the Availability Digest

www.availabilitydigest.com
@availabilitydig

The Cost of Data Breaches

January 2016

The theft of data from a company can have many consequences. Customers may leave and patronize other companies that they consider more secure. Government regulations may be violated. The data breach may inflict severe costs on the company.

The Ponemon Institute has released its tenth annual study on the cost of data breaches.[1] The study was sponsored by IBM and covers data breaches that occurred in 2014. 350 companies that actually suffered a data breach of less than 100,000 records are included in the study (mega-breaches were not included in the study as they tend to skew the results).

The cost of data breaches continues to rise. The average total cost of a data breach increased to $3.79 million,[2] up 23% since 2013. The average cost per breached record increased to $154, a 12% increase since 2013.

There is a growing concern among senior executives and boards of directors about the risks posed by data breaches and cyberattacks, including potential damage to a corporation's reputation, class action lawsuits, and costly mitigation. As a consequence, executives are paying greater attention to the security practices of their corporations in order to thwart data breaches.

Participating Companies

The companies that were involved in the study were located the United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, and the Arabian region (United Arab Emirates and Saudi Arabia). All participating organizations experienced a data breach ranging from 2,200 records to 101,000 records. A compromised record is one that identifies the individual whose information has been stolen or lost in a data breach.

The 350 companies in the study represented sixteen different industries.

Reasons for Higher Data-Breach Costs

There are three major reasons for the increase in data-breach costs:

- Cyberattacks have increased in frequency and in remediation costs. Malicious or criminal attacks represent 47% of all data breaches.

[1] 2015 Cost of Data Breach Study: Global Analysis, *Ponemon Institute*; May 2015.
http://www.ibm.com/security/data-breach
[2] All currency amounts are in U.S. dollars.

- The consequences of lost business are having a greater cost impact. This cost includes the abnormal turnover of customers, increased customer-acquisition activities, reputation losses, and diminished goodwill. The growing awareness of identity theft has contributed to the increase in lost business.

- Costs associated with detection and mitigation have increased. These costs include forensic and investigative activities, assessment and audit services, crisis-team management, notification of those affected, and communications to senior executives and boards of directors.

Main Causes of a Data Breach

There are three main causes of a data breach.

- 47% of data breaches are caused by malicious or criminal attacks. The most common types of malicious or criminal attacks include criminal insiders, malware infections, phishing/social engineering, and SQL injection. These attacks are also the most expensive on a per-record basis. The average cost per record compromised in such an attack is $170. Cost ranges from $230 in the U.S. to $71 in India.

- 29% of data breaches result from system glitches at an average cost of $142 per breached record. Costs range from $210 in the U.S. to $45 in India.

- 25% of data breaches are caused by human error, typically due to carelessness. Such a breach carries an average cost of $137 per breached record. Costs range from $201 in Germany ($198 in the U.S.) to $49 in India.

These proportions are fairly consistent across the twelve countries studied. Data-breach costs in India are low because India has no regulations requiring the notification of a data breach.

Data Breach Costs by Industry

The Ponemon study included sixteen industries. Those with the highest data-breach costs were Health ($363), Education ($300), Pharmaceuticals ($220), Financial ($215), and Communications ($179).

Time to Identify and Contain a Data Breach

Surprisingly, it takes a significant amount of time for a company to discover a data breach. This is because most of the time the data breach is noticed first by a third party, such as a bank that suddenly sees a raft of fraudulent purchases on its credit cards. It can then take some time for the data breach to be contained.

Mean Time to Identify (MTTI)

In the survey sample, the average time that it took to identify a data breach (MTTI) was 206 days. The maximum amount of time in the survey sample to identify a data breach was 582 days (over a year and a half!).

The root cause of the data breach was a factor in the MTTI. For a malicious or criminal attack, the MTTI was 256 days. For a system glitch, it was 173 days. For a human error, it was 158 days.

Mean Time to Contain (MTTC)

Once the data breach was identified, the average time to contain it (MTTC) was 69 days. For a malicious or criminal attack, the MTTC was 82 days. For a system glitch, the MTTC was 60 days. For a human error, the MTTC was 57 days.

