

IBM Report: Total Cost of a Data Breach for Businesses in the Middle East reaches SAR 29.9 million – the highest in 10 years

- The financial sector experienced the highest total data breach costs, reaching SAR 35.29 million.
- Organizations with security AI/Automation experienced SAR 12.22 million lower data breach costs than organizations that didn't deploy these technologies.



23, August 2023, Riyadh, Saudi Arabia -- IBM (NYSE: [IBM](#)) Security has released its annual [Cost of a Data Breach Report](#), highlighting that the total cost of a data breach for organizations in the Middle East reached SAR 29.9 million in 2023 — an all-time high for the report. This represents a 15% increase over the last three years and a marked 155.9% increase over the last decade. These figures highlight the importance of advanced solutions to protect businesses and entities across the Middle East in an increasingly connected world.

In the Middle East, four process-related activities drive the range of expenditures associated with an organization's data breach. Lost business costs topped the list, reaching SAR 10.02 million. This was followed by post-breach responses at SAR 8.86 million, detection and escalation costs at SAR 8.36 million, and notifying relevant stakeholders at SAR 2.36 million.

The 2023 IBM report highlights that the financial sector experienced the highest total cost of data breaches, reaching SAR 35.29 million. The region's energy industry ranked second, reaching SAR 33.75 million, while the

healthcare sector's total cost of a data breach reached SAR 32.46 million.

At a time when digital transformation is reshaping the global economic landscape, presenting both opportunities and unprecedented challenges to businesses and organizations around the world, the IBM report outlines the scale and nature of security issues that Middle Eastern entities must contend with.

AI Picks Up Speed

AI and automation had the greatest impact on the speed of breach identification and containment for studied organizations - showcasing the value of advanced technology and solutions to enhancing security. The 2023 report shows that organizations based in the Middle East that deployed security AI and automation extensively experienced significantly shorter data breach lifecycles — a total of 259 days. In stark contrast, organizations that did not deploy these technologies experienced data breach lifecycles of 393 days — 134 days more.

The report also states that organizations that deployed security AI and automation extensively saw, on average, SAR 12.22 million lower data breach costs than organizations that did not deploy these technologies.

“With the Middle East's rapid growth and development, there has been an increase in cyber attacks.” said Saad Toma, General Manager, IBM Middle East and Africa. “Early detection and fast response can significantly mitigate the damage caused by a data breach. Investments in advanced threat detection and response technologies, using AI and automation, are essential for organizations to stay ahead of cybercriminals.”

“With each passing day, the global economic landscape grows more sophisticated, presenting new and unprecedented challenges for businesses to overcome,” said Fahad Alanazi, General Manager, IBM Saudi Arabia. “This demands equally sophisticated solutions that are fully geared towards empowering organizations to scale the wide-ranging hurdles that line the road to lasting success. At IBM, we pride ourselves on pioneering world-class offerings that safeguard the people, entities and communities we serve. As data breaches become even more damaging and costly, these solutions are essential to helping businesses in the Kingdom navigate the challenges of today's economic environment.”

In the Middle East, some additional key findings showed that:

- **Phishing was the most common cause for data breaches** - constituting 16% breaches experienced in the region and costing businesses and entities SAR 32.2 million. Unknown (zero-day) vulnerabilities accounted for 15%, while attacks through stolen or compromised credentials represented 13% of breaches experienced in the Middle East.
- **Breaching Data Across Environments** - Over 37% of data breaches studied resulted in data loss across multiple environments — showing that attackers could compromise multiple environments while avoiding detection. Data breaches impacting multiple environments also led to higher costs (SAR 33.20 million on average).
- **Reducing the Cost of a Data Breach** - The IBM report pinpoints AI and machines learning-driven insights and attack surface management (ASM) tools as two of the most essential factors that can be deployed to reduce the cost of a data breach, reducing costs by SAR 1.13 million and SAR 1.08 million respectively.

The 2023 Cost of Data Breach Report is based on an in-depth analysis of real-world data breaches experienced

by 553 organizations globally (including 36 in Saudi Arabia and the UAE) 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.

- END -

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](#).
- 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.

<https://mea.newsroom.ibm.com/IBM-Report-Total-Cost-of-a-Data-Breach-for-Businesses-in-the-Middle-East>