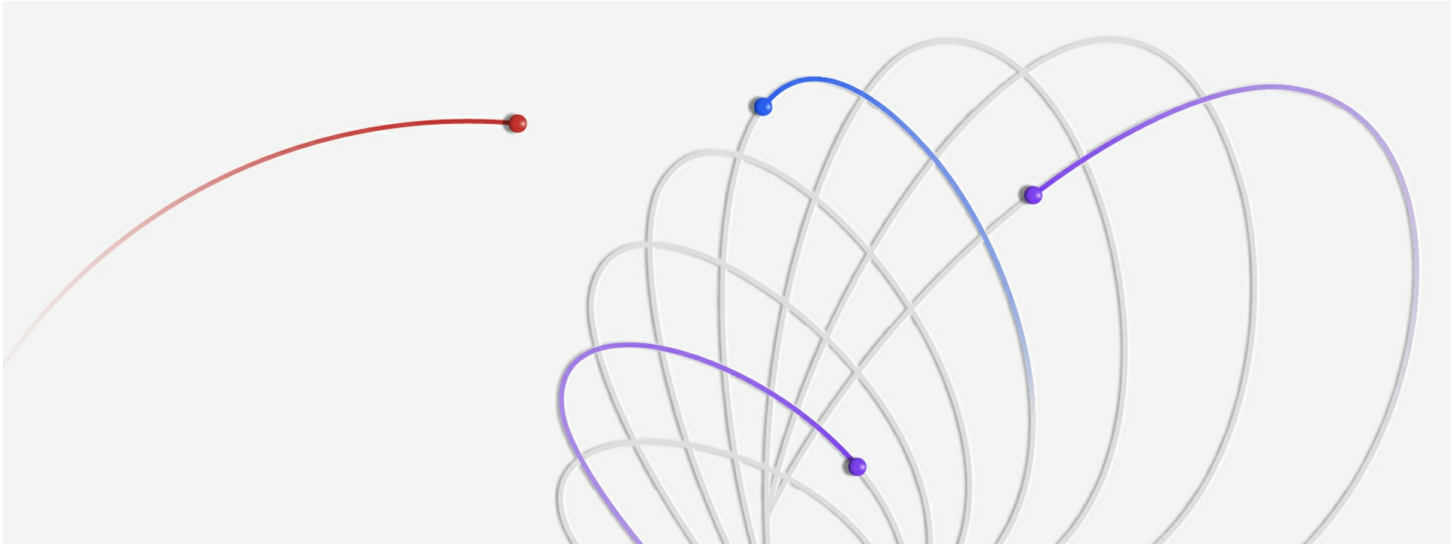
IBM Newsroom

IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs

Intellectual property theft spiked; More than one-third of breaches involved shadow data

Yet use of AI/Automation cut breach costs by $1.88 million



CAMBRIDGE, Mass., July 30, 2024 /PRNewswire/ -- IBM (NYSE:IBM) today released its annual Cost of a Data Breach Report revealing the global average cost of a data breach reached $4.88 million in 2024, as breaches grow more disruptive and further expand demands on cyber teams. Breach costs increased 10% from the prior year, the largest yearly jump since the pandemic, as 70% of breached organizations reported that the breach caused significant or very significant disruption.

Lost business and post-breach customer and third-party response costs drove the year-over-year cost spike, as the collateral

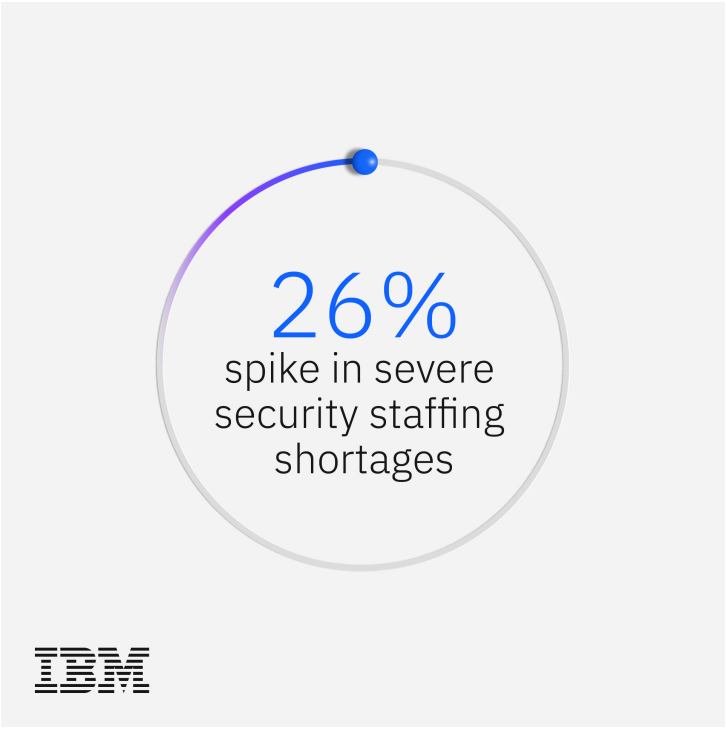
damage from data breaches has only intensified. The disruptive effects data breaches are having on businesses are not only driving up costs, but are also extending the after-effect of a breach, with recovery taking more than 100 days for most of the small number (12%) of breached organizations that were able to fully recover.

The 2024 Cost of a Data Breach Report is based on an in-depth analysis of real-world data breaches experienced by 604 organizations globally between March 2023 and February 2024. The research, conducted by Ponemon Institute, and sponsored and analyzed by IBM, has been published for 19 consecutive years and has studied the breaches of more than 6,000 organizations, becoming an industry benchmark.

Some key findings in the 2024 IBM report include:

- **Understaffed Security Teams –** More organizations faced severe staffing shortages compared to the prior year (26% increase) and observed an average of $1.76 million in higher breach costs than those with low level or no security staffing issues.
- **AI-Powered Prevention Pays Off –** Two out of three organizations studied are deploying security AI and automation across their security operation center (SOC). When these technologies were used extensively across prevention workflows organizations incurred an average $2.2 million less in breach costs, compared to those with no use in these workflows – the largest cost savings revealed in the 2024 report.
- **Data Visibility Gaps –** Forty percent of breaches involved data stored across multiple environments including public cloud, private cloud, and on-prem. These breaches cost more than $5 million on average and took the longest to identify and contain (283 days).

"Businesses are caught in a continuous cycle of breaches, containment and fallout response. This cycle now often includes investments in strengthening security defenses and passing breach expenses on to consumers – making security the new cost of doing business," said Kevin Skapinetz, Vice President, Strategy and Product Design, IBM Security. "As generative AI rapidly permeates businesses, expanding the attack surface, these expenses will soon become unsustainable, compelling business to reassess security measures and response strategies. To get ahead, businesses should invest in new AI-driven defenses and develop the skills needed to address the emerging risks and opportunities presented by generative AI."



Security staffing shortages drove up breach costs

More than half of the organizations studied had severe or high-level staffing shortages last year and experienced significantly higher breach costs as a result ($5.74 million for high levels vs. $3.98 million for low levels or none). This comes at a time when organizations are racing to adopt generative AI (gen AI) technologies, which are expected to introduce new risks for security teams. In fact, according to a study from the IBM Institute for Business Value, 51% of business leaders surveyed were concerned with unpredictable risks and new security vulnerabilities arising, and 47% were concerned with new attacks targeting AI.

Mounting staffing challenges may soon see relief, as more organizations stated that they are planning to increase security budgets compared to last year (63% vs. 51%), and employee training emerged as a top planned investment area. Organizations also plan to invest in incident response planning and testing, threat detection and response technologies (e.g., SIEM, SOAR and EDR), identity and access management and data security protection tools.

Hacking the clock with AI

The report found that 67% of organizations deployed security AI and automation – a near 10% jump from the prior year – and 20% stated they used some form of gen AI security tools. Organizations that employed security AI and automation extensively detected and contained an incident, on average, 98 days faster than organizations not using these technologies. At the same time, the global average data breach lifecycle hit a 7-year low of 258 days – down from 277 days the prior year and revealing that these technologies may be helping put time back on defenders' side by improving threat mitigation and remediation activities.

Shorter breach lifecycles can also be attributed to the increase in internal detection: 42% of breaches were detected by an organization's own security team or tools compared to 33% the prior year. Internal detection shortened the data breach lifecycle by 61 days and saved organizations nearly $1 million in breach costs compared to those disclosed by an attacker.

Data insecurities fuel intellectual property theft

According to the 2024 report, 40% of breaches involved data stored across multiple environments and more than one-third of

breaches involved shadow data (data stored in unmanaged data sources), highlighting the growing challenge with tracking and safeguarding data.

These data visibility gaps contributed to the sharp rise (27%) in intellectual property (IP) theft. Costs associated with these stolen records also jumped nearly 11% from the prior year to $173 per record. IP may grow even more accessible as gen AI initiatives push this data and other highly proprietary data closer to the surface. With critical data becoming more dynamic and active across environments, businesses will need to reassess the security and access controls surrounding it.

Other key findings in the 2024 Cost of a Data Breach Report include:

- **Stolen credentials topped initial attack vectors** – At 16%, stolen/compromised credentials was the most common initial attack vector. These breaches also took the longest to identity and contain at nearly 10 months.
- **Fewer ransoms paid when law enforcement is engaged –** By bringing in law enforcement, ransomware victims saved on average nearly $1 million in breach costs compared to those who didn't – that savings excludes the ransom payment for those that paid. Most ransomware victims (63%) who involved law enforcement were also able to avoid paying a ransom.
- **Critical infrastructure organizations see highest breach costs** - Healthcare, financial services, industrial, technology and energy organizations incurred the highest breach costs across industries. For the 14th year in a row, healthcare participants saw the costliest breaches across industries with average breach costs reaching $9.77 million.
- **Breach costs passed to consumers -** Sixty-three percent of organizations stated they would increase the cost of goods or services because of the breach this year – a slight increase from last year (57%) – this marks the third consecutive year that the majority of studied organizations stated they would take this action.

Additional Sources

- Download a copy of the 2024 Cost of a Data Breach Report.
- Sign up for the 2024 IBM Security Cost of a Data Breach webinar on Tuesday, August 13, 2024, at 11:00 a.m. ET.
- Read more about the report's top findings in this IBM Security Intelligence blog.

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 the competitive edge in their industries. More than 4,000 government 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 ibm.com for more information.

Media Contact:
Georgia Prassinos
IBM
gprassinos@ibm.com

SOURCE IBM

Additional assets available online: Photos (1)
Video (1)

https://stage.mediaroom.com/ibmnewsroom/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs