Commissioned by

SCOTT & SCOTT

Independently Conducted by

Presents

The Business Impact of Data Breach

Publication by Ponemon Institute LLC

Dated May 15, 2007

The Business Impact of Data Breach

By Larry Ponemon, May 15, 2007

Scott & Scott and Ponemon Institute are pleased to report the results of a national survey that seeks to understand how a data breach affects an organization. The study focuses on the organization's response to the data breach, the most common causes of the breach and what measures are put in place to prevent a future breach based on lessons learned. We also compare the prevention practices of organizations that had a breach to those that have been spared. This independently conducted study queried a representative sample of 702 adult-aged respondents who are presently employed within U.S. organizations.

Following are the key questions in our inaugural study:

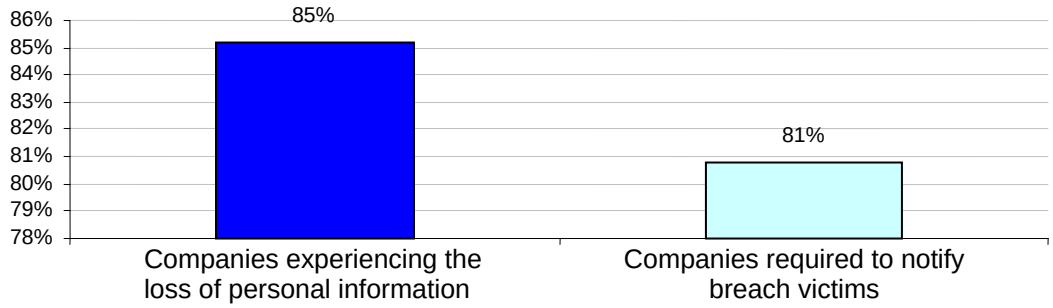
- Were organizations prepared to respond to the breach and what were the most important actions they took?
- Did they measure the cost of the breach to their organization?
- What caused the breach?
- How has the breach affected an organization's strategy for preventing a breach?
- What are the differences in approaches to the prevention and detection of a data breach between organizations that have experienced a breach and organizations that have not had a data breach?

Executive Summary

Following are the ten most salient findings of our study:

An overwhelming number of organizations are experiencing data breaches. Bar Chart 1 shows 85% of respondents report that they had a data breach involving the loss or theft of customer, consumer or employee data in the past 24 months. Further, 81% of the entire sample was required to notify individuals whose data was either lost or stolen based on requirements from state statutes (97%), banking regulations (29%), GLBA (20%) and other regulations.

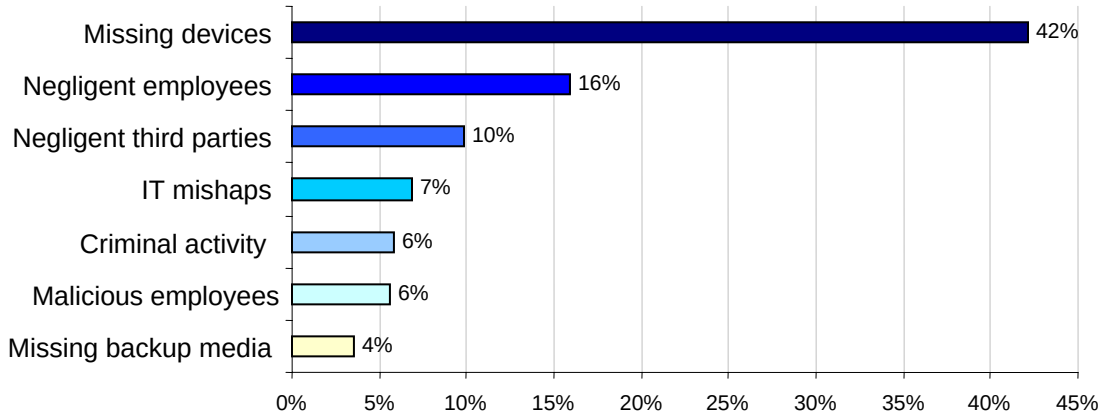
Bar Chart 1
Data breach statistics for the present sample



Data breaches are most likely to be caused by missing laptops, PDAs and memory sticks as well as employee negligence. Bar Chart 2 shows that 42% of respondents place the blame on lost or stolen equipment followed by negligent employees, temporary employees or contractors (16%) and negligent third parties, including vendors and outsourcers (10%). The most unlikely causes

include: malicious employees, temporary employees or contractors; criminal activity, IT mishaps or glitches and missing backup media.

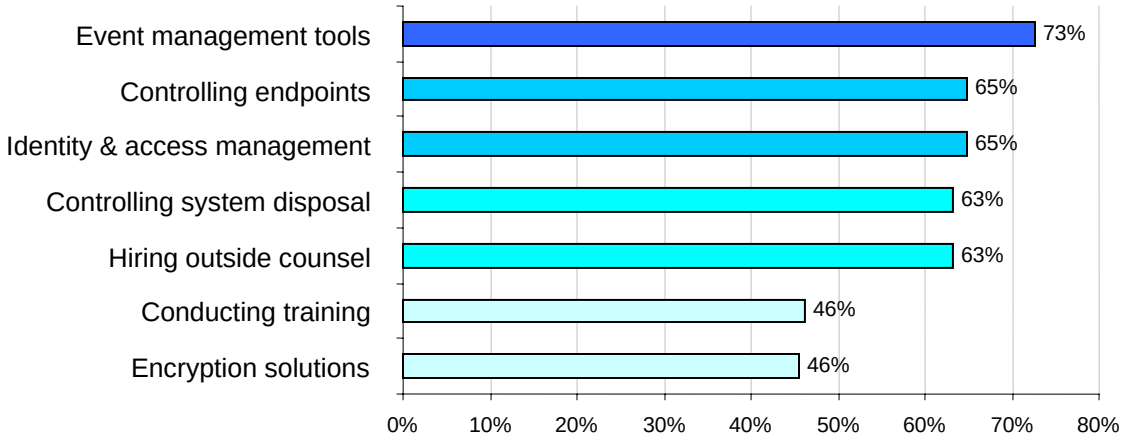
Bar Chart 2
Probable cause of the data breach event



Companies that experienced a data breach may **not** be implementing appropriate measures to prevent repeat incidents. Results in Bar Chart 3 show more than 73% of companies do not invest in event management security tools, and 65% are not taking steps to control endpoints to their organization's systems or networks. Another 65% are not using identity and access management solutions, 63% are not deploying tightly controlled storage device disposal procedures, and 63% do not hire outside legal counsel for incident planning.

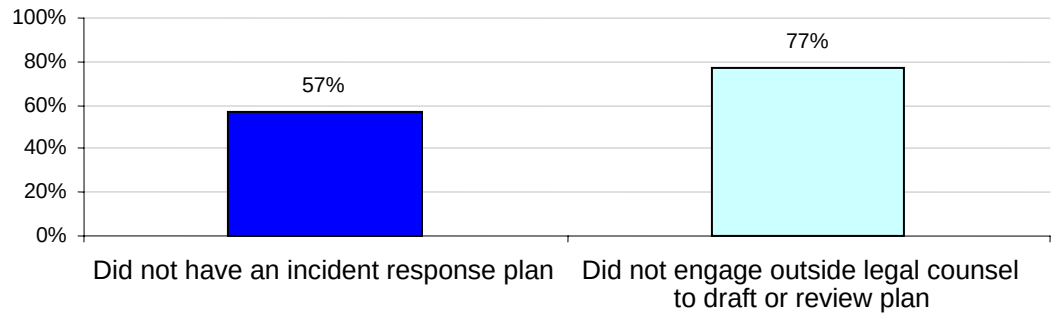
Despite the enormous benefits of having protected files in the event of a data breach, over 46% of companies that experienced data loss or theft do not deploy encryption solutions and do not conduct specialized training to raise awareness about data security and privacy.

Bar Chart 3
Post-Breach Organizational Failures



Organizations may not be prepared for data breaches. More than 57% of respondents did not have an incident response plan in place before the breach occurred. About 77% of companies did not engage outside legal counsel to help draft or edit an incident response plan. These results are shown in Bar Chart 4.

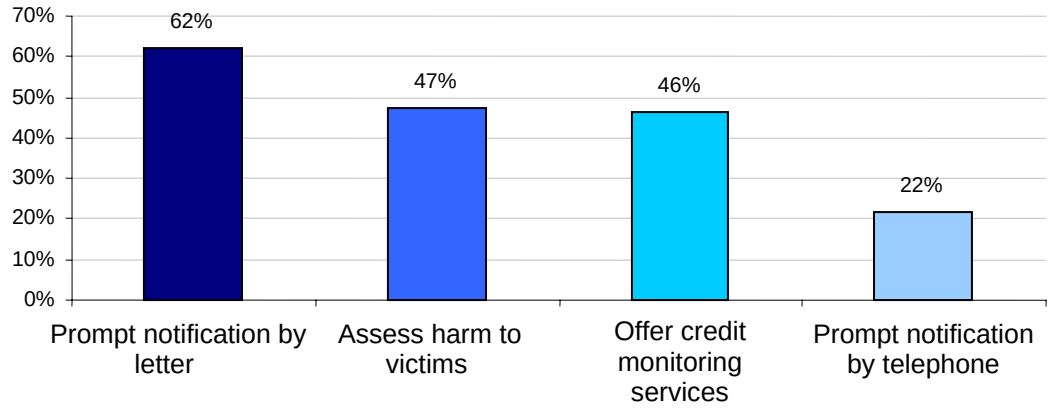
Bar Chart 4
Did you have an incident plan before the breach?



To protect the organization's reputation, many respondents believe it is important to promptly notify victims by letter and offer to help them with credit monitoring services. Other important steps include careful assessment of the types of harm victims experienced, the need to understand the organization's legal rights and obligations, and prompt notification to victims by telephone. Considered least important are offers to compensate victims with coupons or free services, voluntary notification of regulators, the use of forensic experts to determine the cause of the breach, response to media inquiries, prompt notification to regulators as required by law and placement of an ad in a newspaper to notify victims.

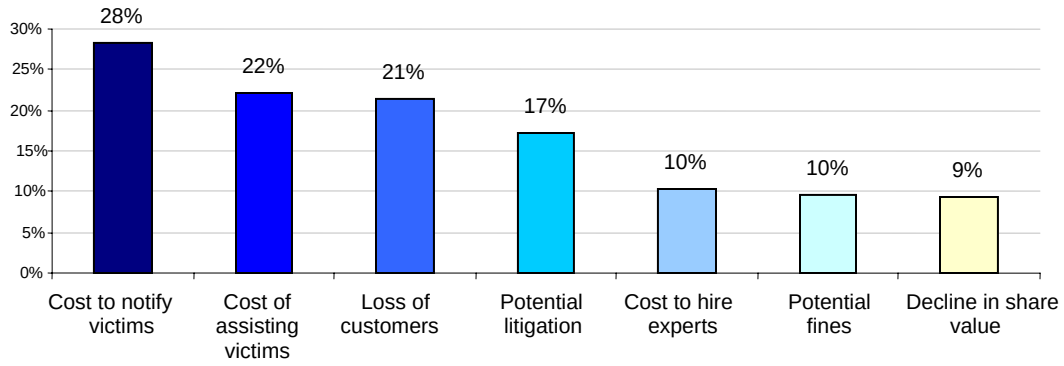
These results are summarized in Bar Chart 5. It is interesting to note that over 82% of respondents state that their organizations did **not** engage outside legal counsel to assist in the data breach planning process (see Table 4).

Bar Chart 5
Immediate response to data breach



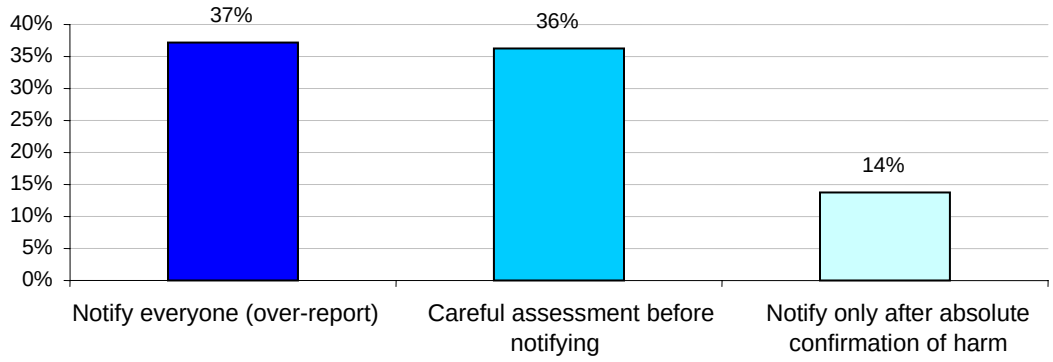
Only 29% of respondents calculated the financial impact of their organization's data breach. The two main reasons for not measuring the cost are that companies do not think they have enough information to determine cost or they do not think a cost analysis is applicable. Approximately 11% do not have any interest in knowing the cost. Those organizations that did measure the cost of the breach were most likely to use these measures in their calculation: the cost to notify victims, the cost of assisting victims, loss of customers, potential litigation and the cost to hire experts. Decline in share value and potential fines were the least used measures. Bar Chart 6 summarizes the cost attributes most likely to be used in the analysis.

Bar Chart 6
Cost included in analysis of data breach



A majority of respondents reported that their organizations attempt to carefully assess who is harmed by the data breach before sending notification. Over 36% of respondents believe only victims who are at risk should be notified, and 14% feel notification should take place only when there is **absolute** confirmation of harm to the victim. Approximately 37% believe everyone should be notified regardless of the potential for harm (a.k.a. over-reporting).

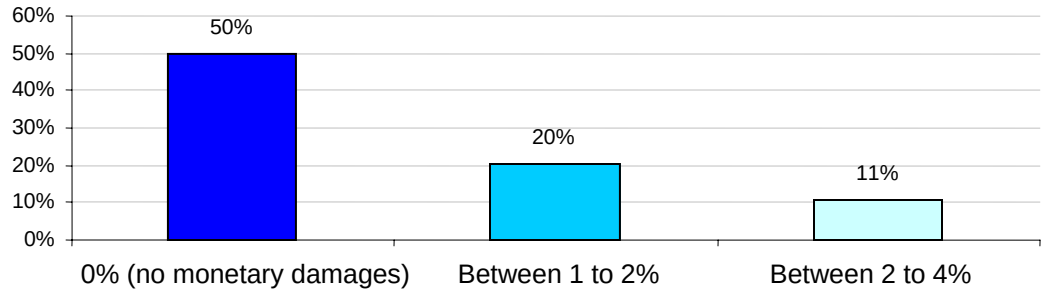
Bar Chart 7
Who needs to be notified?



Respondents believe that data breaches do not cause victims significant monetary losses. Fifty percent believe that victims did not experience any financial impact or monetary damages as a consequence of their organization's data breach. Another 20% believe that between 1% to 2% of data breach victims experienced some monetary affect. Of those respondents who believe data breach victims experienced a financial impact, 39% believe the amount, on average, was less than $10, 19% believe it was less than $50, and 24% believe it was less than $100. Bar Chart 8 summarizes these results.

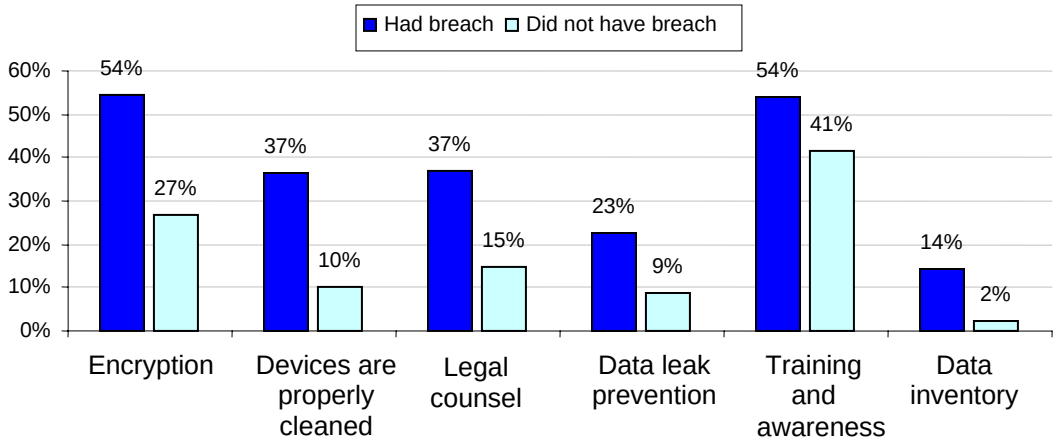
These results suggest a possible disconnect between the values held by businesses and consumers. That is, while data breach laws are costly to companies, respondents do not see how these requirements benefit consumers in terms of avoiding financial loss.

Bar Chart 8
What percentage of breach victims experienced monetary damages?



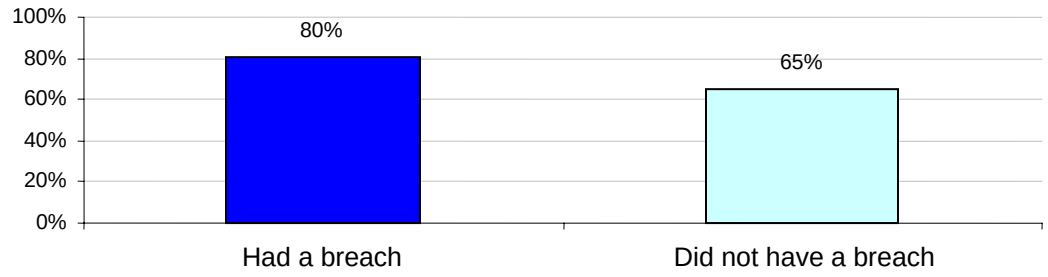
Organizations that did not experience a data breach have a different set of prevention priorities. As shown in Bar Chart 9, companies that had a breach appear to be **more** likely to deploy certain preventive or control procedures such as encryption solutions, secure disposal of IT equipment, engage legal counsel to assist on data breach incidents, and conduct post-mortem analyses.

Bar Chart 9
Percentage difference between companies that experienced a breach and companies that did not experience a breach



As shown in Bar Chart 10, organizations that have had a data breach appear to have greater support from their senior management than organizations that have not as yet experienced this negative event (80% vs. 65%).

Bar Chart 10
Is senior management supportive?



Caveats to this Survey

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from sample findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-Response Bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate have different beliefs than those who completed the instrument.
- Sampling-Frame Bias: Sampling-Frame Bias could impact the accuracy of contact information and the degree to which the list is representative of individuals who are informed about current events. We also acknowledge that the results may be biased by media coverage at the time of the study.

  Compensation was provided to ensure that respondents completed the survey task in a short holdout period. While compensation was held to a nominal amount, we acknowledge potential bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses (form survey or telephone) would result in a different pattern of findings.
- Self-Reported Results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Sample

A random sampling frame of 11,762 adult-aged individuals who reside within the United States was used to recruit participants to this Web survey. Our randomly selected sampling frame was selected from three national mailing lists of information security professionals. In total, 780 respondents completed their survey results during an eight day research period. Of returned instruments, 78 survey forms were rejected because of reliability checks. A total of 702 surveys were used as our final sample. This sample represents a 6.0% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is $\leq$ 3%.

Over 90% of respondents completed all survey items within 10 minutes. Respondents were given the following instruction before starting the survey.

Dear Participant,

Has your company provided notification of a data breach? If you sent notification about the loss or theft of personal information entrusted to you, were you satisfied with the steps your organization took to complete the incident response process?

We appreciate your frank responses to all survey questions. Please be assured that we will not collect any personally identifiable information. If you have any questions, contact Ponemon Institute at research@ponemon.org or call us at 1.800.887.3118.

Thank you in advance for your participation.

L.A. Ponemon

Dr. Larry Ponemon
Chairman

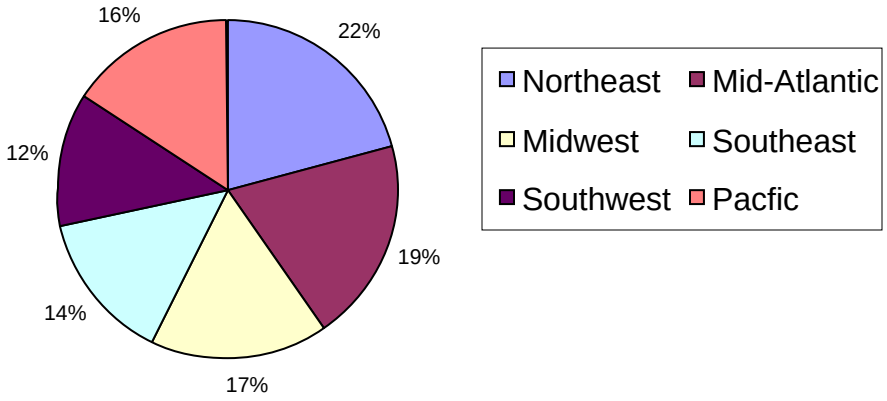
Following are demographics and organizational characteristics for 702 respondents. Table 1a reports the most frequently cited job titles of respondents (Top 5 list). Table 1b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (38%) or director (26%) levels, respectively.

Table 1a: Job Titles (Top 5 Titles)	Freq.	Pct%
IT security director	86	12%
IT security manager	63	9%
IT operations manager	57	8%
Chief information security officer	45	6%
Network security director	38	5%
All other titles	413	59%
Total	702	100%

Table 1b: Organizational levels	Freq.	Pct%
Senior Executive	16	2%
Vice President	24	3%
Director	185	26%
Manager	264	38%
Associate/Staff	213	30%
Total	702	100%

Pie chart 1 reports the geographic distribution across major regions of the United States. As shown, the Northeast region (22%) represents the largest geographic segment. The smallest sample segment is the Southwest region (12%). Please also note that respondents are located in 41 US states.

Distribution of respondents by U.S. geographic regions



On average, respondents have almost 15 years of experience in the information security field and nearly five years of experience in their current position. In total, 81% of respondents were males and 19% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the information security field in North America.

Over 68% of respondents state that their job function or position is located within the corporate CIO or CTO departments. About 7% state that they report to the organization's information security leader (CISO or CSO) and 8% state that they report to the company's chief risk officer.

Table 2a reports the respondent's corporate IT footprint by organizational size or headcount. Table 2b provides the approximate global headcount. As can be seen, 57% of respondents are employed by larger-sized organizations (with more than 25,000 employees).

Table 2a Corporate IT headcount	Freq.	Pct%
Less than 10 people	21	3%
10 to 50 people	40	6%
50 to 100 people	32	5%
100 to 500 people	99	14%
500 to 1,000 people	211	30%
1,000 to 2,000 people	149	21%
Over 2,000 people	150	21%
Total	702	100%

Table 2b Corporate headcount	Freq.	Pct%
Less than 500 people	18	3%
500 to 1,000 people	32	5%
1,001 to 5,000 people	40	6%
5,001 to 25,000 people	207	29%
25,001 to 75,000 people	235	33%
More than 75,000 people	170	24%
Total	702	100%

Detailed Results

The detailed findings are reported below. The survey question frequencies and percentage frequencies are reported in tabular format. The abbreviation "Pct%" denotes that the table percentages sum to the sample total. The column heading "Total%" means that the table percentages sum to the response sample total (which is greater than the sample total if a given question allows more than one response).

Part one of the survey is completed by 567 respondents in organizations that had a data breach requiring notification.

Table 3a Did your organization have an incident response plan in place before the breach incident?	Freq.	Pct%
Yes	246	43%
No	321	57%
Total	567	100%

Table 3b Did you use outside legal counsel to draft an incident response plan?	Freq.	Pct%
Yes	130	53%
No	116	47%
Total	246	100%

Table 4 What steps did you take to respond to the breach? (check all that apply)	Freq.	Total%
Careful assessment of the harm to victims	267	47%
Prompt notification by email	99	17%
Prompt notification by telephone	124	22%
Prompt notification by letter	353	62%
Prompt notification by placing an ad in a newspaper	89	16%
Offer to help victims with credit monitoring services	263	46%
Offer to compensate victims with coupons or free services	63	11%
Involved legal counsel to understand obligations	104	18%
Hired service providers to assist in dealing with the breach	102	18%
Hired forensic experts to investigate the cause of the breach	73	13%
Responded to all media inquiries	17	3%
Other	73	13%
None of the above	100	18%

Table 5 What steps do you believe were most helpful to reducing damage to your organization's reputation?	Freq.	Total%
Careful assessment of the types of harm victims experienced	246	43%
Prompt notification to victims by email	13	2%
Prompt notification to victims by telephone	123	22%
Prompt notification to victims by letter	309	54%
Prompt notification by placing an ad in a newspaper	10	2%
Prompt notification to regulators on voluntary basis	35	6%
Prompt notification to regulators as required by law	16	3%
Offer to help victims with credit monitoring services	250	44%
Offer to compensate victims with coupons or free services	50	9%
Understood legal rights and obligations	213	38%
Hired service providers to assist in dealing with the breach	98	17%
Hired forensic experts to investigate the cause of the breach	31	5%
Responded to all media inquiries	17	3%
Other	45	8%
None of the above	122	22%

Table 6a Did you attempt to measure the cost of the breach to your organization?	Freq.	Pct%
Yes	164	29%
No	403	71%
Total	567	100%

Table 6b If yes, please check the areas of cost included in your measurement.	Freq.	Total%
Loss of customers	121	74%
Decline in share value	53	32%
Potential fines	54	33%
Potential litigation	97	59%
Cost to notify victims	160	98%
Cost of assisting victims	125	76%
Cost to hire experts	59	36%
Other	6	4%

Table 6c If no, why not?	Freq.	Pct%
We don't have enough information to determine cost	136	34%
We don't think that cost analysis is applicable here	145	36%
We don't have any interest in knowing the cost	46	11%
None of the above	76	19%
Total	403	100%

Table 7 What was the most probable cause of the breach event?	Freq.	Pct%
Negligent employees, temporary employees or contractors	90	16%
Negligent third parties including, vendors and outsourcers	56	10%
Malicious employees, temporary employees or contractors	32	6%
Criminal activity including cyber crime and social engineering	33	6%
IT mishaps or glitches	39	7%
Web site mishaps or glitches	5	1%
Missing equipment including portable devices such as laptops, PDAs, and memory sticks	239	42%
Missing backup media	20	4%
Natural disasters such as hurricanes	2	0%
Other	6	1%
Cannot determine	45	8%
Total	567	100%

Table 8 How would you characterize your notification process to victims?	Freq.	Pct%
Our organization is careful in determining who is at risk. Only then, are victims notified.	206	36%
Our organization notifies everyone rather than to take a more focused or surgical approach.	211	37%
Our organization does not notify anyone until we have absolute confirmation of harm to the victim.	78	14%
None of the above.	72	13%
Total	567	100%

Table 9 Based on your experience, what are you doing today to prevent and detect a breach event?	Freq.	Total%
Nothing	76	13%
Investing in data leak detection and prevention technology	128	23%
Investing in encryption solutions	309	54%
Investing in perimeter controls	202	36%
Investing in security event management tools	155	27%
Investing in identity & access management solutions	200	35%
Conducting training and awareness	305	54%
Establishing incident response plan	245	43%
Hiring in-house personnel to lead data protection efforts	145	26%
Hiring outside counsel to provide legal advise	209	37%
Hiring consultants to help establish data protection efforts	85	15%
Conducting post mortem	119	21%
Taking a comprehensive inventory of all data at rest and in motion	82	14%
Ensuring that devices that are removed or recycled are properly cleaned	208	37%
Controlling endpoints to the organization's systems and networks	199	35%
Other	35	6%

Table 10a. Based on your organization's experience, what percentage of data breach victims suffered monetary damages such as identity theft or identity fraud as result of the incident?	Freq.	Pct%
0% (no one)	224	40%
Between 1 to 2%	105	19%
Between 2 to 4%	56	10%
Between 4 to 6%	32	6%
Between 6 to 8%	46	8%
Between 8 to 10%	28	5%
Cannot determine	76	13%
Total	567	100%

Table 10b If you stated **cannot determine**, what is your "gut feel" about the percentage of people who experienced some monetary damages?	Freq.	Pct%
0% (no one)	58	76%
Between 1 to 2%	11	14%
Between 2 to 4%	4	5%
Between 4 to 6%	1	1%
Between 6 to 8%	2	3%
Between 8 to 10%	0	0%
Total	76	100%

Table 10c If you selected a percentage greater than 0%, what is the approximate amount suffered by people who are victims of the breach?	Freq.	Pct%
Nothing	1	0%
Less than $1	51	18%
Between 1 to $10	60	21%
Between 10 to $20	34	12%
Between 20 to $50	20	7%
Between 50 to $100	67	24%
Between 100 to $300	34	12%
Between 300 to $500	4	1%
Between 500 to $1,000	0	0%
Between $1,000 to $2,000	0	0%
Between $2,000 to $5,000	1	0%
Over $5,000	13	5%
Total	285	100%

Table 11 Is your organization's senior management supportive of your practices to prevent and detect data breach incidents?	Freq.	Pct%
Yes	456	80%
No	44	8%
Unsure	67	12%
Total	567	100%

Part two of the survey is completed by 135 respondents in organization that did not (as yet) have a data breach requiring notification.

Table 12 Do you have an incident response plan in place?	Freq.	Pct%
Yes	60	44%
No	75	56%
Total	135	100%

Table 13 What steps have you taken to prevent and detect a breach?	Freq.	Total%
Nothing	45	33%
Investing in data leak detection and prevention technology	12	9%
Investing in encryption solutions	36	27%
Investing in perimeter controls	42	31%
Investing in security event management tools	31	23%
Investing in identity & access management solutions	45	33%
Conducting training and awareness	56	41%
Establishing incident response plan	98	73%
Hiring in-house personnel to lead data protection efforts	23	17%
Hiring outside counsel to provide legal advise	20	15%
Hiring consultants to help establish data protection efforts	14	10%
Conducting post mortem	0	0%
Taking a comprehensive inventory of all data at rest and in motion	3	2%
Ensuring that devices that are removed or recycled are properly cleaned	14	10%
Controlling endpoints to the organization's systems and networks	45	33%
Other	7	5%

Table 14 Is your organization's senior management supportive of your practices to prevent and detect data breach incidents?	Freq.	Pct%
Yes	88	65%
No	10	7%
Unsure	37	27%
Total	135	100%

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686
1.800.887.3118
research@ponemon.org

Scott & Scott, LLP
2200 Ross Avenue
Suite 5350E
Dallas, Texas 75201
1.800.596.6176
rjscott@scottandscottllp.com

About Scott & Scott LLP

Scott & Scott is an international law and technology services firm dedicated to helping senior executives assess and reduce the legal, financial, and regulatory risks associated with information technology issues. An innovative approach to legal services, Scott & Scott believes that collaboration between legal and technology professionals is necessary to solve and defend against the complex problems our clients face, including privacy and network security, IT asset management, software license compliance, and IT transactions. Legal and technology professionals work in tandem to provide full-service representation. By combining these resources, Scott & Scott is better able to serve clients' needs than law firms and technology services firms working independently of one another. Visit Scott & Scott online at www.scottandscottllp.com.

About the Ponemon Institute LLC

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions. For more information, please visit http://www.ponemon.org.