IBM Newsroom

IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years

Breaches Pose Growing Risk for Small Businesses, Costing up to 5% of Annual Revenue

CAMBRIDGE, Mass., July 23, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the results of its annual study examining the financial impact of data breaches on organizations. According to the report, the cost of a data breach has risen 12% over the past 5 years[1] and now costs $3.92 million on average. These rising expenses are representative of the multiyear financial impact of breaches, increased regulation and the complex process of resolving criminal attacks.[2]

The financial consequences of a data breach can be particularly acute for small and midsize businesses. In the study, companies with less than 500 employees suffered losses of more than $2.5 million on average – a potentially crippling amount for small businesses, which typically earn $50 million or less in annual revenue.

For the first time this year, the report also examined the longtail financial impact of a data breach, finding that the effects of a data breach are felt for years. While an average of 67% of data breach costs were realized within the first year after a breach, 22% accrued in the second year and another 11% accumulated more than two years after a breach. The longtail costs were higher in the second and third years for organizations in highly-regulated environments, such as healthcare, financial services, energy and pharmaceuticals.

"Cybercrime represents big money for cybercriminals, and unfortunately that equates to significant losses for businesses," said Wendi Whitmore, Global Lead for IBM X-Force Incident Response and Intelligence Services. "With organizations facing the loss or theft of over 11.7 billion records in the past 3 years alone, companies need to be aware of the full financial impact that a data breach can have on their bottom line –and focus on how they can reduce these costs."

Sponsored by IBM Security and conducted by the Ponemon Institute, the annual Cost of a Data Breach Report is based on in-depth interviews with more than 500 companies around the world that suffered a breach over the past year.[3] The analysis takes into account hundreds of cost factors including legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity. Some of the top findings from this year's report include:

- **Malicious Breaches – Most Common, Most Expensive:** Over 50% of data breaches in the study resulted from malicious cyberattacks and cost companies $1 million more on average than those originating from accidental causes.
- **"Mega Breaches" Lead to Mega Losses:** While less common, breaches of more than 1 million records cost companies a projected $42 million in losses; and those of 50 million records are projected to cost companies $388 million.[4]
- **Practice Makes Perfect:** Companies with an incident response team that also extensively tested their incident response plan experienced $1.23 million less in data breach costs on average than those that had neither measure in place.
- **U.S. Breaches Cost Double:** The average cost of a breach in the U.S. is $8.19 million, more than double

the worldwide average.

- **Healthcare Breaches Cost the Most:** For the 9th year in a row, healthcare organizations had the highest cost of a breach – nearly $6.5 million on average (over 60% more than other industries in the study).

Malicious Breaches Pose a Growing Threat; Accidental Breaches Still Common
The study found that data breaches which originated from a malicious cyberattack were not only the most common root cause of a breach, but also the most expensive.

Malicious data breaches cost companies in the study $4.45 million on average **–** over $1 million more than those originating from accidental causes such as system glitch and human error. These breaches are a growing threat, as the percentage of malicious or criminal attacks as the root cause of data breaches in the report crept up from 42% to 51% over the past six years of the study (a 21% increase).

That said, inadvertent breaches from human error and system glitches were still the cause for nearly half (49%) of the data breaches in the report, costing companies $3.50 and $3.24 million respectively. These breaches from human and machine error represent an opportunity for improvement, which can be addressed through security awareness training for staff, technology investments, and testing services to identify accidental breaches early on. One particular area of concern is the misconfiguration of cloud servers, which contributed to the exposure of 990 million records in 2018, representing 43% of all lost records for the year according to the IBM X-Force Threat Intelligence Index[5].

Breach Response Remains Biggest Cost Saver
For the past 14 years, the Ponemon Institute has examined factors that increase or reduce the cost of a breach and has found that the speed and efficiency at which a company responds to a breach has a significant impact on the overall cost.

This year's report found that the average lifecycle of a breach was 279 days with companies taking 206 days to first identify a breach after it occurs and an additional 73 days to contain the breach. However, companies in the study who were able to detect and contain a breach in less than 200 days spent $1.2 million less on the total cost of a breach.

A focus on incident response can help reduce the time it takes companies to respond, and the study found that these measures also had a direct correlation with overall costs. Having an incident response team in place and extensive testing of incident response plans were two of the top three greatest cost saving factors examined in the study. Companies that had both of these measures in place had $1.23 million less total costs for a data breach on average than those that had neither measure in place ($3.51 million vs. $4.74 million).

Additional factors impacting the cost of a breach for companies in the study included:

- Number of compromised records: Data breaches cost companies around **$150 per record** that was lost or stolen.
- Companies that fully deployed **security automation technologies** experienced around half the cost of a breach ($2.65 million average) compared to those that did not have these technologies deployed ($5.16 million average).
- **Extensive use of encryption** was also a top cost saving factor, reducing the total cost of a breach by

$360,000.

- **Breaches originating from a third party** – such as a partner or supplier – cost companies $370,000 more than average, emphasizing the need for companies to closely vet the security of the companies they do business with, align security standards, and actively monitor third-party access.

Regional and Industry Trends

The study also examined the cost of data breaches in different industries and regions, finding that data breaches in the U.S. are vastly more expensive – costing $8.19 million, or more than double the average for worldwide companies in the study. Costs for data breaches in the U.S. increased by 130% over the past 14 years of the study; up from $3.54 million in the 2006 study.

Additionally, organizations in the Middle East reported the highest average number of breached records with nearly 40,000 breached records per incident (compared to global average of around 25,500.)

For the 9th year in a row, healthcare organizations in the study had the highest costs associated with data breaches. The average cost of a breach in the healthcare industry was nearly $6.5 million - over 60% higher than the cross-industry average.

Download Full Reports & Register for the Webinar

Click here to view the full 2019 Cost of a Data Breach Report.

You may also register to attend the IBM Security and Ponemon Institute webinar taking place Tuesday, July 30, 2019.

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 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 70 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
cllalan@us.ibm.com

[1] Comparison of the average global cost of a data breach from the 2014 Cost of a Data Breach Report to the 2019 report.

[2] IBM analysis based on Cost of a Data Breach Report data.

[3] The limitations of the report and methodologies employed can be found in the full Cost of a Data Breach Report.

[4] Mega breach cost calculations are based on an analysis of 14 companies, applying a Monte-Carlo analytic approach to simulate results of greater statistical significance.

[5] IBM X-Force Threat Intelligence Index 2019

SOURCE IBM

---

https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years?ref=kogni-io-read-latest-enterprise-data-security-article