IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses

Study for First Time Calculates the Full Cost of "Mega Breaches," as High as $350 Million

CAMBRIDGE, Mass., July 11, 2018 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the results of a global study examining the full financial impact of a data breach on a company's bottom line. Overall, the study found that hidden costs in data breaches – such as lost business, negative impact on reputation and employee time spent on recovery – are difficult and expensive to manage. For example, the study found that one-third of the cost of "mega breaches" (over 1 million lost records) were derived from lost business.

Sponsored by IBM Security and conducted by Ponemon Institute, the 2018 Cost of a Data Breach Study[1] found that the average cost of a data breach globally is $3.86 million,[2] a 6.4 percent increase from the 2017 report. Based on in-depth interviews with nearly 500 companies that experienced a data breach, the study analyzes hundreds of cost factors surrounding a breach, from technical investigations and recovery, to notifications, legal and regulatory activities, and cost of lost business and reputation.

This year for the first time, the study also calculated the costs associated with "mega breaches" ranging from 1 million to 50 million records lost, projecting that these breaches cost companies between $40 million and $350 million respectively.

"While highly publicized data breaches often report losses in the millions, these numbers are highly variable and often focused on a few specific costs which are easily quantified," said Wendi Whitmore, Global Lead for IBM X-Force Incident Response and Intelligence Services (IRIS). "The truth is there are many hidden expenses which must be taken into account, such as reputational damage, customer turnover, and operational costs. Knowing where the costs lie, and how to reduce them, can help companies invest their resources more strategically and lower the huge financial risks at stake."

Hidden Figures – Calculating the Cost of a Mega Breach

In the past five years, the amount of mega breaches (breaches of more than 1 million records) has nearly doubled - from just nine mega breaches in 2013, to 16 mega breaches in 2017.[3] Due to the small amount of mega breaches in the past, the Cost of a Data Breach study historically analyzed data breaches of around 2,500 to 100,000 lost records.

Based on analysis of 11 companies experiencing a mega breach over the past two years, this year's report uses statistical modelling to project the cost of breaches ranging from 1 million to 50 million compromised records. Key findings include:

- Average cost of a data breach of 1 million compromised records is nearly $40 million dollars
- At 50 million records, estimated total cost of a breach is $350 million dollars
- The vast majority of these breaches (10 out of 11) stemmed from malicious and criminal attacks (as opposed to system glitches or human error)
- The average time to detect and contain a mega breach was 365 days – almost 100 days longer than a smaller scale breach (266 days)

For mega breaches, the biggest expense category was costs associated with lost business, which was estimated at nearly $118 million for breaches of 50 million records – almost a third of the total cost of a breach this size. IBM analyzed the publicly reported costs of several high profile mega breaches, and found the reported numbers are often less than the average cost found in the study.[4] This is likely due to publicly reported cost often being limited to direct costs, such as technology and services to recover from the breach, legal and regulatory fees, and reparations to customers.

What Impacts the Average Cost of a Data Breach?

For the past 13 years, the Ponemon Institute has examined the cost associated with data breaches of less than 100,000 records, finding that the costs have steadily risen over the course of the study. The average cost of a data breach was $3.86

million in the 2018 study, compared to $3.50 million in 2014 – representing nearly 10 percent net increase over the past 5 years of the study.

The study also examines factors which increase or decrease the cost of the breach, finding that costs are heavily impacted by the amount of time spent containing a data breach, as well as investments in technologies that speed response time.

- The average time to identify a data breach in the study was 197 days, and the average time to contain a data breach once identified was 69 days.
- Companies who contained a breach in less than 30 days saved over $1 million compared to those that took more than 30 days ($3.09 million vs. $4.25 million average total)

The amount of lost or stolen records also impacts the cost of a breach, costing $148 per lost or stolen record on average. The study examined several factors which increase or decrease this cost:

- Having an incident response team was the top cost saving factor, reducing the cost by $14 per compromised record
- The use of an AI platform for cybersecurity reduced the cost by $8 per lost or stolen record
- Companies that indicated a "rush to notify" had a higher cost by $5 per lost or stolen record

This year for the first time, the report examined the effect of security automation tools which use artificial intelligence, machine learning, analytics and orchestration to augment or replace human intervention in the identification and containment of a breach. The analysis found that organizations that had extensively deployed automated security technologies saved over $1.5 million on the total cost of a breach ($2.88 million, compared to $4.43 million for those who had not deployed security automation.)

Regional and Industry Differences

The study also compared the cost of data breaches in different industries and regions, finding that data breaches are the costliest in the U.S. and the Middle East, and least costly in Brazil and India.

- U.S. companies experienced the highest average cost of a breach at $7.91 million, followed by the Middle East at $5.31 million.
- Lowest total cost of a breach was $1.24 million in Brazil, followed by $1.77 million in India.

One major factor impacting the cost of a data breach in the U.S. was the reported cost of lost business, which was $4.2 million – more than the total average cost of a breach globally, and more than double the amount of "lost business costs" compared to any other region surveyed. One major factor impacting lost business costs is customer turnover in the aftermath of a breach; in fact a recent IBM / Harris poll report found that 75 percent of consumers in the U.S. say that they will not do business with companies that they do not trust to protect their data.

For the 8th year in a row, Healthcare organizations had the highest costs associated with data breaches – costing them $408 per lost or stolen record – nearly three times higher than the cross-industry average ($148).

"The goal of our research is to demonstrate the value of good data protection practices, and the factors that make a tangible difference in what a company pays to resolve a data breach," said Dr. Larry Ponemon, chairman and founder of Ponemon Institute. "While data breach costs have been rising steadily over the history of the study, we see positive signs of cost savings through the use of newer technologies as well as proper planning for incident response, which can significantly reduce these costs."

Download Full Reports & Register for the Webinar

To download the 2018 Cost of a Data Breach Study: Global Overview, visit https://www.ibm.com/security/data-breach/

To view the digital infographic with study highlights, visit:https://costofadatabreach.mybluemix.net

To register to attend the IBM Security and Ponemon Institute webinar onJuly 26th at 11 a.m. ET, visit: https://ibm.biz/BdYDvf

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 35 billion security events per day in more than 130 countries, and has been granted more than 8,000 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

IBM Security Communications

319-230-2232

cllalan@us.ibm.com

[1] Data collection began February 2017 and interviews were completed in April 2018

[2] Average cost for data breaches of 2,500-100,000 lost or stolen records

[3] Source: IBM analysis of Privacy Rights Clearinghouse's Chronology of Data Breaches

[4] Equifax data breach reported to cost company $275 million; Target 2016 financial report estimated $292 million loss as a result of 2013 data breach; Ruby Corp (the parent company of Ashley Madison) reportedly paid $11.2 million for the settlement of its 2015 breach.

SOURCE IBM

Additional assets available online: Photos (1)