Reputation Impact of a Data Breach
Executive Summary

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: October 2011

Reputation Impact of a Data Breach
Executive Summary
October 2011

We are pleased to present the findings of the *Reputation Impact of a Data Breach* conducted by Ponemon Institute and sponsored by Experian® Data Breach Resolution. In this report, we describe how a negative event such as a data breach can affect the reputation and brand image of an organization. We specifically examine how organizations were affected by a data breach and what steps are important to take in order to restore reputation and brand image.

We believe this is the first study to examine the relationship between the loss or theft of confidential customer, employee, and business information. As a result of this research, businesses can better understand how a potential data breach might affect their brand and reputation and what the potential financial consequences might be.

The study surveyed 843 senior-level individuals with deep expertise and knowledge about their organization's brand and reputation management objectives. Ninety-five percent of these respondents hold positions at the manager level or higher in their organization. More than 40 percent report directly to the CEO or other C-level executives in the organization and 26 percent report directly to the head of brand management or marketing and communications. Forty percent of respondents say that the CEO is most responsible in their organization for protecting the company's reputation or brand image.

We asked individuals participating in our study to estimate the economic value of their organizations' corporate brand or reputation. The responses ranged from a value of less than $1 million to greater than $10 billion. We determined the average value for the organizations participating in our study to be approximately $1.5 billion. Depending upon the type of information lost as a result of the breach, the average loss in the value of the brand ranged from $184 million to more than $330 million.

As a percentage of their organizations' annual gross revenues, the economic value of reputation and brand ranged from less than 10 percent to greater than 5X. Again, depending upon the type of breach, the value of brand and reputation could decline as much as 17 percent to 31 percent.

We also learned that it is not just the decline in the value that can harm an organization. For organizations in this study, respondents estimated that in some cases it could take longer than a year to recover and restore reputation and brand image.

The study focuses on the following four topics:

- How valuable is an organization's brand and reputation
- A calculation of the economic value of reputation and brand
- What type of data loss (customer, employee or intellectual property) has the greatest affect on reputation and brand
- The data breach experience of organizations in our study

Key Findings

Reputation is one of an organization's most important and valuable assets. Seventy-four percent of respondents say that their organizations' reputation is key and a similar percentage (73 percent) say that reputation and brand image are inextricably linked.

While reputation and brand image are perceived as very valuable, less than half of respondents (49 percent) say these are resilient assets and can withstand negative events, including a data breach. To keep reputation and brand as resilient as possible, the factors that are believed to make the most difference are good business practices, senior leadership and market leadership.

Calculating the value of reputation and brand reveals how valuable these assets are to an organization. The senior-level respondents in our study provided an estimate on the economic value of their organizations' corporate brand or reputation. The responses ranged from a value of less than $1 million to greater than $10 billion. We determined the average value for the organizations participating in our study to be approximately $1.5 billion. Depending upon the type of information lost as a result of the breach, the average loss in the value of the brand ranged from $184 million to more than $330 million.

As a percentage of their organizations' annual gross revenues, the economic value of reputation and brand ranged from less than 10 percent to greater than 5X. Again, depending upon the type of breach, the value of brand and reputation could decline as much as 17 percent to 31 percent of annual gross revenues.

The five most important factors contributing to an organization's brand and reputation are: financial health and stability, product or service quality, the company's leadership, Internet and social media communications and the company's history or legacy.

Not all data breaches are equal. Some breaches are more devastating than others to an organization's reputation and brand image, as described below. However, when asked to rank the information if lost or stolen would result in a diminished reputation or image respondents say customer information would be most devastating. This is followed by confidential financial business information and confidential non-financial business information.

Records containing confidential customer information are lost or stolen. We asked respondents to evaluate the consequences of an organization that had a data breach involving the loss or theft of more than 100,000 confidential consumer records. We also told them that the breach was widely reported in the media. Eighty-one percent of respondents say this would affect the economic value of their organization's reputation and brand image. According to respondents, the average diminished value of the brand as a direct result of the incident is 21 percent.

To restore the organization's reputation would take on average about one year (11.8 months). The most important steps to take, according to respondents, are to conduct an investigation and forensics, work closely with law enforcement, conduct employee training and awareness programs and protect customers from potential harms such as identity theft. Of least interest is to engage consultants to help remediate problems or gaps in systems. These steps seem to be based on the need to understand the root cause of the loss of customer records and to mitigate employee negligence through training and awareness.

Records containing confidential employee information are lost or stolen. We asked respondents to evaluate the consequences of an organization that had a data breach involving the loss or theft of more than 100,000 confidential employee records. Again, the breach was widely reported in the media. About half (51 percent) of respondents say this would affect the economic value of their organization's reputation and brand image. According to respondents, the average diminished value of the brand as a direct result of the incident is 12 percent.

To restore the organization's reputation would take an average of about 8 months. The most important steps to take, according to respondents, are to conduct investigations and forensics, work closely with law enforcement and protect employees from potential harms such as identity theft. While not considered as important as the first three steps, employee training and awareness programs would be conducted. Of least interest is to engage public relations and communications firms. These practices indicate again the need to understand the root cause of the data breach, protect those affected by the breach and improve employees' knowledge about how to reduce the risks associate with the handling of confidential information.

Records containing confidential business information are lost or stolen. We asked respondents to evaluate the consequences of an organization that had a data breach involving the loss or theft of trade secrets, new product designs, source code or strategic plans. The breach involved a small number of extremely sensitive files. Eighty percent of respondents say this would affect the economic value of their organization's reputation and brand image. According to respondents, the average diminished value of the brand as a direct result of the incident is 18 percent.

To restore the organization's reputation would take on average about 8 months. The most important steps to take, according to respondents, are to immediately respond to the incident, conduct investigations and forensics, work closely with law enforcement and conduct employee training and awareness programs. Of least interest is the need to engage consultants to help remediate problems or gaps in systems and engage a public relations and communications firm. These actions seem to be based on the need to make sure the theft of confidential business information is stopped quickly, prevent future theft and mitigate employee negligence through training and awareness.

Data breaches occur in most organizations represented in this study and have at least a moderate or a significant impact on reputation and brand image. According to 82 percent of respondents, their organizations had a data breach involving sensitive or confidential information. On average, they had 2.7 breaches in the past 2 years. Fifty-three percent say the data breaches had a moderate impact on reputation and brand image and 23 percent say it was significant. It is interesting to note that before having a data breach less than half had an incident response plan for customer data breaches in place. However, after the breach 76 percent say their organization put an incident plan in place.

Data breaches involving confidential employee information are less frequent than data breaches involving confidential customer information. Less than half (46 percent) of organization in this study had a data breach involving the loss or theft of sensitive or confidential employee information. On average, organizations reporting such breaches had 1.5 in the past two years. Only 23 percent say such a breach had a moderate or significant impact on their organization's reputation and brand image. While one-third say their organization had an incident response plan in place before the breach, 54 percent say they had such a plan in place following the breach.

Most organizations in our study have had a data breach involving the theft of sensitive or confidential business information. On average these have occurred 2.9 times in these organizations. It is interesting to note that of all types of breaches, the theft or loss of confidential financial information experienced by these organizations seemed to have the most significant impact. Forty-six percent say the impact was moderate and 29 percent say it was significant. Prior to having such a breach, 57 percent had an incident plan in place. However, after such an incident 80 percent say they put a plan in place.

Respondents strongly believe in understanding the root cause of the breach and protecting victims from identity theft. When asked what their organizations did following a breach to preserve or restore the top three steps are: conduct investigations and forensics, work

closely with law enforcement and protect those affected from potential harms such as identity theft. They also believe these are the most effective steps to take in order to preserve and restore reputation. Considered least effective is providing customers/employees with free or discounted products or services.

Conclusion

We believe this is the first study to show the serious impact a data breach can have on the economic value of an organization's reputation and brand image. Considered by respondents to be one of the most valuable assets an organization can have, reputation and brand image is not the most resilient. This is evidenced by the length of time it can take to restore a company's good name. In the case of a data breach involving confidential customer information it can take more than a year.

The findings of this study further demonstrate how devastating a data breach can be for an organization and how important it is to reduce the risk of such an incident. As is revealed in this study, respondents agree that the steps they are most likely to take following a breach are the same measures they believe can preserve and restore reputation and brand image. These steps involve investigating the breach to determine what happened and the extent of the harms, working with law enforcement and making sure victims of the breach are protected from identity theft.