IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High

Jul 26, 2022

- 60% of breached businesses raised product prices post-breach; vast majority of critical infrastructure lagging in zero trust adoption; $550,000 in extra costs for insufficiently staffed businesses

India & CAMBRIDGE, Mass., July 27, 2022 – IBM Security today released the annual Cost of a Data Breach Report,[1] revealing costlier and higher-impact data breaches than ever before, with the global average cost of a data breach reaching an all-time high of $4.35 million for surveyed organizations. With breach costs increasing nearly 13% over the last two years of the report, the findings suggest these incidents may also be contributing to rising costs of goods and services. In fact, 60% of studied organizations raised their product or services prices due to the breach, when the cost of goods is already soaring worldwide amid inflation and supply chain issues.

The perpetuality of cyberattacks is also shedding light on the "haunting effect" data breaches are having on businesses, with the IBM report finding 83% of studied organizations have experienced more than one data breach in their lifetime. Another factor rising over time is the after-effects of breaches on these organizations, which linger long after they occur, as nearly 50% of breach costs are incurred more than a year after the breach.

The 2022 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 550 organizations globally between March 2021 and March 2022. The research, which was sponsored and analyzed by IBM Security, was conducted by the Ponemon Institute.

Some of the key findings in the 2022 IBM report include:

- **Critical Infrastructure Lags in Zero Trust –** Almost 80% of critical infrastructure organizations studied don't adopt zero trust strategies, seeing average breach costs rise to $5.4 million – a $1.17 million increase compared to those that do. All while 28% breaches amongst these organizations were ransomware or destructive attacks.

- **It Doesn't Pay to Pay –** Ransomware victims in the study that opted to pay threat actors' ransom demands saw only $610,000 less in average breach costs compared to those that chose not to pay – not including the cost of the ransom. Factoring in the high cost of ransom payments, the financial toll may rise even higher, suggesting that simply paying the ransom may not be an effective strategy.

- **Security Immaturity in Clouds –** Forty-three percent of studied organizations are in the early stages or have not started applying security practices across their cloud environments, observing over $660,000 on average in higher breach costs than studied organizations with mature security across their cloud environments.

- **Security AI and Automation Leads as Multi-Million Dollar Cost Saver** – Participating organizations fully deploying security AI and automation incurred $3.05 million less on average in breach costs compared to studied organizations that have not deployed the technology – the biggest cost saver observed in the study.

Read the full global release: https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

India Data Points

- **INR 176 million - Average total cost of a data breach** : Reaching an all-time high, the cost of a data breach averaged 176 million in 2022. This represents a 6.6% increase from last year, when the average cost of a breach was 165 million. The average cost has climbed 25% from 140 million in the 2020 report.

- **INR 6,100 - Average per record cost of a data breach hit an eleven-year high:** India's average per-record cost of a data breach in 2022 was 6,100, a 3.3% increase from 5900 in 2021. The increase from 5522 in 2020 is an increase of 10.4%.

- **29,500 - Average records breached in 2022**

- **Top three industries per record cost- Industrial- INR 9024; Services- INR 7085; Technology Sector – INR 6900**
    - Industrial (Chemical processing, engineering, and manufacturing companies) was highest cost industry. The average total cost of a breach in industrial industry, comprised of chemical, engineering and manufacturing organizations, was reported at INR 9,024 in 2022.

    - Following industrial industry were the Services industry comprised of professional services such as legal, accounting and consulting firms and technology industries comprising software and hardware companies. The services industry reported average total cost of a breach at INR 7,085 while the technology industry, reported average total cost of a breach at INR 6,900.

- **Post Breach response costs surpassed other costs as the largest of four cost categories comprising the cost of a data breach, continuously for the 6th year**: Broken down into four cost categories — lost business, detection and escalation, notification and post breach response — the largest share of data breach costs in 2022 was post breach response, at INR 71 million. Post Breach response costs increased from INR 67.20 million in 2021 to INR 71 million in 2022, an increase of 5.65%.

- Top three primary initial attack vector for data breach- **stolen or compromised credentials** – INR 216 millions; **Phishing** - INR 206 millions; **Accidental data loss or lost device** – INR 190 millions.

- The average mean time to identify a data breach **decreased** from **239 to 221 days** and the average mean time to contain a data breach **increased** from **81 to 82 days.**

- Further, we witnessed organizations with less than 50% remote work adoption took 212 days as the average mean time to identify a data breach and 75 days as the average mean time to contain a data breach.

- However, organizations with over 50% remote work adoption took 266 days as the average mean time to identify a data breach and 91 days as the average mean time to contain a data breach.

- **Impact of zero trust on total cost of a data breach:** Organizations in India that are in the mature stages of adopting zero trust deployment witnessed INR 151 million as the total cost of a data breach as compared to organizations who have not yet started zero trust deployment and witnessed INR 246 millions as the total cost of data breach. This cost was INR 95 million more than breaches at mature organizations, a difference of 62.9%.

- **Factors that may increase or decrease the cost of a data breach**

    - AI platforms, engaged red team testing and Extended detection and response or XDR technologies were the three factors associated with the highest cost decrease.

    - Third party involvement, occurrence of cloud migration (when the organization is in the process of migrating to the cloud) and IoT and OT (Operational Technology) environment being impacted were the three factors associated with the highest cost increase.

- **State of security automation comparing three levels of deployment** - Fully deployed security automation was 30% in 2022. The share of organizations with partial or no security automation deployed was 35%.

- Breaches at **organizations with mature cloud security**, cost an average of INR 160 million, compared to INR 190 million at mid-stage organizations, INR 192 million at early-stage organizations. The cost difference between mature stage and early stage represented a 16.6% savings for mature stage organizations.

Speaking on the findings, **Viswanath Ramaswamy, Vice President, Technology, IBM Technology Sales, IBM India and South Asia** said, “Today, we have reached a point where cyberattacks are evolving into market stressors, hurting the economy. 60% of global businesses have raised their prices as a result of the data breach, contributing to inflation, and inadvertently passing the cost on to customers. Hackers are exploiting these circumstances to force organizations to pay ransoms, which is further compounded by the cyber skills shortage. Essentially, this is all leading to the creation of a “cyber tax” – where businesses can pass some of the costs of a breach on to the consumer.

India findings from Cost of Data Breach 2022 report illustrate the growing magnitude of the threat over time, with average data breaches costing 176 million, a 6.6% increase from 2021. It’s clear, businesses cannot evade

cyberattacks. Keeping security capabilities flexible enough to match attacker agility will be the biggest challenge as the industry moves forward. To stay on top of growing cybersecurity challenges investment in zero-trust deployments, mature security practices, and AI-based platforms can help make all the difference when businesses are attacked."

Additional Data Breach Statistics

- To download a copy of the 2022 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 2022 IBM Security Cost of a Data Breach webinar on Wednesday, August 3, 2022, 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.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. 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. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

---

[1] Cost of a Data Breach Report 2022, conducted by Ponemon Institute, sponsored and analyzed by IBM

Blog Categories

Secure