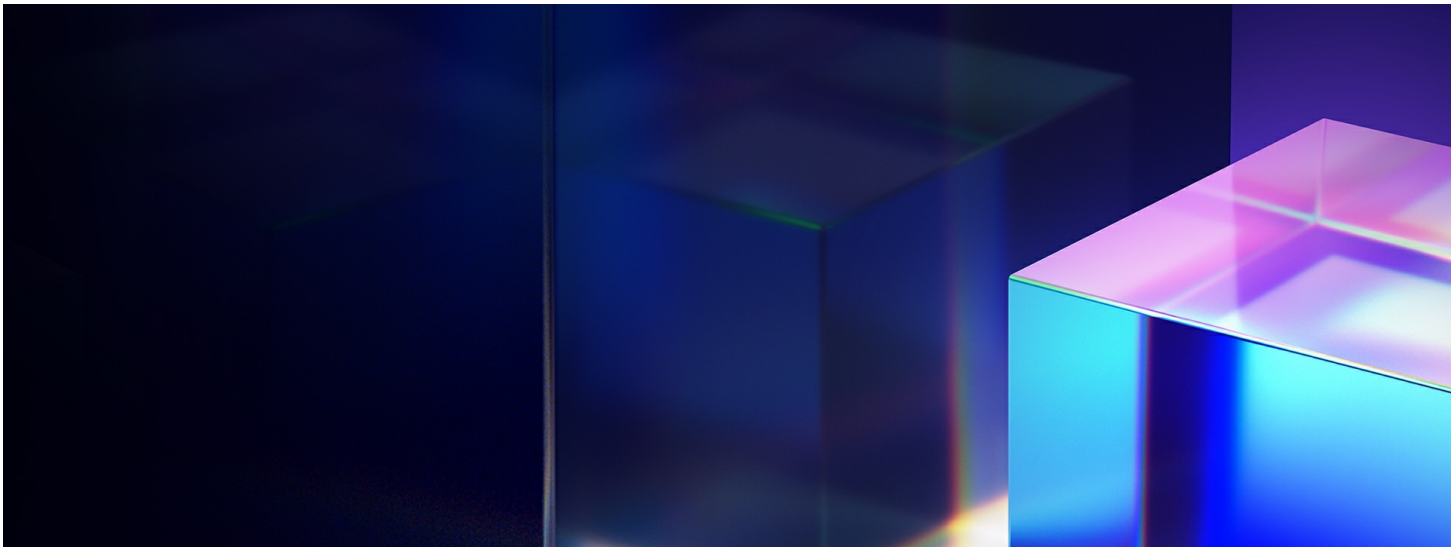
IBM UK Newsroom

IBM Report: UK Sees Drop in Breach Costs as AI Speeds Detection

AI/Automation Slashes Breach Costs by Over £600,000 for UK Firms



LONDON, UK, 30 July 2025 - IBM today released the UK edition of its 2025Cost of a Data Breach Report, revealing that UK organisations using AI and automation extensively across their security operations saw data breach costs drop to £3.11 million per year, significantly lower than the £3.78 million average cost for those not using these technologies. Yet less than one-third of UK organisations have deployed these technologies extensively, revealing more room for savings across the region.

The 2025 report, conducted by Ponemon Institute, sponsored and analysed by IBM, is based on real world data breaches experienced by 600 organisations across the global including those in the UK, from March 2024 through February 2025. Some of the key UK findings in the 2025 report include:

- **AI Outpacing Policy:** Only 31% of the UK organisations which have responded have governance policies in place to manage the use of AI and prevent shadow AI. Of those with these policies, the most common components include strict approval processes for AI deployments (45%) and use of AI governance technology (47%).

- **Overexposed AI.** Most (63%) of the UK organisations which responded reported not having AI access controls in place to reduce risks associated with attacks on AI models or applications, making these systems easy targets for bad actors.

- **Accelerated Breach Response with AI:** In the UK, organisations that responded made extensive use of security AI and automation achieved a mean time to identify (MTTI) and contain (MTTC) data breaches of 148 and 42 days, respectively—cutting breach response by 42 days compared to those not using these technologies (168 and 64 days).

