Ponemon INSTITUTE

Aftermath of a Data Breach Study

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: January 2012

Aftermath of a Data Breach Study

January 2012

Part 1: Introduction

We are pleased to present the findings of the *Aftermath of a Data Breach* conducted by Ponemon Institute and sponsored by Experian® Data Breach Resolution. The study was conducted to learn what organizations did to recover from the financial and reputational damage of a data breach involving customer and consumer records. We also asked questions from a similar study conducted in 2007[1] to determine if organizations are changing their approach to managing the aftermath of a data breach and addressing their vulnerabilities to future breaches.

Consumer and customer information collected by organizations is at great risk due to employee negligence, insider maliciousness, system glitches or attacks by cyber criminals. Since 2005, according to the Privacy Rights Clearinghouse (PRC), 543 million records containing sensitive information have been breached. PRC says this number is conservative because they track only those breaches that are reported in the media and many states do not require companies to report data breaches to a central clearinghouse.

In 2011, what is considered the biggest consumer data breach ever occurred. As reported by PRC, as many as 250 million consumers received notices telling them that their email addresses and names were exposed. Another significant data breach took place at the end of the year and involved the theft of credit card information.

The organizations represented in this study have had at least one data breach involving customer and consumer records in the past 24 months. The final sample of respondents was 725 IT professionals. We asked only those individuals (584) who self-reported that they work in organizations that had a data breach to complete the survey.

On average, respondents have 10.5 years of IT or IT experience. Seventy-three percent report either directly or indirectly to the chief information officer (CIO) or the chief information security officer (CISO). When responding to the survey questions, we asked respondents to focus on the one data breach they believe had the greatest financial and reputational impact to their organizations.

In the aftermath of a data breach, IT respondents believe the following:

- They are more confident than senior leadership about the ability to keep customer data secure from future breaches.
- By far, negligent employees, temporary employees or contractors make organizations vulnerable to future breaches. Accordingly, conducting training and awareness programs and enforcing security policies should be a priority for organizations.
- Privacy and data protection became a greater priority for senior leadership following the breach. As a result, IT security budgets for most organizations in this study increased.
- They are concerned that customer data stolen from their organizations will be used to commit identity fraud.

[1] The Business Impact of a Data Breach, conducted by Ponemon Institute and sponsored by Scott & Scott, 2007

- The top three actions believed to reduce the negative consequences of the data breach are hiring legal counsel, assessing the harm to victims and employing forensic experts.

- Lessons learned from the data breach are to limit the amount of personal data collected, limit sharing with third parties and limit the amount of personal data stored.

Part 2: Key Findings

All of the organizations in this study had at least one data breach involving consumer information and 85 percent of the IT practitioners in this study report that more than one breach involving customer/consumer data occurred in the past 24 months. In our previous study, *Reputation Impact of a Data Breach,* we learned that data breaches involving customer and consumer data are more damaging to an organization's reputation and brand than data breaches involving employee or business confidential data. In fact, the findings reveal that it can take a year to restore an organization's reputation with an average loss of $332 million in the value of its brand.[2]

For purposes of this study, we asked respondents to focus on the one data breach they believe had the most significant financial and reputational impact on their organizations.

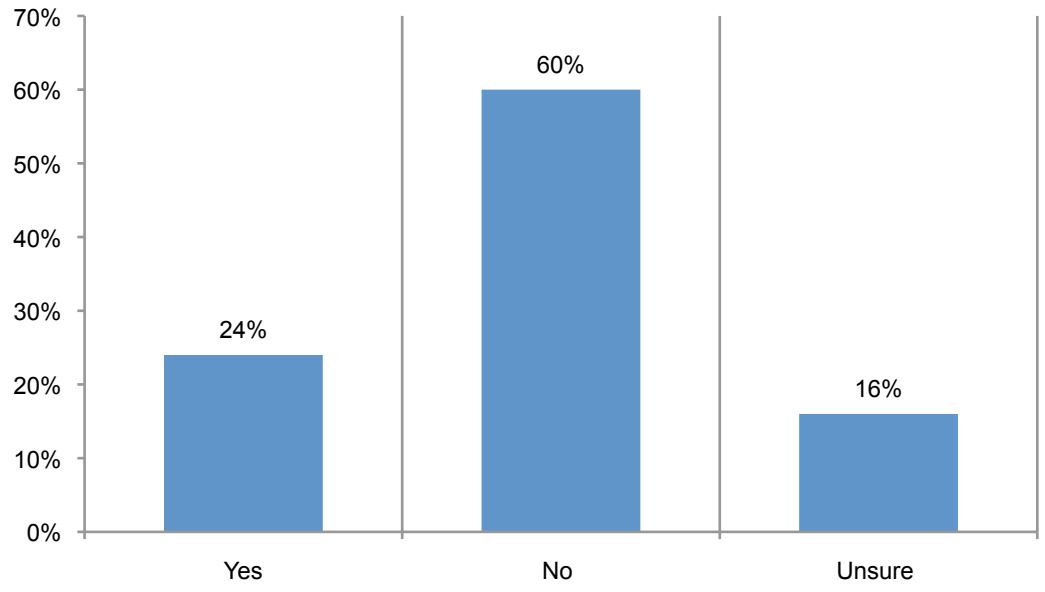
The study is organized according to the following three topics:

- Circumstances of the data breach
- Response to the data breach
- Impact of the breach on privacy and data protection practices

1. Circumstances of the data breaches

In most cases, sensitive data lost or stolen was not encrypted. As shown in Bar Chart 1, 60 percent of respondents say the customer data that was lost or stolen was not encrypted and 16 percent are unsure.

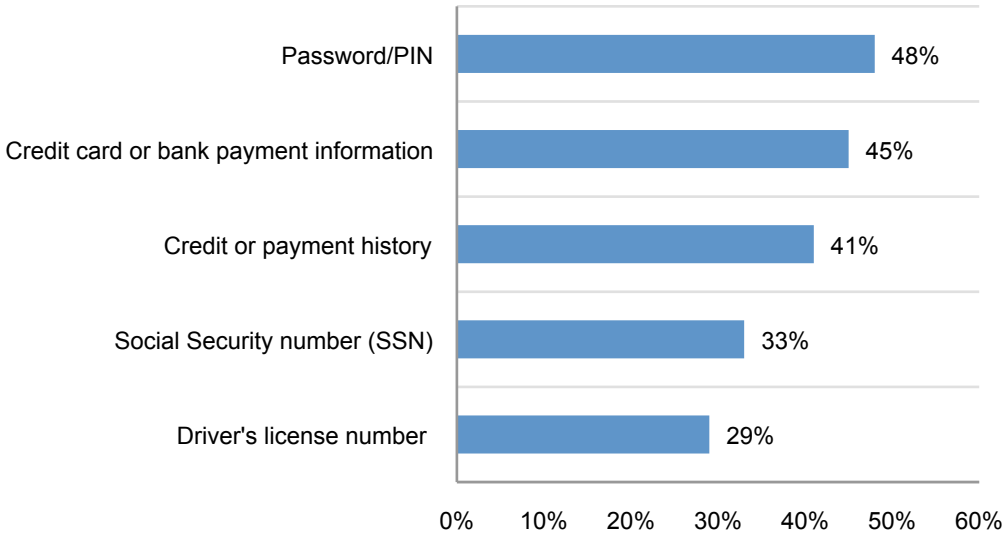
Bar Chart 1: Was the customer data that was lost or stolen encrypted?



[2] Reputation Impact of a Data Breach: U.S. Study of Executives & Managers, Ponemon Institute, sponsored by Experian®Data Breach Resolution, November 2011

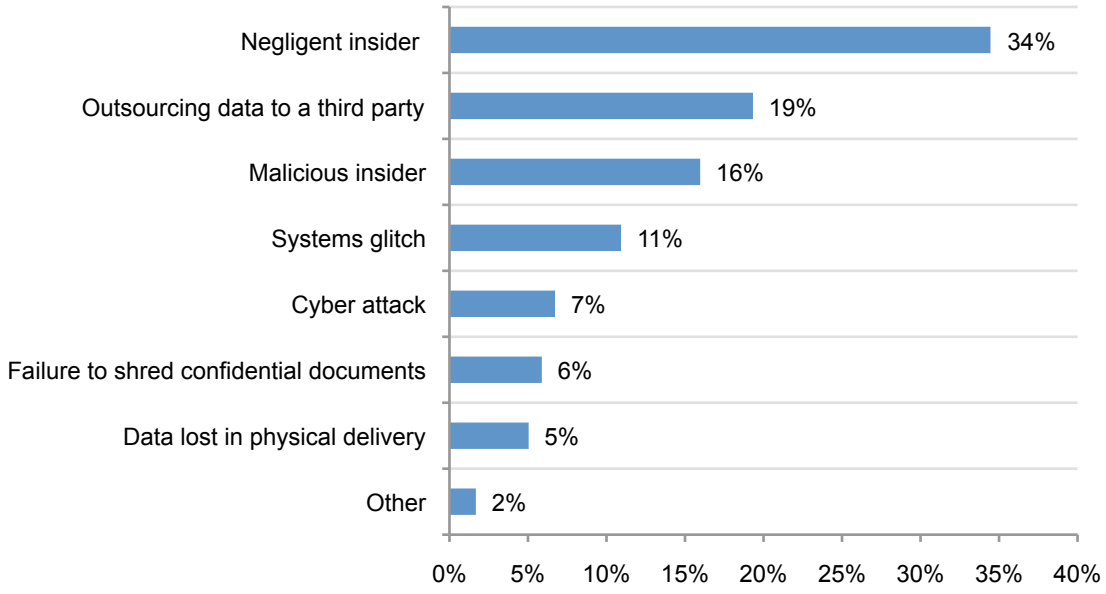
Organizations report that their most sensitive data was lost or stolen. We asked the IT practitioners participating in this study to focus on the one data breach that had the most severe consequences for their organizations. Bar Chart 2 reveals that similar to the mega breaches of 2011, respondents report the loss of email addresses and credit card or payment information. According to the Privacy Rights Clearinghouse, there were 121 incidents in 2011 targeting credit card data. Respondents also report the loss of Social Security numbers and credit or payment history. A complete list of the types of data lost by organizations in this study is presented in the Appendix of this paper. (Please add Email data 70 percent)

Bar Chart 2: What type of data did your organization lose?



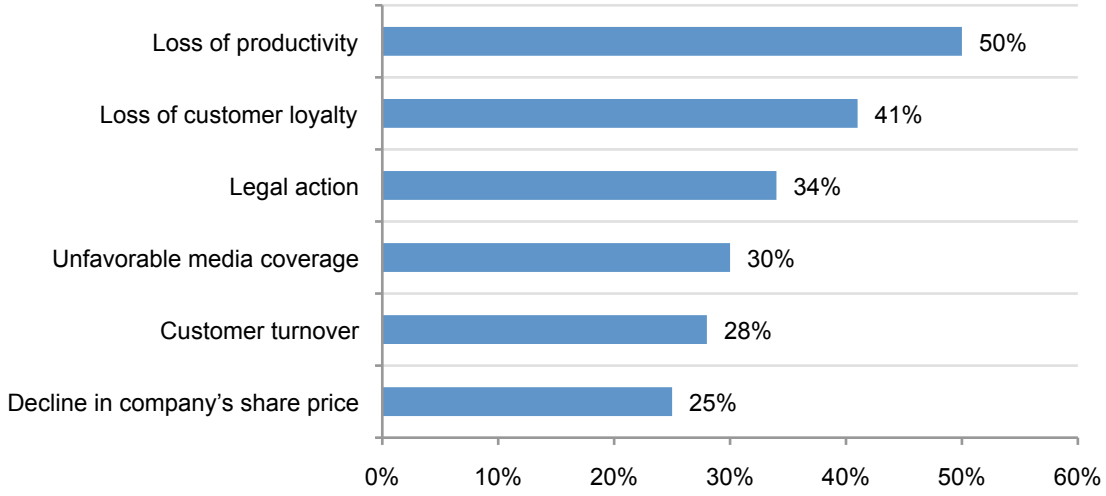
Insiders and third parties are most often the cause of the data breach. Forty-four percent of respondents say they were not able to determine the root causes of the breach or are unsure. As shown in Bar Chart 3, if the organization was able to determine the cause of the breach, most often it was the negligent insider (34 percent). Nineteen percent say it was the outsourcing of data to a third party and 16 percent say a malicious insider was the main cause. On a positive note, the human factor risks are easier to mitigate through policies, procedures and technologies than the cyber attacks reported by 7 percent of the respondents.

Bar Chart 3: What was the main cause of the data breach?



Data breaches reduce an organization's productivity. Fifty percent of respondents say the most negative consequence of the breach was the loss of productivity (Bar Chart 4). In the aftermath of a data breach, key employees may be diverted from their usual responsibilities to help the organization respond to and resolve the data breach. This is followed by a loss of customer loyalty (41 percent) and legal action (34 percent) as the most negative consequences.

Bar Chart 4: What were the most negative consequences of the data breach?
More than one choice permitted.

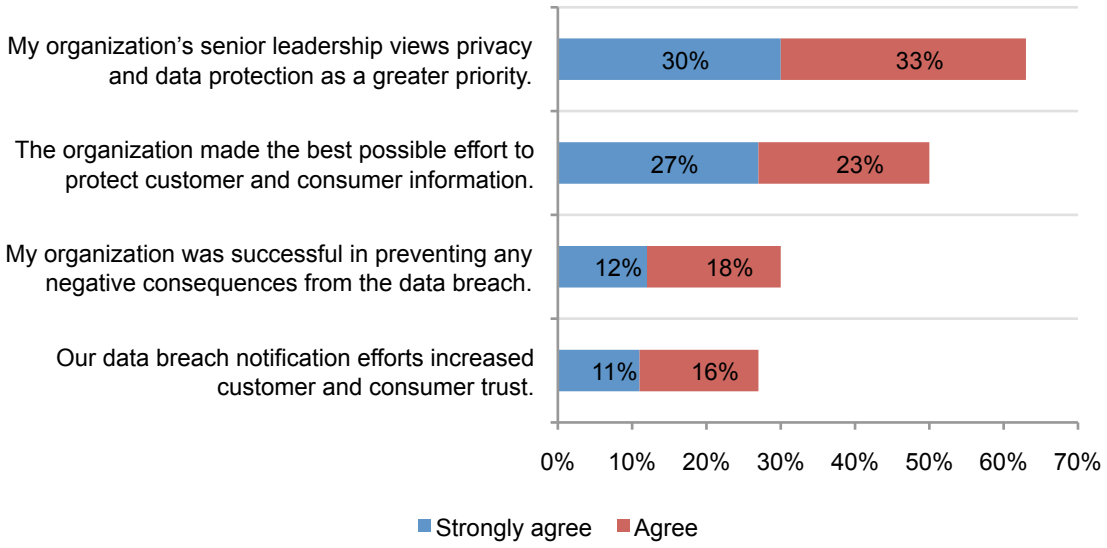


2. Response to the data breach

Data breach response strategies need improvement. As shown in Bar Chart 5, 50 percent (27 percent + 23 percent) believe the organization made the best possible effort following the data breach. However, only 30 percent say that it was successful in preventing any negative consequences from the data breach (12 percent + 18 percent). In addition, only 27 percent (11 percent + 16 percent) believe their data breach notification efforts increased customer and consumer trust in their organization.

There is good news. Sixty-three percent believe their senior leadership views privacy and data protection as a greater priority than before the breach. This change in thinking may result in the allocation of more resources to prevent and detect future breaches as well as in programs to protect victims from future harms.

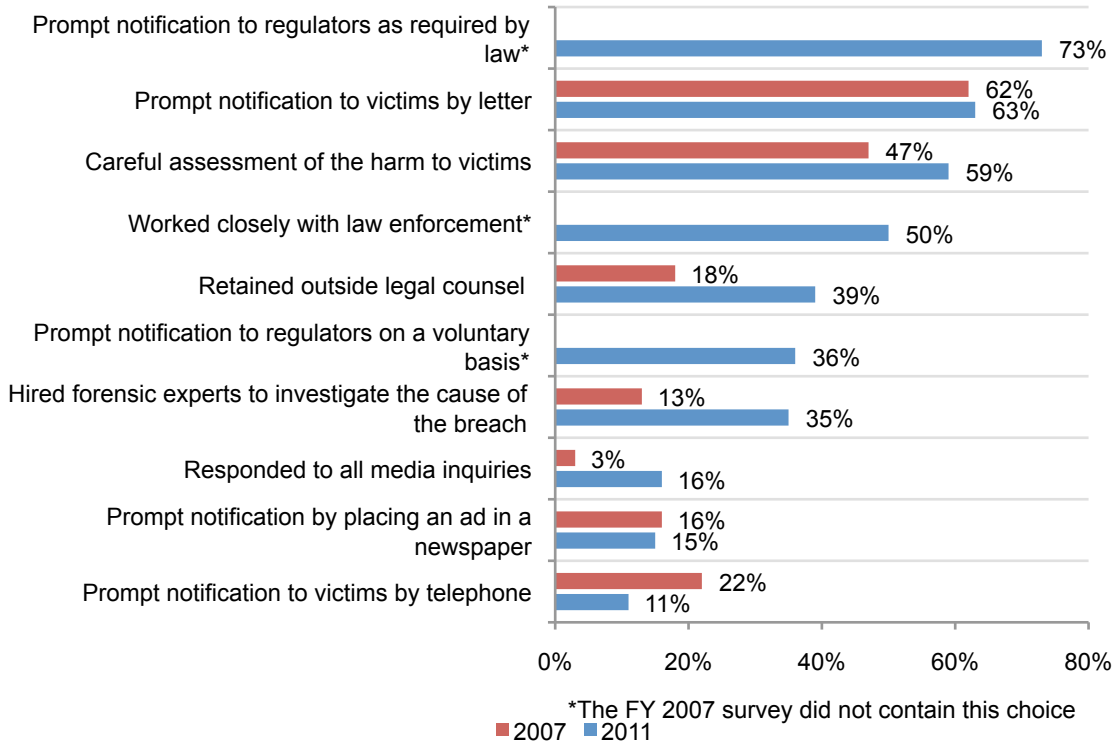
Bar Chart 5: Perceptions about organizations' response to a data breach
Strongly agree and agree response.



Prompt notification and assessment of harm to victims are the steps most often taken in response to a data breach. Bar Chart 6 reveals that the top three data breach response activities are: prompt notification to regulators as required by law, prompt notification to victims by letter and careful assessment of the harm to victims. When we asked the question in 2007, the steps taken were somewhat similar: prompt notification to victims by letter, careful assessment of the harm to victims and prompt notification to victims by telephone. The prompt notification to regulators on a voluntary basis was not included in the 2007 study.

The hiring of forensic experts to investigate the cause of the breach and retaining legal counsel had the greatest increase since the 2007 study. The biggest decrease was prompt notification to victims by telephone.

Bar Chart 6: What steps did you take to respond to the data breach?
More than one choice permitted.

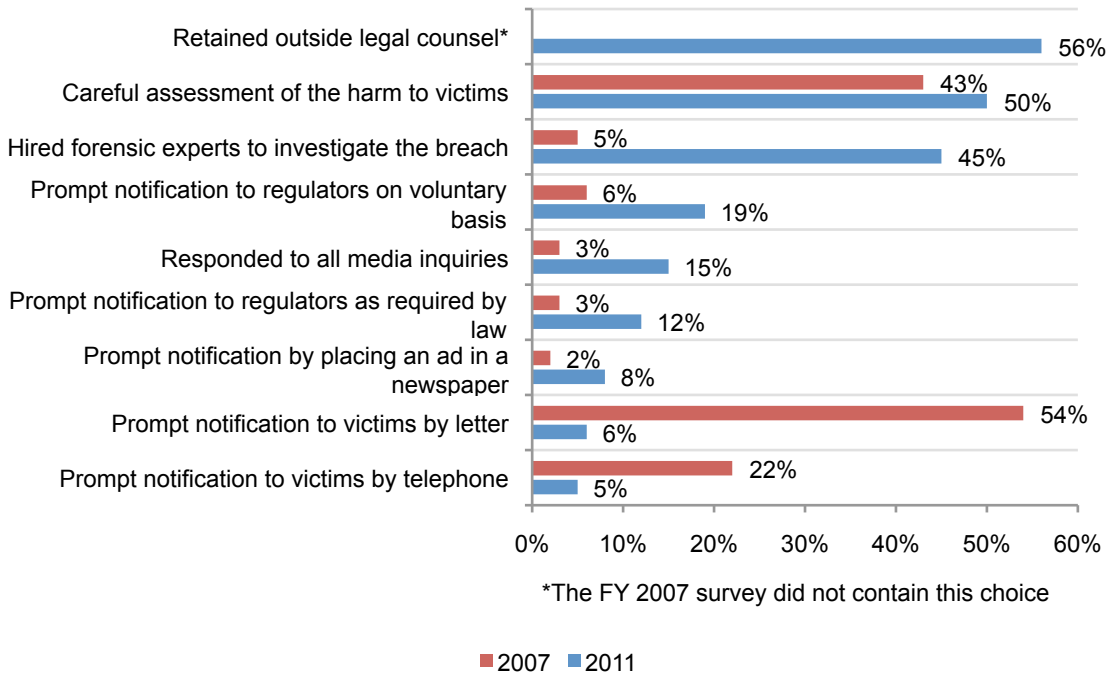


New steps are taken to reduce negative consequences. As shown in Bar Chart 7**,** prompt notification to victims is no longer considered most helpful in reducing the negative consequences of the data breach. While required by law, data breach notification does not prevent the loss of customer loyalty or reputation.

The most helpful steps are: retaining outside legal counsel, carefully assessing the harm to victims and hiring forensic experts. We believe organizations recognize the importance of knowing as much as possible about the breach to improve their communications about the incident and to make the right decisions about how to prevent future breaches. In 2007, what was considered most helpful were: notifying victims promptly by letter, carefully assessing the harm to victims and understanding legal rights and obligations.

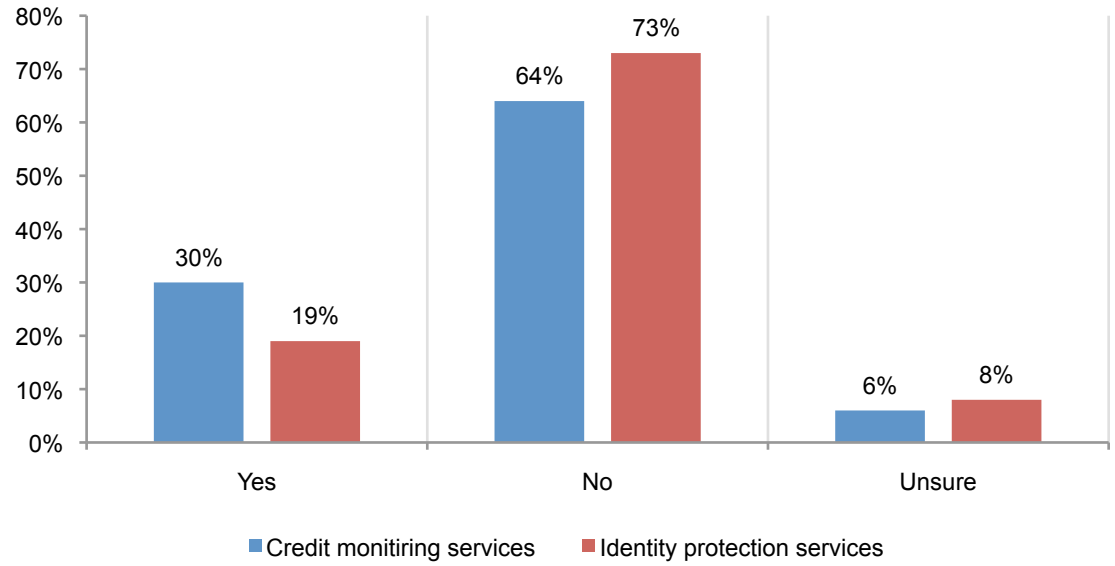
Major changes in what organizations believe to be the best strategies in reducing the negative consequences are an increased use of forensic experts, prompt notification to regulators on a voluntary basis and response to all media inquiries. Actions that declined in value are the prompt notification of victims by letter and telephone.

Bar Chart 7: What steps do you believe were most helpful to reducing the negative consequences of the data breach?
More than one choice permitted.



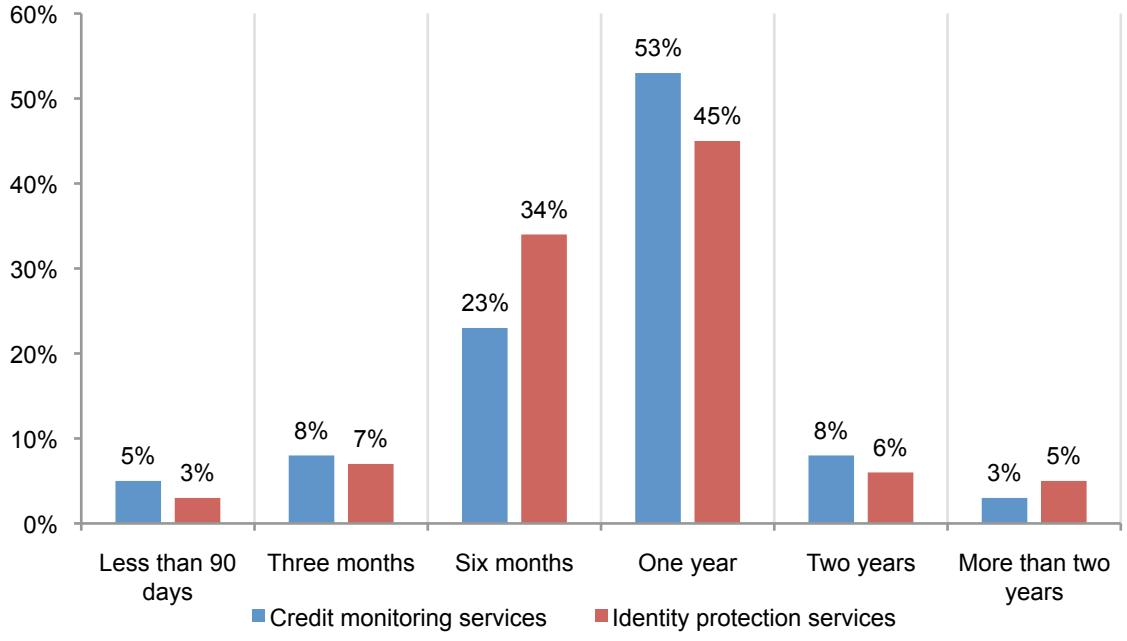
Credit monitoring and identity protection services are not often offered to victims. Despite the fact that many organizations lose the loyalty of their customers following a data breach services that might maintain or even strengthen the customer's relationship with organization are not offered as frequently on a voluntary basis. Bar Chart 8 reveals that only 30 percent say they offer credit monitoring services and only 19 percent say they offer identity protection services such as credit monitoring and other identity theft protection measures, including fraud resolution, scans and alerts.

Bar Chart 8: Did you offer victims credit monitoring and identity protection services?



If services are offered, they are provided for one year or less. As shown in Bar Chart9, only 11 percent offer credit monitoring or identity protection services for two or more years.

Bar Chart 9: If yes, for what length of time were these services provided?



Company's data will be used to commit other types of identity fraud. While many of the respondents are confident about protecting their customers' personal information, 64 percent say they are concerned that now that the data may be in the hands of criminals it will be used to commit other types of identity fraud. This perception should encourage organizations to consider programs that protect victims from future harms.

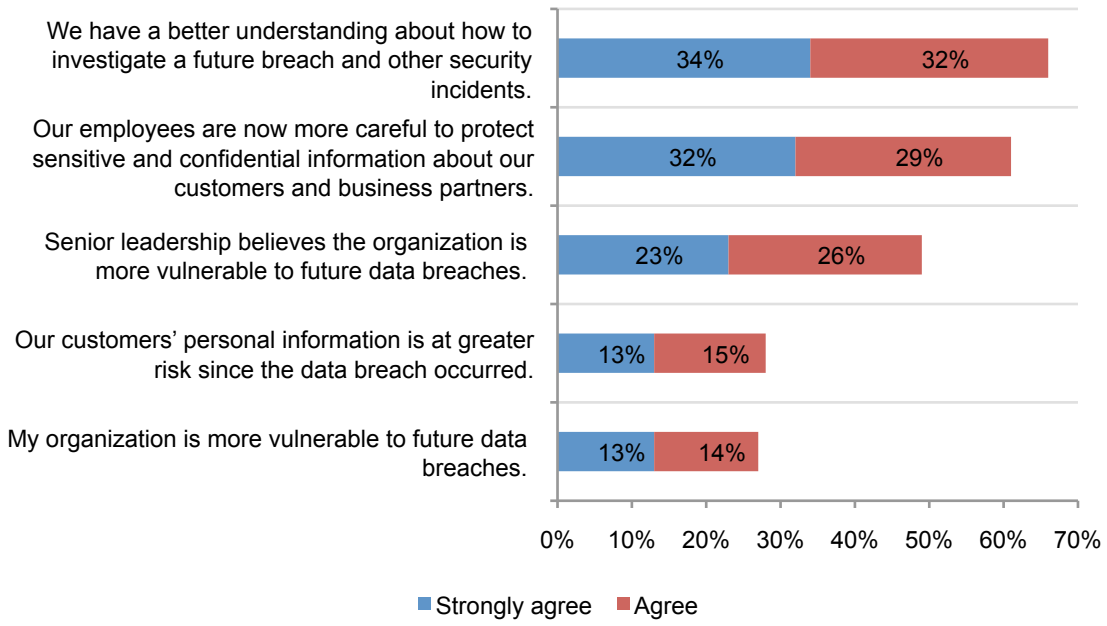
3. Impact of a breach on privacy & data protection practices

In the aftermath of a breach, senior leadership believes the organization is more vulnerable to a breach. According to the findings in Bar Chart 10, just about half (49 percent) of respondents say senior leadership believes the organization is more vulnerable to future data breaches (23 percent + 26 percent). In contrast, only 27 percent of the IT respondents say the organization is more vulnerable (13 percent + 14 percent), indicating their confidence in preventing future breaches and only 28 percent believe their customers' personal information is at greater risk since the data breach occurred (13 percent + 15 percent).

Lessons learned may improve privacy and data protection practices. Responding to the breach improved organizations' understanding about how to investigate a future breach (Bar Chart 10). The majority of respondents (66 percent) say that the experience of investigating the causes of the breach will help them in determining the root causes of future breaches (34 percent + 32 percent).

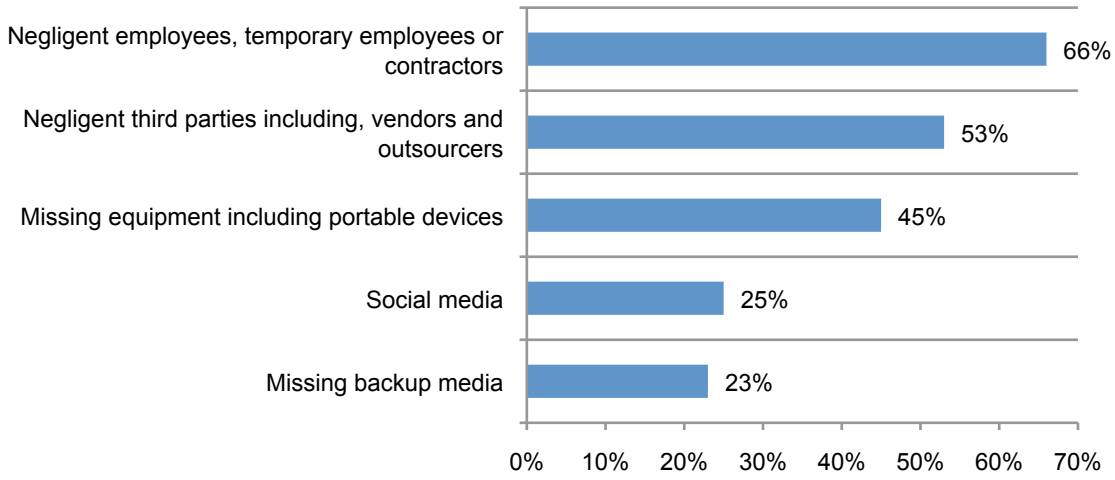
Employees are more careful to protect data**.** Sixty-one percent believe employees are more aware of the need to protect sensitive and confidential information. Training and awareness is the most often cited activity put in place to prevent future data breaches

Bar Chart 10: Lessons learned in the aftermath
Strongly agree and agree response.



Employees and other insiders pose the greatest threat to an organization's sensitive data. As shown in Bar Chart 11, making employees more aware of the need to be careful when handling sensitive and confidential information can help avoid future breaches. Negligent insiders and third parties are the main reasons organizations are vulnerable to future breaches. Negligence also includes losing laptops, mobile phones, PDAs and USB drives. Twenty-five percent say social media is posing a threat. IT mishaps or glitches, website mishaps or glitches, malicious insiders and criminal activity are not considered as much a threat. Q 24

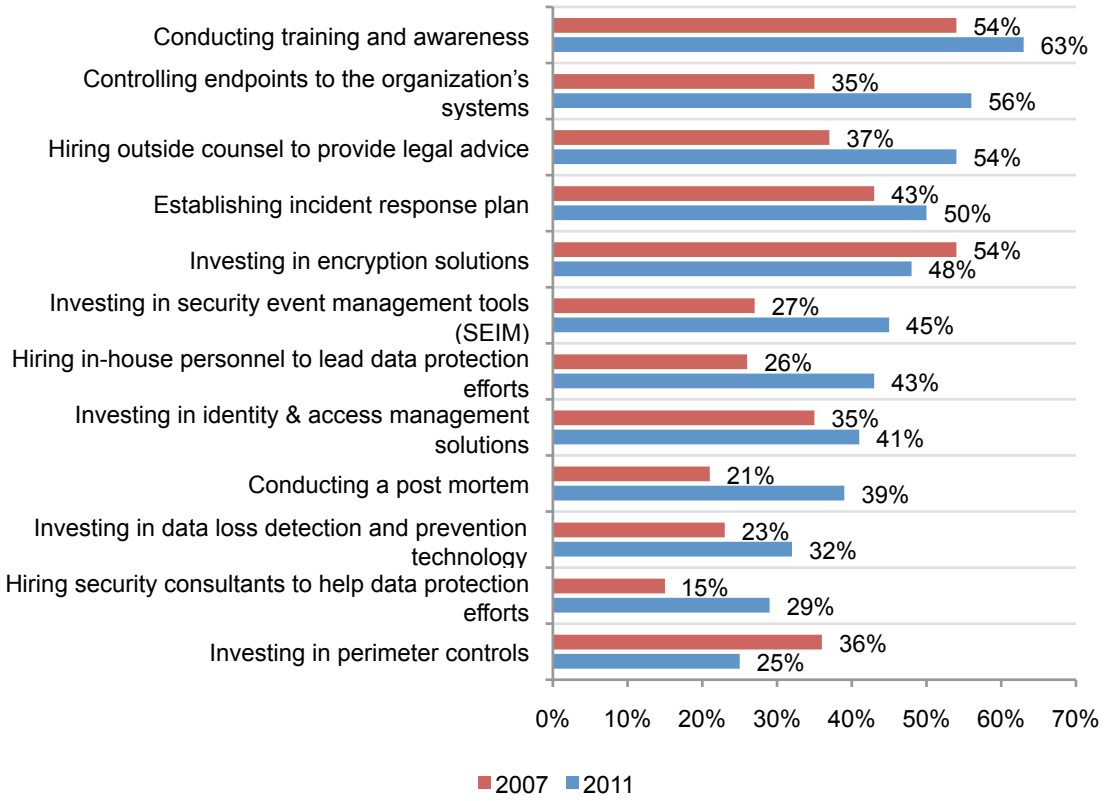
Bar Chart 11: Based on your data breach experience, please select the top three reasons your organization is vulnerable for another breach.



To reduce the risk of these vulnerabilities, organizations are conducting training and awareness programs, hiring outside counsel to provide legal advice and establishing an incident response plan. In 2007 when we asked this question, respondents cited investing in encryption solutions, conducting training and awareness, establishing incident response plans, hiring outside counsel and ensuring the removal of all sensitive and confidential data on devices that are removed or recycled.

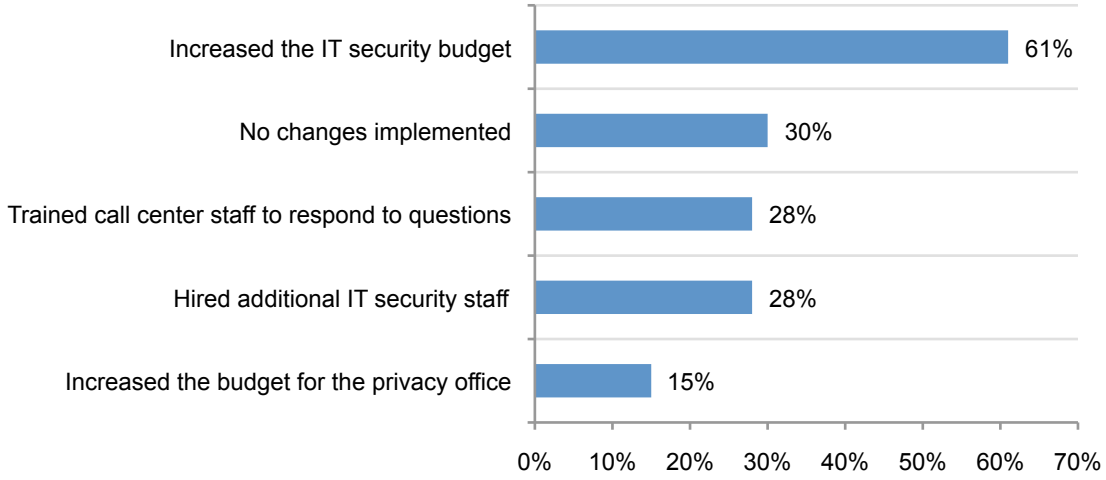
Practices that increased the most since 2007 and shown in Bar Chart 12 are: controlling endpoints to the organization's systems and networks, conducting a post mortem, investing in security event management tools (SEIM), hiring in-house personnel to lead data protection efforts and hiring outside counsel to provide legal advice. The practice that declined the most is investing in perimeter controls. Q 25

Bar Chart 12: What is your organization doing to address these vulnerabilities?
More than one choice permitted.



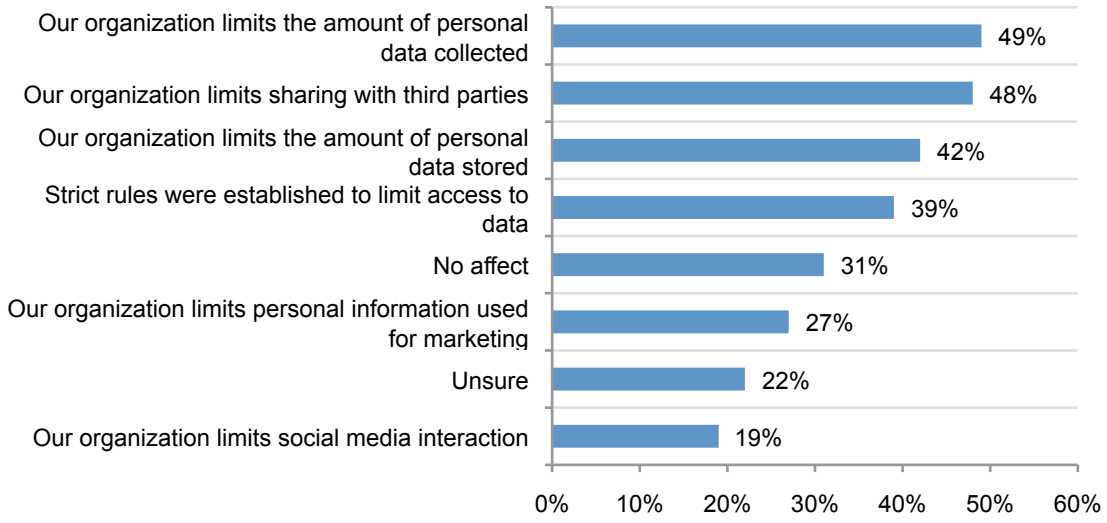
Privacy and data protection became more of a priority and IT security resources increased. Following the data breach, 61 percent of respondents say their organizations increased the security budget and 28 percent hired additional IT security staff (Bar Chart 13). Only nine percent say they increased the budget for the compliance staff and four percent say they hired additional privacy office staff. Q 27

Bar Chart 13: Following the data breach were any of the following actions taken?
More than one choice permitted.



Organizations are now minimizing the amount of personal data collected, shared and stored. Bar Chart 14 reports **that** while 31 percent say the data breach had no affect on how the organization uses personal data, almost half (49 percent) now say they limit the amount of personal data collected and 48 percent now limit the sharing of this data with third parties. Forty-two percent say the organization limits the amount of personal data stored. However, only 27 percent say the organization now limits the amount of personal information used for marketing purposes. Q 28

Bar Chart 14: How did the data breach affect the organization's use of personal and confidential information?
More than one choice permitted.



Conclusion

We conducted this study to better understand how a data breach affects organizations over the long term. It is interesting to note that it took a serious data breach that had both financial and reputational consequences to make privacy and data protection a greater priority and allocate additional resources to the IT security function.

While many respondents were unable to determine the root cause of the data breach, there is a consensus among respondents that insider negligence is making their organizations vulnerable to a data breach. As a result, organizations are investing in training and awareness and technologies that minimize the human factor risk.

The findings also show the concern organizations have about losing the loyalty of their customers. Of the IT practitioners surveyed, few felt that prompt notification to victims is helpful in reducing the negative consequences of the data breach. This suggests that compliance with data breach notifications laws is not sufficient if an organization is concerned about customer loyalty and reputation.

Part 3. Methods

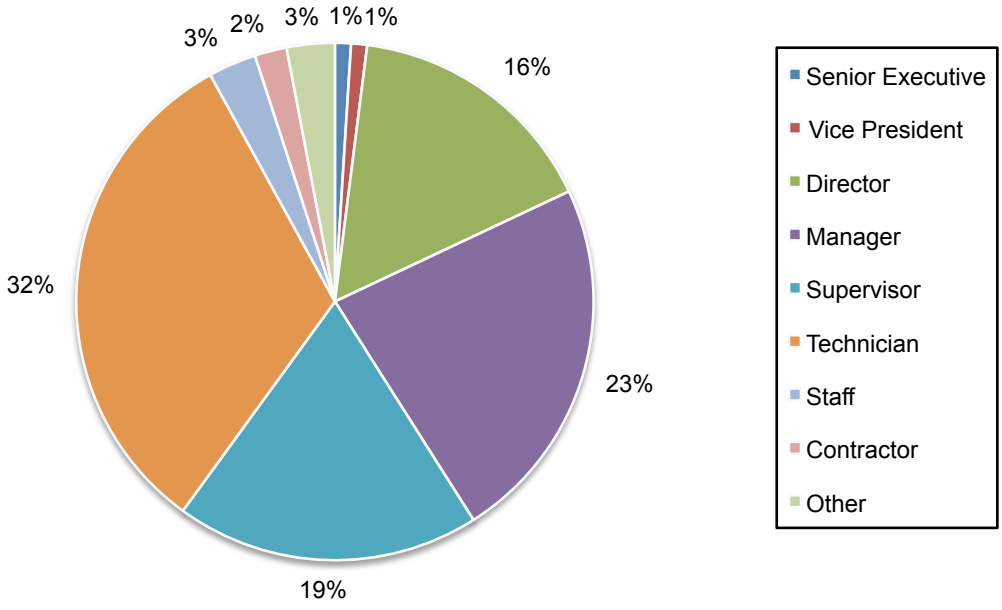
A random sampling frame of 16,209 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of highly experienced IT operations and IT security professionals with bona fide credentials. As shown in Table 1, 15,447 respondents completed the survey. Of the returned instruments, 789 surveys were screened to identify those respondents that have experienced a data breach. After removing 64 surveys that failed reliability checks the final sample was 725 individuals (or a 4.5 percent response rate).

Table 1. Survey response	Freq
Sample frame	16,209
Total returns	15,447
Screened responses	789
Rejected surveys	64
Final sample	725
Response rate	4.5%

Table 2. Experience	**Average**
Total years of IT or IT security experience	10.50
Total years in current position	5.00

Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 60 percent of respondents are at or above the supervisory levels. On average, respondents had more than 10 years of IT or IT security experience.

Pie Chart 1: What organizational level best describes your current position?



Pie Chart 2 reports the industry distribution of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (15 percent) and health and pharmaceutical (11 percent).

Pie Chart 2. Industry distribution of respondents' organizations

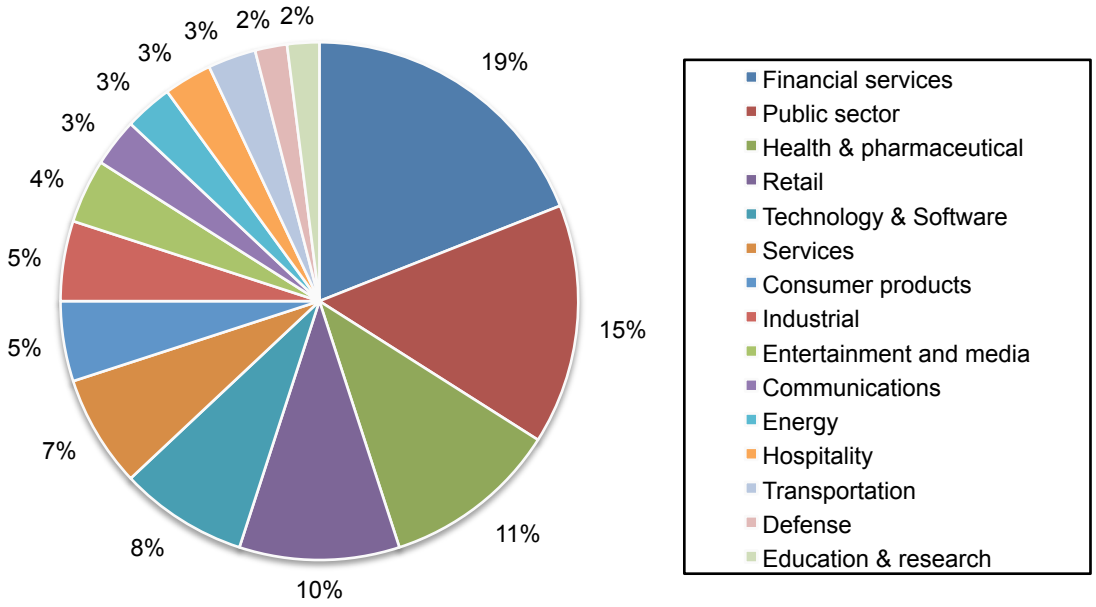


Table 3 reports the respondent organization's global footprint. The survey results indicate that a large number of participating organizations are multinational companies that operate outside the United States.

Table 3. Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	75%
Europe	67%
Middle East & Africa	38%
Asia-Pacific	58%
Latin America (including Mexico)	41%

Table 4 reports the worldwide headcount of participating organizations. Thirty-five percent of respondents are in organizations with more than 5,000 employees.

Table 4. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	19%
500 to 1,000 people	22%
1,001 to 5,000 people	24%
5,001 to 25,000 people	16%
25,001 to 75,000 people	12%
More than 75,000 people	7%
Total	100%

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured over a x-week period ending in x 2011.

Sample response	Freq	Pct%
Total sampling frame	16209	100.0%
Total invitations	15447	95.3%
Total returns	789	4.9%
Rejected surveys	64	0.4%
Final sample	725	4.5%

Part 1. Background

Q1. In the past 24 months, how many data breaches did your organization have involving consumer or customer data?	Freq	Pct%
None (stop)	86	12%
Unsure (stop)	55	8%
One	94	13%
Two	157	22%
Three	126	17%
Four	92	13%
Five	51	7%
More than five	64	9%
Total	725	100%

Revised sample	**584**

When responding to the following survey questions, please refer to the one data breach that occurred in the past 24 months that you believe had the most significant financial and reputational impact on your organization.

Q2. What type of data did your organization lose?	Pct%
Name	85%
Address	69%
Email address	70%
Telephone number	58%
Age	43%
Gender	35%
Employer	20%
Educational background	18%
Credit card or bank payment information	45%
Credit or payment history	41%
Password/PIN	48%
Social Security number (SSN)	33%
Driver's license number	29%
Other (please specify)	9%
Don't know	11%
Total	614%

Q3. Was the customer data that was lost or stolen encrypted?	Pct%
Yes	24%
No	60%
Unsure	16%
Total	100%

Q4. Were you able to determine the root causes of the breach?	Pct%
Yes	56%
No	25%
Unsure	19%
Total	100%

Q5. If yes, what was the main cause of the data breach? Please select only one choice.	Pct%
Negligent insider	34%
Malicious insider	16%
Systems glitch	11%
Cyber attack	7%
Outsourcing data to a third party	19%
Data lost in physical delivery	5%
Failure to shred confidential documents	6%
Other	2%
Total	100%

Part 2. Attributions: Please rate each one of the following statements using the five-point scale provided below each item. Strongly agree and agree response.	Strongly agree	Agree
Q6. Since the data breach, I believe my organization is more vulnerable to future data breaches.	13%	14%
Q7. Since the data breach, senior leadership believes the organization is more vulnerable to future data breaches.	23%	26%
Q8. I believe the data breach we experienced caused significant financial harm to my organization.	22%	38%
Q.9 I believe the data breach caused significant reputation and brand damage to my organization.	21%	36%
Q10. Since the data breach, I believe my organization's senior leadership views privacy and data protection as a greater priority than before the data breach.	30%	33%
Q11. Since the data breach, we have a better understanding about how to investigate a future breach and other security incidents.	34%	32%
Q12. I believe our customers' personal information is at greater risk since the data breach occurred.	13%	15%
Q13. I believe our employees are now more careful to protect sensitive and confidential information about our customers and business partners.	32%	29%
Q14 I believe our data breach notification efforts increased customer and consumer trust in our organization.	11%	16%
Q15. I believe the organization made the best possible effort following the data breach to protect customer and consumer information.	27%	23%
Q16. I believe the individuals who stole our company's data will use it to commit other types of fraud.	33%	31%
Q17. I believe my organization was successful in preventing any negative consequences from the data breach.	12%	18%
Q.18 I believe data breach notification provides a benefit to consumers who have had their personal information lost or stolen.	9%	11%

Q19. What were the most negative consequences of the data breach? Please check all that apply.	Pct%
Unfavorable media coverage	30%
Decline in company's share price	25%
Loss of customer loyalty	41%
Customer turnover	28%
Loss of revenue	15%
Loss of productivity	50%
Legal action	34%
Regulatory fines	9%
Other	2%
None of the above	25%
Total	259%

Q20. What steps did you take to respond to the data breach? Please check all that apply.	Pct%	FY 2007*
Careful assessment of the harm to victims	59%	47%
Prompt notification to victims by email	20%	17%
Prompt notification to victims by telephone	11%	22%
Prompt notification to victims by letter	63%	62%
Prompt notification by placing an ad in a newspaper	15%	16%
Prompt notification to regulators on a voluntary basis	36%	
Prompt notification to regulators as required by law	73%	
Offer to compensate victims with coupons or free services from our organization	8%	11%
Understood legal rights and obligations	47%	
Retained outside legal counsel	39%	18%
Hired crisis management or PR firm	13%	
Hired forensic experts to investigate the cause of the breach	35%	13%
Worked closely with law enforcement	50%	
Responded to all media inquiries	16%	3%
Other	4%	13%
None of the above	15%	18%
Total	504%	240%
*The Business Impact of a Data Breach. Ponemon Institute, May 2007		

Q21. What steps do you believe were most helpful to reducing the negative consequences of the data breach? Please check the top three steps.	Pct%	FY 2007*
Careful assessment of the harm to victims	50%	43%
Prompt notification to victims by email	6%	2%
Prompt notification to victims by telephone	5%	22%
Prompt notification to victims by letter	6%	54%
Prompt notification by placing an ad in a newspaper	8%	2%
Prompt notification to regulators on voluntary basis	19%	6%
Prompt notification to regulators as required by law	12%	3%
Offer to compensate victims with coupons or free services from our organization	5%	9%
Understood legal rights and obligations	35%	38%
Retained outside legal counsel	56%	
Hired crisis management or PR firm	12%	
Hired forensic experts to investigate the cause of the breach	45%	5%
Worked closely with law enforcement	12%	
Responded to all media inquiries	15%	3%
Other	2%	6%
None of the above	10%	22%
Total	298%	215%
*The Business Impact of a Data Breach. Ponemon Institute, May 2007		

Q22a. Did you offer victims credit-monitoring services?	Pct%
Yes	30%
No	64%
Unsure	6%
Total	100%

Q22b. If yes, for what length of time were these services provided?	Pct%
Less than 90 days	5%
Three months	8%
Six months	23%
One year	53%
Two years	8%
More than two years	3%
Total	100%

Q23a. Did you offer victims identity protection services such as credit monitoring and other identity theft protection measures, including fraud resolution, scans and alerts?	Pct%
Yes	19%
No	73%
Unsure	8%
Total	100%

Q23b. If yes, for what length of time were these services provided?	Pct%
Less than 90 days	3%
Three months	7%
Six months	34%
One year	45%
Two years	6%
More than two years	5%
Total	100%

Q24. Based on your data breach experience, please select the top three reasons your organization is vulnerable for another breach.	Pct%
Negligent employees, temporary employees or contractors	66%
Negligent third parties including, vendors and outsourcers	53%
Malicious employees, temporary employees or contractors	15%
Criminal activity including cyber crime and social engineering	9%
IT mishaps or glitches	18%
Web site mishaps or glitches	15%
Missing equipment including portable devices such as laptops, mobile phones PDAs, and USB drives	45%
Missing backup media	23%
Natural disasters such as hurricanes	0%
Social media	25%
Other	4%
Cannot determine	22%
Total	295%

Q25. What is your organization doing to address these vulnerabilities? Please select all that apply.	Pct%	FY 2007*
Nothing	9%	13%
Investing in data loss detection and prevention technology	32%	23%
Investing in encryption solutions	48%	54%
Investing in perimeter controls	25%	36%
Investing in security event management tools (SEIM)	45%	27%
Investing in identity & access management solutions	41%	35%
Conducting training and awareness	63%	54%
Creating policies and procedures	23%	
Establishing incident response plan	50%	43%
Hiring in-house personnel to lead data protection efforts	43%	26%
Hiring outside counsel to provide legal advice	54%	37%
Hiring security consultants to help establish data protection efforts	29%	15%
Conducting a post mortem	39%	21%
Taking a comprehensive inventory of all data at rest and in motion	20%	14%
Ensuring the removal of all sensitive and confidential data on devices that are removed or recycled	33%	37%
Controlling endpoints to the organization's systems and networks	56%	35%
Other	4%	6%
Total	614%	476%
*The Business Impact of a Data Breach. Ponemon Institute, May 2007		

Q26. Is your organization adopting any of the following practices designed to protect customer and consumer information? Please check all that apply.	Pct%
Training and awareness programs to address the risk of employee negligence	66%
Investment in security solutions to protect information from malicious insiders or hackers	45%
Conduct risk assessments/audits to understand how to improve the protection of customer and consumer information within the organization	52%
Conduct marketing campaigns to educate consumers and customers about how to protect their personal information	8%
Other	4%
None of the above	29%
Total	204%

Q27. Following the data breach were any of the following actions taken? Please check all that apply.	Pct%
Increased the IT security budget	61%
Hired additional IT security staff	28%
Increased the budget for the compliance department	9%
Increased the budget for the privacy office	15%
Hired additional privacy office staff	4%
Trained call center staff to respond to questions about privacy and the protection of customers' personal information	28%
Adopted new advertising/marketing campaigns designed to focus on privacy and protection of personal information	4%
Other	6%
No changes implemented	30%
Total	185%

Q28. How did the data breach affect the organization's use of personal and confidential information? Please check all that apply.	Pct%
No affect	31%
Our organization now limits the amount of personal data collected	49%
Our organization now limits the amount of personal data stored	42%
Strict rules were established to limit employees and third parties access to sensitive and confidential data	39%
Our organization now limits the amount of personal information used for marketing purposes	27%
Our organization now limits sharing with third parties	48%
Our organization now limits social media interaction	19%
Other	6%
Unsure	22%
Total	283%

Part 3: Organization characteristics and demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	16%
Manager	23%
Supervisor	19%
Technician	32%
Staff	3%
Contractor	2%
Other	3%
Total	100%

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	2%
General Counsel	2%
Chief Information Officer	58%
Chief Technology Officer	9%
Chief Information Security Officer	15%
Compliance Officer	4%
Chief Security Officer	3%
Chief Risk Officer	7%
Other	0%
Total	100%

D3. Experience	Mean	Median
D3a. Total years of IT or IT security experience	9.97	10.50
D3b. Total years in current position	4.95	5.00

D4. What industry best describes your organization's industry focus?	Pct%
Communications	3%
Consumer products	5%
Defense	2%
Education & research	2%
Energy	3%
Entertainment and media	4%
Financial services	19%
Health & pharmaceutical	11%
Hospitality	3%
Industrial	5%
Public sector	15%
Retail	10%
Services	7%
Technology & Software	8%
Transportation	3%
Total	100%

D5. Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	75%
Europe	67%
Middle East & Africa	38%
Asia-Pacific	58%
Latin America (including Mexico)	41%

D6. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	19%
500 to 1,000 people	22%
1,001 to 5,000 people	24%
5,001 to 25,000 people	16%
25,001 to 75,000 people	12%
More than 75,000 people	7%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

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.