IBM Newsroom

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

- 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

CAMBRIDGE, Mass., July 28, 2021 /PRNewswire/ -- 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).

"Higher data breach costs are yet another added expense for businesses in the wake of rapid technology shifts during the pandemic," said Chris McCurdy, Vice President and General Manager, IBM Security. "While data breach costs reached a record high over the past year, the report also showed positive signs about the impact of modern security tactics, such as AI, automation and the adoption of a zero trust approach – which may pay off in reducing the cost of these incidents further down the line."

Impact of Remote Work and Shift to Cloud on Data Breaches

With society leaning more heavily on digital interactions during the pandemic, companies embraced remote work and cloud as they shifted to accommodate this increasingly online world. The report found that these factors had a significant impact on data breach response. Nearly 20% of organizations studied reported that remote work was a factor in the data breach, and these breaches ended up costing companies $4.96 million (nearly 15% more than the average breach).

Companies in the study that experienced a breach during a cloud migration project had 18.8% higher cost than average. However, the study also found that those who were further along in their overall cloud modernization strategy ("mature" stage) were able to detect and respond to incidents more effectively – 77 days faster on average than those who were in early-stage adoption. Additionally, for cloud-based data breaches studied, companies 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).

Compromised Credentials a Growing Risk

The report also shed light on a growing problem in which consumer data (including credentials) is being compromised in data breaches, which can then be used to propagate further attacks. With 82% of individuals surveyed admitting they reuse passwords across accounts, compromised credentials represent both a leading

cause and effect of data breaches, creating a compounding risk for businesses.

- **Personal Data Exposed:** Nearly half (44%) of the breaches analyzed exposed customer personal data, such as name, email, password, or even healthcare data – representing the most common type of breached record in the report.
- **Customer PII Most Costly:** The loss of customer personal identifiable information (PII) was also the most expensive compared to other types of data ($180 per lost or stolen record vs $161 for overall per record average).
- **Most Common Attack Method:** Compromised user credentials were the most common method used as an entry point by attackers, representing 20% of breaches studied.
- **Longer to Detect & Contain:** Breaches resulting from compromised credentials took the longest to detect – taking an average of 250 days to identify (vs. 212 for the average breach.)

Businesses That Modernized Had Lower Breach Costs

While certain IT shifts during the pandemic increased data breach costs, organizations who said they did not implement any digital transformation projects in order to modernize their business operations during the pandemic actually incurred higher data breach costs. The cost of a breach was $750,000 higher than average at organizations that had not undergone any digital transformation due to COVID-19 (16.6% higher than the average).

Companies studied that adopted a zero trust security approach were better positioned to deal with data breaches. This approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources. Organizations with a mature zero trust strategy had an average data breach cost of $3.28 million – which was $1.76 million lower than those who had not deployed this approach at all.

The report also found that more companies were deploying security automation compared to prior years, leading to significant cost savings. Around 65% of companies surveyed reported they were partially or fully deploying automation within their security environments, compared to 52% two years ago. Those organizations with a "fully deployed" security automation strategy had an average breach cost of $2.90 million – whereas those with no automation experienced more than double that cost at $6.71 million.

Investments in incident response teams and plans also reduced data breach costs amongst those studied. Companies with an incident response team that also tested their incident response plan had an average breach cost of $3.25 million, while those that had neither in place experienced an average cost of $5.71 million

(representing a 54.9% difference.)

Additional findings from the 2021 report include:

- **Time to respond:** The average time to detect and contain a data breach was 287 days (212 to detect, 75 to contain) – which is one week longer than the prior year report.
- **Mega breaches:** Average cost of a mega breach was $401 million, for breaches between 50 million and 65 million records.[3] This is nearly 100x more expensive than the majority of breaches studied in the report (which ranged from 1,000-100,000 records.)
- **By industry:** Data breaches in healthcare were most expensive by industry ($9.23m), followed by the financial sector ($5.72m) and pharmaceuticals ($5.04m). While lower in overall costs, retail, media, hospitality and public sector experienced a large increase in costs vs. the prior year.
- **By country/region:** The US had the most expensive data breaches at $9.05 million per incident, followed by Middle East ($6.93m) and Canada ($5.4m).

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.

Media Contact:
Cassy Lalan
Media Relations, IBM Security
319-230-2232 (m)
cllalan@us.ibm.com

[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

[3] The 2021 Cost of a Data Breach Report examines the cost of a mega breach based on a separate analysis of a specific sample involving loss or theft of one million records or more. The mega breach sample is not included in the overall average data breach report calculations, which examines data breaches ranging from 1,000-100,000 records.

SOURCE IBM

Additional assets available online: Photos

https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic