

ThreatRate RISK MANAGEMENT

CALCULATING THE COST OF MEGA SECURITY BREACHES

PUBLISHED
21 August 2018

CATEGORY
Other

OTHER · AUGUST 2018

Calculating the Cost of Mega Security Breaches

The Ponemon Institute in a study sponsored by IBM Security found that the global average cost of data breaches has increased by more than six percent from 2017 to 2018 to an average of nearly 3.9 million dollars. The study, 2018 Cost of a Data Breach Study, also, for the first time, studied so-called mega breaches whose record losses range from 1-50 million. The study also articulated some of hidden costs to an organization that occur during a data breach and that often are not, when costs reported, tabulated.

For example, in the mega breach category, the biggest cost was not related to remediating the actual data breach; rather, the largest expense related to mega breaches was lost business. This is often not included in publicly reported costs which typically report only costs related to legal, recovery costs, regulatory expenses, and customer reparations. The study found, as an example, that with a breach of 50 million records, the total costs could reach more than 350 million dollars.

The study also found that there is significant regional variation in costs related to data breaches. The United States and the Middle East were the costliest regions; whereas, countries such as Brazil and India were significantly lower. The study also found that the United States and the Middle East also spent the most on post-breach response activities such as help desk expenditures, legal expenses, discounts, and identity protection services. Interestingly, Canada – not the United States – had the highest direct costs. The United States, however, did have the highest indirect costs.

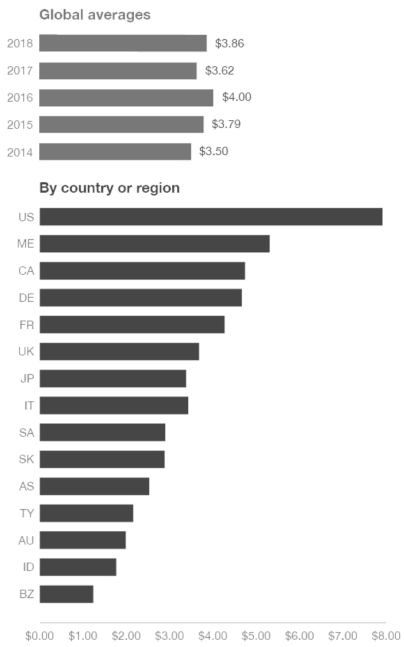
There were some factors that researchers found that led to lower overall incident costs during a data breach. Firms that, for example, found and contained a data breach in less than 30 days ended up saving more than a million dollars. Also, the existence of incident response teams saved up to 14 dollars per record, and the extensive use of encryption lowered the per record costs by 13 dollars.

Like the Ponemon and IBM Security study, Experian produced a data breach study that contained predictions about the future of data breaches and security in general. They found for example, that estimates of the number of IoT devices in use by 2025 will range from 25 to 50 billion. Such devices have, as the study noted, been susceptible to distributed denial-of-service attacks and may, in the future, continue to be vulnerable to cyberattacks. Experian also predicted that cyberattacks against nation-states will continue, and their motivations will continue to be political in nature. The researchers noted that cyberattacks are often difficult to attribute with high degrees of confidence; thus, they are an extremely useful tool for governmental actors that wish to covertly cause damage to other nations. Examples of such attacks recently – although they have not been fully attributed to governmental actors – are the 2017 attacks against the British and Scottish parliaments. The upcoming elections in the United States and the European Union are obvious targets for such attacks. Experian also predicted that the increase in artificial intelligence will likely both help to prevent attacks and lead to more

© 2018 ThreatRate Risk Management. All Rights Reserved

effective attacks (depending on the user).

It is evident to all observers that data breaches and cybersecurity in general remain evolving areas of study and concern that will change as technology improves and will increasingly become used as a tool that nations and criminal/terrorist groups use to assert dominance over competitors.



https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Soundbite analytics

- The number of so-called mega breaches – breaches of more than a million records – increased from nine in 2013 to 16 in 2017.
- The average time to detect and contain a mega breach was 365 days.
- The average time to detect and contain a smaller breach was 266 days.
- The average cost per stolen record is 148 dollars.
- The extensive use of automated security tools decreased the total cost of a breach by 1.5 million dollars.
- An IBM/Harris poll found that three-fourths of American consumers said that they will not do business with companies that they don't trust.

SOURCES

1 https://ponemon.org

2 https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

3 http://experian.com/assets/data-breach/white-papers/2018-experian-data-breach-industry-forecast.pdf

4 https://theguardian.com/politics/2017/aug/15/scottish-parliament-hit-by-cyber-attack-westminster-assault-holyrood-hackers-email

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT