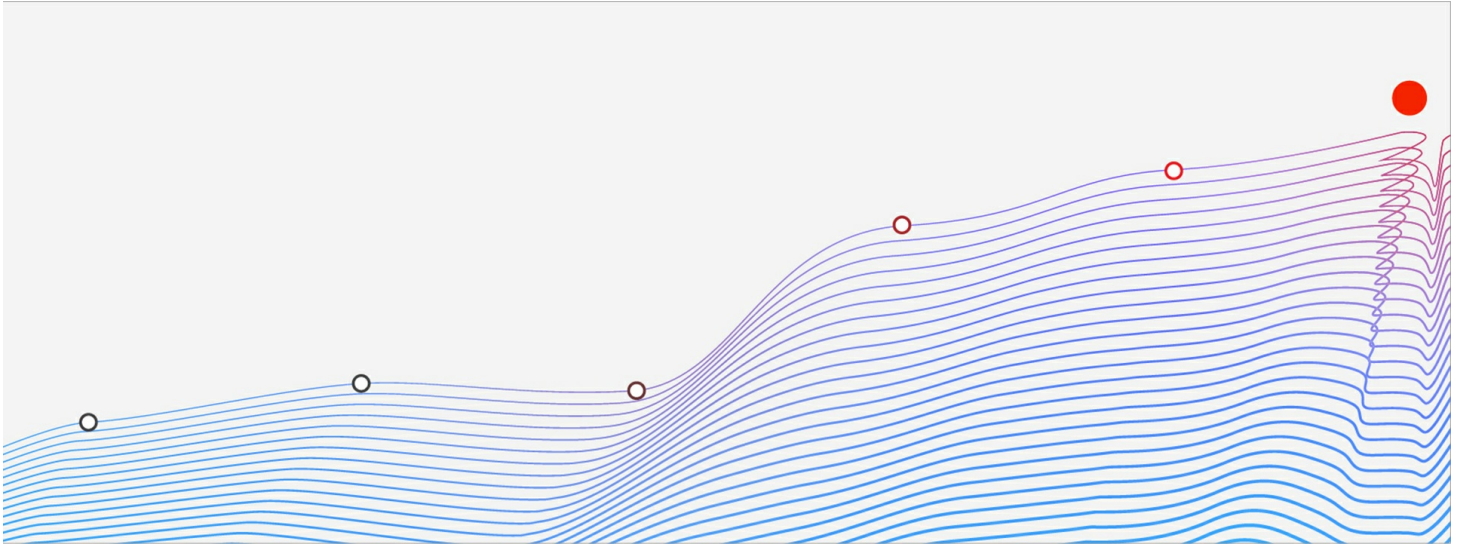


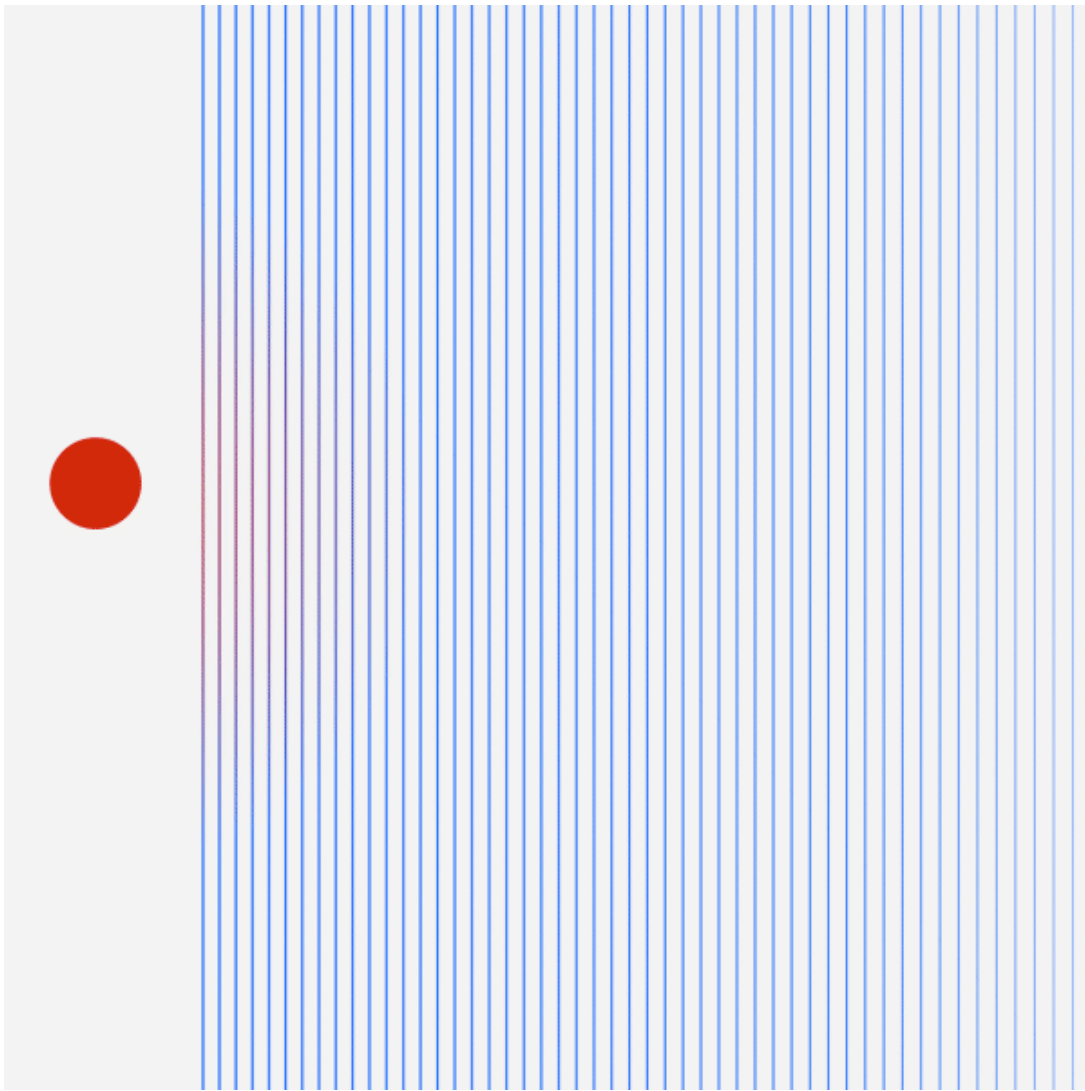
IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs

AI/Automation cut breach lifecycles by 108 days; \$470,000 in extra costs for ransomware victims that avoid law enforcement; Only one third-of organizations detected the breach themselves



CAMBRIDGE, Mass., July 24, 2023 /PRNewswire/ -- IBM (NYSE: [IBM](#)) Security today released its annual [Cost of a Data Breach Report](#),¹ showing the global average cost of a data breach reached \$4.45 million in 2023 – an all-time high for the report and a 15% increase over the last 3 years. Detection and escalation costs jumped 42% over this same time frame, representing the highest portion of breach costs, and indicating a shift towards more complex breach investigations.

According to the 2023 IBM report, businesses are divided in how they plan to handle the increasing cost and frequency of data breaches. The study found that while 95% of studied organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%).



The 2023 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 553 organizations globally between March 2022 and March 2023. The research, sponsored and analyzed by IBM Security, was conducted by Ponemon Institute and has been published for 18 consecutive years. Some key findings in the 2023 IBM report include:

- **AI Picks Up Speed** – AI and automation had the biggest impact on speed of breach identification and containment for studied organizations. Organizations with extensive use of both AI and automation experienced a data breach lifecycle that was 108 days shorter compared to studied organizations that have not deployed these technologies (214 days versus 322 days).
- **The Cost of Silence** – Ransomware victims in the study that involved law enforcement saved \$470,000 in average costs of a breach compared to those that chose not to involve law enforcement. Despite these potential savings, 37% of ransomware victims studied did not involve law enforcement in a ransomware attack.
- **Detection Gaps** – Only one third of studied breaches were detected by an organization's own security team, compared to 27% that were disclosed by an attacker. Data breaches disclosed by the attacker cost nearly \$1 million more on average compared to studied organizations that identified the breach themselves.

"Time is the new currency in cybersecurity both for the defenders and the attackers. As the report shows, early detection and fast response can significantly reduce the impact of a breach," said Chris McCurdy, General Manager, Worldwide IBM Security Services. "Security teams must focus on where adversaries are the most successful and concentrate their efforts on stopping

them before they achieve their goals. Investments in threat detection and response approaches that accelerate defenders speed and efficiency – such as AI and automation – are crucial to shifting this balance."

Ransomware victims saved time and money when they involved law enforcement

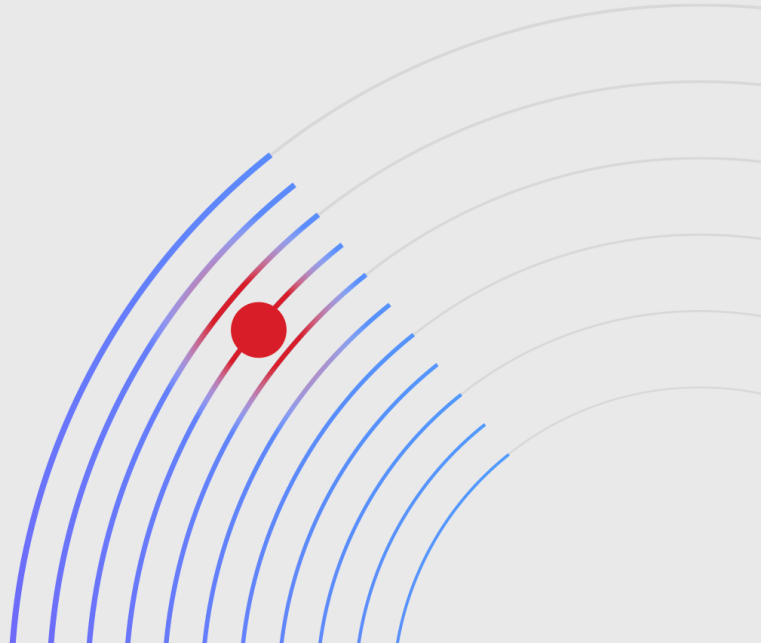
\$470,000

saved in average costs of a breach

33 Days

cut from the average breach life cycle

Source: IBM Security Cost of a Data Breach Report 2023



Every Second Counts

According to the 2023 report, studied organizations that fully deploy security AI and automation saw 108-day shorter breach lifecycles on average compared to organizations not deploying these technologies – and experienced significantly lower incident costs. In fact, studied organizations that deployed security AI and automation extensively saw, on average, nearly \$1.8 million lower data breach costs than organizations that didn't deploy these technologies – the biggest cost saver identified in the report.

At the same time, adversaries have reduced the average [time to complete a ransomware attack](#). And with nearly 40% of studied organizations not yet deploying security AI and automation, there is still considerable opportunity for organizations to boost detection and response speeds.

Ransomware 'Discount Code'

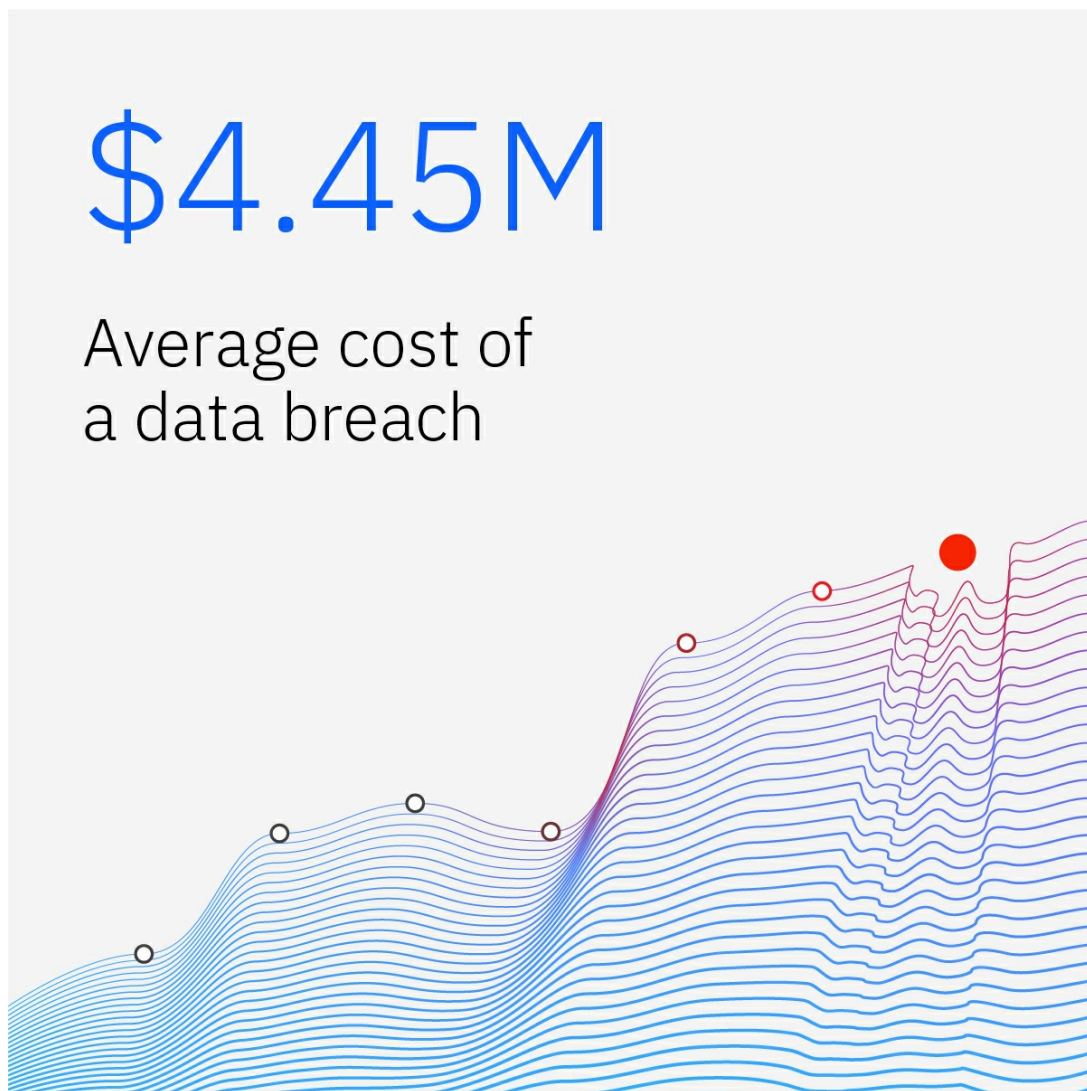
Some studied organizations remain apprehensive to engage law enforcement during a ransomware attack due to the perception that it will only complicate the situation. For the first time this year, the IBM report looked closer at this issue and found evidence to the contrary. Participating organizations that did not involve law enforcement experienced breach lifecycles that were 33-days longer on average than those that did involve law enforcement – and that silence came with a price. Ransomware victims studied that didn't bring in law enforcement paid on average \$470,000 higher breach costs than those that did.

Despite ongoing efforts by law enforcement to collaborate with ransomware victims, 37% of respondents still opted not to bring them in. Add to that, nearly half (47%) of studied ransomware victims reportedly paid the ransom. It's clear that organizations should abandon these misconceptions around ransomware. Paying a ransom, and avoiding law enforcement, may only drive-up incident costs, and slow the response.

Security Teams Rarely Discover Breaches Themselves

Threat detection and response has seen some progress. According to IBM's [2023 Threat Intelligence Index](#), defenders were able to halt a higher proportion of ransomware attacks last year. However, adversaries are still finding ways to slip through the cracks of defense. The report found that only one in three studied breaches were detected by the organization's own security teams or tools, while 27% of such breaches were disclosed by an attacker, and 40% were disclosed by a neutral third party such as law enforcement.

Responding organizations that discovered the breach themselves experienced nearly \$1 million less in breach costs than those disclosed by an attacker (\$5.23 million vs. \$4.3 million). Breaches disclosed by an attacker also had a lifecycle nearly 80 days longer (320 vs. 241) compared to those who identified the breach internally. The significant cost and time savings that come with early detection show that investing in these strategies can pay off in the long run.



Additional findings in the 2023 IBM report include:

- **Breaching Data Across Environments** – Nearly 40% of data breaches studied resulted in the loss of data across multiple environments including public cloud, private cloud, and on-prem—showing that attackers were able to compromise multiple environments while avoiding detection. Data breaches studied that impacted multiple environments also led to higher breach costs (\$4.75 million on average).
- **Costs of Healthcare Breaches Continue to Soar** – The average costs of a studied breach in healthcare reached nearly

\$11 million in 2023 – a 53% price increase since 2020. Cybercriminals have started making stolen data more accessible to downstream victims, according to the 2023 [X-Force Threat Intelligence Report](#). With medical records as leverage, threat actors amplify pressure on breached organizations to pay a ransom. In fact, across all industries studied, customer personally identifiable information was the most commonly breached record type and the costliest.

- **The DevSecOps Advantage** – Studied organizations across all industries with a high level of DevSecOps saw a global average cost of a data breach nearly \$1.7 million lower than those studied with a low level/no use of a DevSecOps approach.
- **Critical Infrastructure Breach Costs Break \$5 Million** – Critical infrastructure organizations studied experienced a 4.5% jump in the average costs of a breach compared to last year – increasing from \$4.82 million to \$5.04 million – \$590K higher than the global average.

Additional Sources

- To download a copy of the 2023 Cost of a Data Breach Report, please visit <https://www.ibm.com/security/data-breach>.
- Read more about the report's top findings in this IBM Security Intelligence [blog](#).
- Sign up for the 2023 IBM Security Cost of a Data Breach webinar on Tuesday, August 1, 2023, at 11:00 a.m. ET [here](#).
- Connect with the IBM Security X-Force team for a personalized review of the findings: <https://ibm.biz/book-a-consult>.
- For a closer look at the report recommendations visit: [Cost of a Data breach Action Guide](#).

About IBM Security

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

Media Contact:



Cassy Lalan

IBM Communications, Security

cllalan@us.ibm.com | Chicago

¹ The 2023 Cost of a Data Breach Report, conducted by Ponemon Institute, is sponsored and analyzed by IBM Security.

SOURCE IBM

Additional assets available online:  [Photos \(1\)](#)  [Video \(1\)](#)



<https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend->