Factors Affecting the Cost of a Data Breach

Several factors affect the cost of a data breach. Some are best practices that can reduce the cost. Others are expanded efforts to mitigate the effect of the data breach but that carry additional costs.

Major Cost Components of a Data Breach

There are four major cost components of a data breach:

- Lost Business has the most severe financial consequences. This category includes the abnormal loss of customers due to a data breach, increased customer-acquisition activities, reputation losses, and diminished goodwill. Lost business contributes $1.57 million to the cost of a data breach.

- Detection and Escalation activities add $0.99 million to the cost of a data breach. Detection includes activities that enable a company to detect the breach of data at rest or in motion. Escalation involves activities necessary to report the breach to appropriate personnel. These activities include forensic and investigative activities, assessment and audit services, crisis-team management, and communications to executive management and the board of directors.

- Notification activities inform affected people or companies of the data breach. These activities include the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to email or email bounce-backs, and inbound communications. Notification activities represent the lowest data-breach cost component, adding $0.17 million to the cost of a data breach.

- Post Data-Breach activities help victims of a breach to communicate with the company to ask additional questions or to obtain recommendations in order to minimize potential harm. These activities contribute $1.07 million to the cost of a data breach. Post data-breach costs include help-desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services, and regulatory interventions.

Best Practices to Reduce Costs

The following best practices can reduce the cost of a data breach:

- Maintain an incident response team that can immediately take actions to limit the effect of a data breach.
- Use encryption for data-at-rest and data-in-flight.
- Train employees on how to properly handle sensitive data and to avoid phishing attacks or other social-media incursions.
- Have a well-thought-out Business Continuity Management (BCM) plan, and involve all employees in the execution of the plan.
- Appoint a Chief Information Security Officer (CISO), and give him the authority to ensure the security of all data.
- Involve the Board of Directors in data-security issues.
- Acquire insurance to cover the cost of a data breach.

Factors That Increase Costs

The following factors can increase the costs of a data breach:

- Consultants retained to help identify the cause of the data breach and to mitigate its consequences.

- Rapid notification of those affected by the data breach.
- A data breach caused by lost or stolen devices.
- A data breach in which a third party was involved.

The Impact of a Business Continuity Management Plan

The Ponemon report focuses on the advantages of using a good BCM plan. The survey results indicated that a BCM plan reduced the per-record cost of a breach from $161 to $147 and reduced the total average cost of a data breach by $500,000, from $4 million to $3.5 million. It reduced the likelihood of a data breach form 28% to 21%.

A BCM decreased the MTTI from 234 days to 178 days and the MTTC from 83 days to 55 days.

Probability of a Data Breach

Based on its study, the Ponemon Institute has generated an algorithm that it believes will predict the probability that a data breach will occur in the next 24 months. The algorithm is based on two factors: the size of the data breach and the country. It applies to companies that already have had a data breach.

According to its algorithm, the probability of a company experiencing a data breach involving a minimum of 10,000 records in the next 24 months is estimated to be 22%. The probability of a data breach involving 100,000 records in the next 24 months is less than 1%.

This should be a wakeup call to executives whose companies have experienced a data breach to be on the lookout for another small data breach.

So far as countries are concerned, companies in Brazil are most likely to experience a data breach of at least 10,000 records (37%). Companies in the U.S. have a 22% probability of experiencing such a data breach, and Germany has a 16% chance, the lowest of all twelve countries.

Summary

Some of the main takeaways for executives who are concerned about data breaches are:

- Hackers and criminal insiders cause almost half of all data breaches.
- Business Continuity Management plays an important role in reducing the cost of a data breach.
- Reducing the time to identify and contain a data breach can reduce its cost.
- Board level involvement and obtaining insurance can reduce a data-breach cost.
- The loss of customers is one of the highest costs of a data breach, but it can be controlled with timely notification, which is a low-cost activity.

Data breaches are a fact of life, since hackers always seem to be smarter than those trying to protect the data. But there are steps to control the costs of the inevitable data breach.