defence."

- Rob Pocock, Technical Director

Conclusion

The cyber landscape in 2026 is defined by the convergence of advanced AI, professionalised criminal operations, interconnected supply chains, and heightened regulatory scrutiny. Organisations must assume that breaches are inevitable and focus on resilience, recovery, and governance.

Strategic imperatives include:

- Prioritising identity protection, zero-trust architectures, and behavioural monitoring
- Implementing comprehensive AI governance, security and agent oversight
- Securing cloud, IoT, and supply chain infrastructures
- Allocating resources for continuous detection, response, and forensic readiness
- Engaging in proactive compliance and regulatory alignment

By integrating these measures, organisations can navigate evolving cyber threats while maintaining operational continuity and stakeholder confidence. Evidence-based decision-making, investment in skilled personnel, and intelligent adoption of AI tools will define success in 2026.

References

CrowdStrike. European Threat Landscape Report 2025. crowdstrike.com

Check Point Research. The State of Ransomware Q3 2025. research.checkpoint.com

Verizon. Data Breach Investigations Report 2025. verizon.com/dbir/2025

ENISA. Threat Landscape 2025. enisa.europa.eu/publications

Microsoft Security. Identity Threat Report 2025. microsoft.com/security/blog/2025

ODPA. Medical Group Fine Announcement. odpa.gg

Gartner. Market Forecast for Agentic AI 2026. gartner.com

Goldman Sachs Research. Agentic AI and Market Outlook. goldmansachs.com/research