iSTORM®
Privacy • Security • Pentesting

THREAT INTELLIGENCE REPORT

OCTOBER 2026

Contact

Phone +44 (0)1789 608708
Website www.istormsolutions.co.uk
Email info@istormsolutions.co.uk

iSTORM Privacy. Security. Pentesting

Overview

This report provides an overview of the key information security risks facing organisations in today's evolving threat landscape. It explores emerging threats, common attack methods and the activities of known threat actors, alongside real-world examples of reported cyber incidents.

Using recent statistics, industry insights and threat intelligence, the report highlights the potential impact these threats can have on organisations and individuals, including financial loss, operational disruption, data breaches and reputational damage.

The aim is to help organisations better understand the risks they face, recognise emerging threats and make more informed decisions about their cyber security priorities and protective measures.

Critical Vulnerabilities ---------- 02

AI-Enabled Cyber Attacks ---------- 02

Ransomware ---------- 03

Data Protection and Agentic AI ---------- 03

AI Governance ---------- 04

Phishing and Social Engineering ---------- 04

1. Critical Vulnerabilities

Critical PHP Vulnerability Highlights “Black October”

A severe vulnerability disclosed in the PHP programming language in October has highlighted the increasing speed at which weaknesses in widely used internet infrastructure can be discovered and targeted.

Cyber-security leaders have warned that AI-assisted vulnerability research may significantly increase the volume of newly identified vulnerabilities, while malicious actors may use the same capabilities to accelerate exploitation.

Recommendation:

Organisations should maintain accurate asset and software inventories, prioritise remediation of internet-facing and critical vulnerabilities, monitor vendor security advisories, and apply emergency patching processes where active exploitation or critical severity is identified.

---

2. AI-Enabled Cyber Attacks

AI Expected to Increase the Scale and Impact of Cyber Attacks

The UK National Cyber Security Centre assesses that AI is already being used in malicious cyber activity and is expected to increase the volume and impact of cyber attacks, including ransomware.

AI can lower the barrier to entry for less-skilled attackers and improve reconnaissance, targeting, phishing content and vulnerability discovery. This makes established controls such as MFA, patching, monitoring and staff awareness increasingly important.

Recommendation:

Organisations should continue to implement defence-in-depth controls, including phishing-resistant MFA where appropriate, timely vulnerability management, endpoint and network monitoring, tested backups, security awareness and incident-response exercises.

3. Ransomware

Ransomware Remains an Acute Threat to UK Organisations

The NCSC continues to identify ransomware as one of the most acute cyber threats facing UK organisations. AI is expected to assist threat actors with access, targeting and operational efficiency rather than replace existing ransomware methods.

Organisations with exposed services, weak identity controls, unpatched vulnerabilities or inadequate backup segregation remain particularly vulnerable to disruptive ransomware and data-extortion activity.

Recommendation:

Maintain tested offline or logically separated backups, restrict administrative privileges, use MFA, patch critical systems rapidly, monitor for unusual authentication and endpoint activity, and maintain a documented and exercised incident response plan.

---

4. Data Protection and Agentic AI

ICO Examines Data Protection Risks from Agentic AI

In October 2026 the Information Commissioner's Office opened a call for evidence on the application of data protection law to agentic AI. The areas identified include data security, transparency, accountability, automated decision-making, fairness, purpose limitation and lawfulness of processing.

Agentic AI can take actions across connected systems with a degree of autonomy. This can create additional privacy and security risks where agents are given access to personal data, email, files, business systems or external tools.

Recommendation:

Before deploying AI agents, organisations should identify personal-data processing, apply data minimisation and least-privilege access, complete DPIAs where high risk is likely, maintain human oversight and audit logging, and ensure suppliers and connected services are appropriately assessed.

5. AI Governance

Privacy and Security Controls for Enterprise AI Use

The growing use of generative and agentic AI means organisations should treat AI platforms as part of their information-security, privacy and supplier-risk environment rather than as standalone productivity tools.

Prompts, uploaded files and connected data sources can contain confidential or personal information. Uncontrolled adoption can therefore create risks around inappropriate disclosure, retention, access permissions and inaccurate automated outputs.

Recommendation:

Maintain an approved AI tools register, define acceptable-use rules, restrict sensitive data input where not authorised, review supplier data-handling terms, provide user training, and periodically review AI risks through the ISMS/AIMS and data-protection processes.

---

6. Phishing and Social Engineering

AI Continues to Strengthen Social Engineering

Phishing remains a primary route for credential theft and initial access. AI allows attackers to produce more convincing messages, rapidly tailor content to individuals and organisations, and support impersonation through synthetic text, images and voice.

Traditional visual indicators such as poor grammar are becoming less reliable. Verification of unusual payment, credential, access or data requests is therefore increasingly important.

Recommendation:

Use MFA, email and URL filtering, user awareness training and independent verification for unusual or sensitive requests. High-risk financial or access requests should be confirmed using a trusted communication channel rather than contact details supplied in the original message.

iSTORM'S Approach

We are the humans in the loop.

We are an award-winning GRC consultancy specialising in Data Protection and Penetration Testing.

We combine deep technical expertise with a personal, client-focused approach, offering the high-quality delivery of a large consultancy with the care, attention and flexibility of a smaller, dedicated team.

We work alongside organisations to help them understand their risks, strengthen their security and navigate the ever-changing world of data protection, governance and cyber security.

Let's put the right people in your corner.

For more information on how any of the current threats may impact your organisation or for information on our range of Privacy, Security and Pentesting consultancy services, contact the team for a no obligation conversation.

Contact us directly:
info@istormsolutions.co.uk or call +44 (0) 1789 608708

iSTORM®
Privacy • Security • Pentesting

iSTORM Privacy. Security. Pentesting