- **Rising Cyber Threats from Supply Chains, Phishing, and Credential Breaches.**Among surveyed UK organisations, the most commonly reported causes of data breaches were third-party vendor and supply chain compromises (18%), phishing attacks (16%), and compromised credentials (11%).

- **Financial Services Breaches Remain the Costliest** The survey results indicated that the financial services sector remains the costliest UK industry for data breaches, with an average cost of £5.74 million in 2025—a 5% decrease from

the previous year.

"The data speaks for itself as organisations implementing robust AI-driven security automation are significantly reducing breach costs" said Georgie Cohen, UKI Cybersecurity Services Leader, IBM. "And yet at the same time, UK organisations are lacking the security controls and governance policies needed to protect AI systems from misuse or attacks. Now is the time to act decisively and match the investments made in AI with securely protecting the AI systems being deployed across every industry."

"IBM's report shows a clear trend that AI technologies continue to be a great tool, not just for productivity but also for security purposes" said Matthew Evans, COO and Director for Markets, techUK. "However, AI alone is not the answer – as data breaches become faster and smarter, people and organisations need the proper tools and skills to use AI in the right way to protect themselves. Lifelong learning in the form of courses, training, and certifications can make the difference in supporting organisations and their employees in protecting themselves from costly data breaches."

Other global findings in the 2025 Cost of a Data Breach Report include:

- **Data Breach Costs**. The global average cost of a data breach fell to $4.44 million, the first decline in five years

- **Overexposed AI.** Nearly all (97%) of global respondents who experienced an AI-related security incident reported lacking proper AI access controls.

- **Security Investments Stall Amid Rising AI Risks.** There was a significant reduction in the number of global organisations that said they plan to invest in security following a breach (49% in 2025 compared to 63% in 2024). Less than half of those that plan to invest post-breach will focus on AI-driven security solutions or services.

- **The High Cost of Shadow AI.** Organisations that used high levels of shadow AI (unregulated, unauthorised use of AI) paid an average of £498,000 in higher breach costs than those with a low level or no shadow AI – one of the largest cost drivers revealed in the 2025 report.

- **Ransom Payment Fatigue.** Last year, organisations pushed back against ransom demands, with more opting not to pay (63%) compared to the year prior (59%). However, even as more organisations refuse to pay ransoms, the average cost of an extortion or ransomware incident remains high, particularly when disclosed by an attacker (£4.72 million).

About the Cost of a Data Breach Report

The Cost of a Data Breach Report has investigated nearly 6,500 data breaches over the past 20 years. Since the inaugural report in 2005, the nature of breaches has evolved dramatically. Back then, risk was largely physical. Today, the threat landscape is overwhelmingly digital and increasingly targeted, with breaches now driven by a spectrum of malicious activity.

With the pace of enterprise AI adoption proliferating, for the first time, the Cost of a Data Breach research studied the state of security and governance for AI, the type of data targeted in security incidents involving AI, breach costs associated with AI-driven attacks, and the prevalence and risk profile of shadow AI (unregulated, unauthorised use of AI). Historical findings from past reports include the following:

- **2005:** nearly half (45%) of all data breaches were caused by lost or stolen computing devices, such as a laptop or thumb drive, and only 10% of breaches were due to hacked electronic systems.

- **2015:** breaches due to cloud misconfiguration weren't even a categorized threat, today they are a leading target.

- **2020:** ransomware began to surge, and by 2021 it accounted for an average of $4.62 million in breach costs, and this year that number reached an average of $5.08 million (when the incident was disclosed by an attacker).

- **2025:** AI security, which was included for the first time in the research this year, is quickly emerging as a high value target.

Additional sources:

- Download a copy of the 2025 Cost of a Data Breach Report to learn more.
- Sign up for the 2025 IBM Cost of a Data Breach webinar on Wednesday, August 13, 2025, at 11:00 a.m. ET.

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs, and gain a competitive edge in their industries. Thousands of governments and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently, and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity, and service. Visit www.ibm.com for more information.

Media contact

Imtiaz Mufti
IBM Communications
Imtiaz.mufti@ibm.com
Tel: +44 (0)7909020019
