# IBM Report: Cost of a Data Breach Hits Record High During Pandemic

Jul 27, 2021

- *Data breaches cost surveyed companies $4.24 million per incident on average; highest in 17-year report history*
- *Adoption of AI, hybrid cloud, and zero trust approach lowered data breach costs*

**India & CAMBRIDGE, Mass., July 28, 2021** – IBM (NYSE: IBM) Security today announced the results of a global study which found that data breaches now cost surveyed companies $4.24 million per incident on average – the highest cost in the 17-year history of the report. Based on in-depth analysis of real-world data breaches experienced by over 500 organizations, the study suggests that security incidents became more costly and harder to contain due to drastic operational shifts during the pandemic, with costs rising 10% compared to the prior year.

Businesses were forced to quickly adapt their technology approaches last year, with many companies encouraging or requiring employees to work from home, and 60% of organizations moving further into cloud-based activities during the pandemic.[1] The new findings released today suggest that security may have lagged behind these rapid IT changes, hindering organizations' ability to respond to data breaches.

The annual cost of a Data Breach Report, conducted by Ponemon Institute and sponsored and analyzed by IBM Security, identified the following trends amongst the organizations studied:

- **Remote work impact:** The rapid shift to remote operations during the pandemic appears to have led to more expensive data breaches. Breaches cost over $1 million more on average when remote work was indicated as a factor in the event, compared to those in this group without this factor ($4.96 vs. $3.89 million.)[2]
- **Healthcare breach costs surged:** Industries that faced huge operational changes during the pandemic (healthcare, retail, hospitality, and consumer manufacturing/distribution) also experienced a substantial increase in data breach costs year over year. Healthcare breaches cost the most by far, at $9.23 million per incident – a $2 million increase over the previous year.
- **Compromised credentials led to compromised data:** Stolen user credentials were the most common root cause of breaches in the study. At the same time, customer personal data (such as name, email, password) was the most common type of information exposed in data breaches – with 44% of breaches

including this type of data. The combination of these factors could cause a spiral effect, with breaches of username/passwords providing attackers with leverage for additional future data breaches.

- **Modern approaches reduced costs:** The adoption of AI, security analytics, and encryption were the top three mitigating factors shown to reduce the cost of a breach, saving companies between $1.25 million and $1.49 million compared to those who did not have significant usage of these tools. For cloud-based data breaches studied, organizations that had implemented a hybrid cloud approach had lower data breach costs ($3.61m) than those who had a primarily public cloud ($4.80m) or primarily private cloud approach ($4.55m).

**Read the full global release:** https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

**India data points**

- ₹165 million was the average total cost of a data breach in the 2021 study, an increase of 17.85% from 2020
- ₹5,900 was the cost per lost or stolen record in the 2021 study, an increase of 6.85% from 2020
- 27,966 average records breached between May 2020 and March 2021
- Top three industries per record cost- Financial- ₹5536; Education- ₹3139; Public Sector ₹2100
- Top three primary initial attack vector for data breach- Phishing- ₹ 247.24 millions; Malicious Insider- ₹ 242.66 millions; Physical security compromise- ₹ 242.13 millions
- The average mean time to identify a data breach increased from 230 to 239 days and the average mean time to contain a data breach decreased from 83 to 81 days
    - Further, we witnessed organizations with less than 50% remote work adoption took 208 days as the average mean time to identify a data breach and 72 days as the average mean time to contain a data breach
    - However, organizations with over 50% remote work adoption took 271 days as the average mean time to identify a data breach and 83 days as the average mean time to contain a data breach
- Organizations in India that are in the mature stages of adopting zero trust deployment witnessed ₹131.80 million as the total cost of a data breach as compared to organizations who are in the early stage of adoption and witnessed ₹198.75 millions as the total cost of data breach.

**Prashant Bhatkal, Security Software Sales Leader, IBM Technology Sales, India/South Asia,** *"The rapid shift to remote work witnessed a tremendous disruption of security programs. Organizations were focused on getting online and security became an afterthought. India witnessed a record high in Data Breach during the Pandemic leading to many organizations evaluating their security posture. It's important to learn from these findings every year and adopt an open approach required to address the fragmentation and complexity challenges facing security teams today coupled with embracing a zero trust strategy. Further, it is evident that with modernization including the adoption of AI, security analytics, and applying a zero trust approach, comes significantly decreased costs associated with data breaches. What's important is to learn and apply measures that saved organizations the most money when a breach occurred –including applying zero trust, automation, hybrid cloud, and encryption.*

**Methodology and Additional Data Breach Statistics**

The 2021 Cost of a Data Breach Report from IBM Security and Ponemon Institute is based on in-depth analysis of real-world data breaches of 100,000 records or less, experienced by over 500 organizations worldwide between May 2020 and March 2021. The report takes into account hundreds of cost factors involved in data breach incidents, from legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity.

To download a copy of the 2021 Cost of a Data Breach Report, please visit: ibm.com/databreach

Sign up for the 2021 Cost of a Data Breach Report webinar on August 18 at 11:00 AM ET, here: ibm.biz/CODBwebinar

**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] IBM Institute for Business Value: COVID-19 and the future of business

[2] Average cost of $4.96 million for those surveyed where remote work was a factor vs. $3.89 million when remote work was not a factor

## Blog Categories

Secure