



Business Case for Data Protection

Study of CEOs and other C-level Executives

Sponsored by

Ounce Labs

Independently conducted by Ponemon Institute LLC

Publication Date: July 15, 2009

Business Case for Data Protection

By Dr. Larry Ponemon July 31, 2009

I: Executive Summary

The Business Case for Data Protection, conducted by Ponemon Institute and sponsored by Ounce Labs, is the first study to determine what senior executives think about the value proposition of corporate data protection efforts within their organizations. In times of shrinking budgets, it is important for those individuals charged with managing a data protection program to understand how key decision makers in organizations perceive the importance of safeguarding sensitive and confidential information.

The research focused on how aware CEOs and other senior executives are about their organization's data protection efforts, what they believe is the economic justification for investment in a data protection program, how data protection programs support organizational goals, how effective they think their data protection leader is at using objective measures to justify spending and what objective measures should be used.

In this study, we learned that C-level executives believe good data protection practices can support important organizational goals such as compliance, reputation management, and customer trust. However, we also learned that the majority of respondents are not confident in their ability to safeguard sensitive and confidential information. Consequently, C-level executives see the importance of the following: developing a data protection strategy, training employees, temporary employees and contractors to safeguard sensitive data, and reducing potential security flaws within business-critical applications.

Our study also revealed CEOs hold a more positive view about the importance of data protection with respect to meeting organizational goals. For example, CEOs are more likely to believe that data protection increases corporate value. They also are more likely to believe their organizations are successful in preventing data loss or theft.

The following are what we believe to be the top findings in this study. We organized these findings according to five major themes that emerged: perceived threats to sensitive and confidential information, responsibility and accountability, impact on the organization, perceived value of a data protection program, and perception gaps between CEOs and other C-level executives.

1. C-level executives are concerned about threats to sensitive and confidential consumer and business customer data.

Eighty-two percent of C-level executives in our study report that their organization has experienced a data breach and many are not confident that they can prevent future breaches. Further, 94% of respondents report that they have had their data attacked in the last six months. In general, CEOs are more confident than others that their organizations are able to prevent data breaches.

Consumer and business customer data appear to be the most difficult to secure. Intellectual property and employee information seem to be easier to safeguard against loss or theft. In the last six months, 51% of respondents say that their organizations' data has been attacked daily, hourly and even more often. Only 6% of respondents report that their data is never attacked.

Respondents in companies that have a fully dedicated privacy leader (CPO) are more confident that their organization will not suffer a data breach. Those in companies that have a fully dedicated information security leader (CISO) are less confident that their organization will not suffer a data breach.

2. The person responsible for data protection is not held accountable for serious data breaches.

In the study, 79% of respondents report that one person is considered to be in charge of data protection and that person is considered by most to be the CIO, especially by the CEO. The CISO and CPO follow closely as being in charge of data protection. Very few have a chief data protection officer. It is interesting to note that the organizations really don't hold these individuals accountable. Specifically, the overwhelming majority (85%) do not believe a failure to stop a data breach under their watch would put their job in jeopardy.

The data protection function is located in legal (21%), followed by regulatory compliance (19%) and privacy (16%). We found that the data protection position has status within the organization. Despite this status, the data protection function is managed at the manager/director level.

3. Data protection programs help organizations achieve their business goals.

C-level executives believe data protection programs should have the following impact on an organization: ensuring regulatory and legal compliance, increasing or maintaining marketplace reputation and brand and increasing customer trust and loyalty. Enhancing the value of information assets and decreasing employee turnover are goals not considered dependent upon good data protection efforts.

When asked what the most important and important activities are for a data protection program, 75% of respondents believe it is a data protection strategy, 71% say training of employees, temporary employees and contractors and 70% believe it is reducing potential security flaws within business-critical applications.

In order to achieve organizational goals it is important to collaborate with the legal department, information security, privacy office and corporate IT. Logistics and sales are not considered important functions with whom to collaborate.

4. C-level executives believe data protection programs yield an excellent ROI.

C-level executives believe the cost savings from investing in a data protection program of \$16 million is substantially higher than the extrapolated value of data protection spending of \$3.7 million. This suggests a very healthy ROI for data protection programs.

Respondents believe the purpose of data protection programs is to reduce or mitigate the risk of data loss or theft (i.e. data breach), improve information flows about people, such as consumers, customers, business partners and other stakeholders, and increase brand or marketplace image. The reduction of potential risks under e-discovery laws and increasing employee trust are not considered as important.

Similar to above, the value proposition of a good data protection program, according to respondents, is improvement of information flows about people, the increase in brand recognition, and the reduction in operational inefficiencies by creating more efficient uses of data.

Currently, the most frequently used measures to determine the success of a data protection program include how much data breach recovery costs, fines and legal defense costs are reduced. Given the goals C-level executives have for their data protection programs, they feel they should have measures that determine asset performance, asset protection, including the protection of intellectual properties, and reputation management.

5. CEOs are more positive about data protection than other C-level executives.

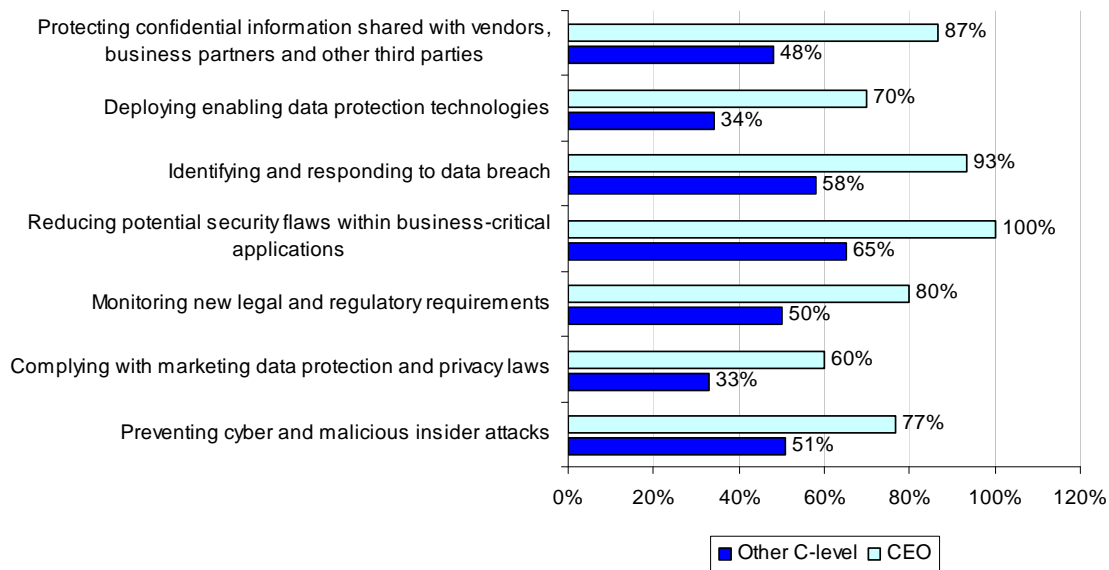
Thirty respondents (14%) in this study are CEOs. The remaining 183 respondents are C-level executives who report to their company's CEO, such as chief operating officers, division presidents, general managers, chief information officers and other titles.

In general, CEOs responses track closely to the overall sample. However, CEOs are more likely to see data protection as increasing the ability to achieve such organizational goals as improving the flow of relevant information about customers and employees across national borders and enabling the pursuit of new global business opportunities. Table 1 reports the data protection efforts rated by all respondents. Each percentage is the combined very important and important rating (from a five-point scale ranging from very important to irrelevant).

Table 1 Typical data protection efforts rated as important or very important combined	Other C-level	CEO
Developing a data protection strategy for the organization	70%	87%
Training employees, temporary employees and contractors	72%	63%
Reducing potential security flaws within business-critical applications	65%	100%
Establishing and managing a crisis management, disaster management, and business continuity plan	63%	70%
Identifying and responding to data breach (loss or theft of personal information)	58%	93%
Conducting due diligence on transactions and relationships that involve the sharing of personal and confidential information	66%	53%
Protecting personal or confidential information shared with vendors, business partners and other third parties	48%	87%
Ensuring record retention requirements are met	57%	53%
Monitoring new legal and regulatory requirements	50%	80%
Preventing cyber and malicious insider attacks	51%	77%
Conducting data vulnerability or privacy impact assessments for new products	43%	60%
Auditing business processes for compliance with data protection and privacy policies	49%	40%
Mapping data flows and conducting a data inventory	48%	40%
Implementing customer access and redress programs	43%	43%
Deploying enabling data protection technologies	34%	70%
Creating policies and SOPs for the handling and use of personal information	39%	63%
Complying with employee data protection and privacy laws	42%	27%
Analyzing data collection, use and sharing	44%	23%
Complying with marketing data protection and privacy laws	33%	60%
Implementing employee access and redress programs	39%	23%
Responding to e-discovery requests	25%	43%
Performing background checks on employees, temporary employees and contractors	20%	13%
Average	48%	58%

Bar Chart 1 reports those priorities with the largest differences or gaps between CEOs and other C-level executives. As can be seen, CEOs perceive the protection confidential information shared with third parties, deploying enabling technologies, responding to data breach and reducing security flaws in business-critical applications as more important than other C-level executives.

Bar Chart 1
Gap between CEOs and other C-level executives (CEO > other C-level)
 Each bar represents the combined percentage of very important & important



Other salient differences between the CEO and other C-level executives are:

- CEOs are more confident that a data breach can be avoided than other C-level executives. They are also less aware of data breach incidents than other respondents.
- CEOs are more likely to believe marketplace reputation and customer trust are dependent upon good data protection efforts than other C-level executives. In contrast, they are less likely to believe that ensuring regulatory and legal compliance is dependent upon good data protection efforts.
- CEOs more strongly believe that data protection reduces or mitigates the risk of data loss or theft followed by increasing their organization's marketplace image and brand than other C-level executives.

II: Analysis of key findings

Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as the Appendix to this paper.

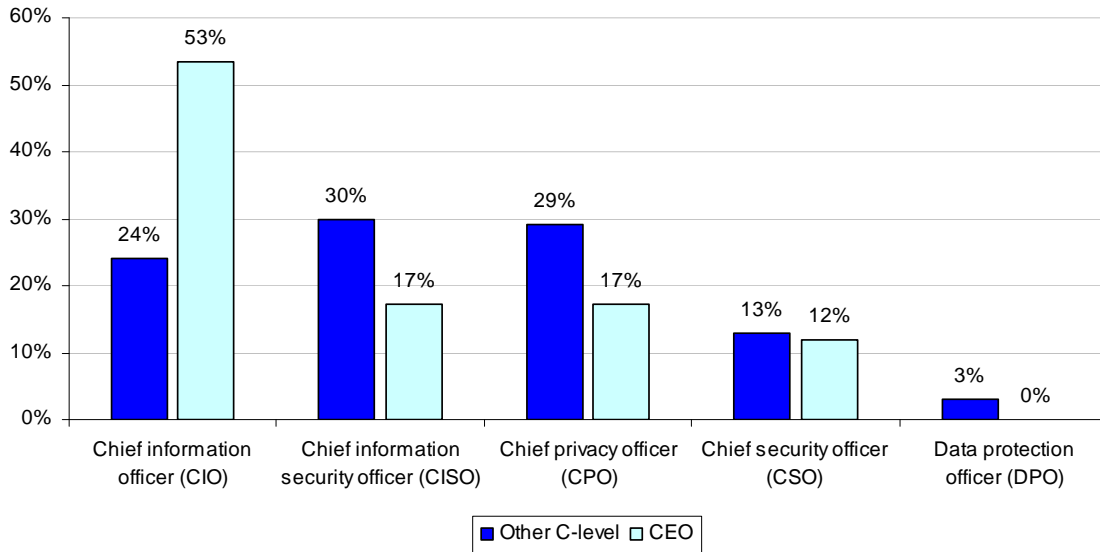
The CIO is considered by the largest number of respondents to be responsible for data protection.

A large majority of respondents (79%) report that there is one person responsible for the overall data protection effort within their organizations.

As shown in Bar Chart 2, 53% of CEOs believe their company's chief information officer (CIO) is accountable for data protection. In sharp contrast, only 24% of the other C-level executives believe the CIO is most accountable for data protection. Both CEOs and other C-level executives

believe that the chief information security officer (CISO) and the chief privacy officer (CPO) are next in line in terms of individual responsibility or accountability for protecting information assets.

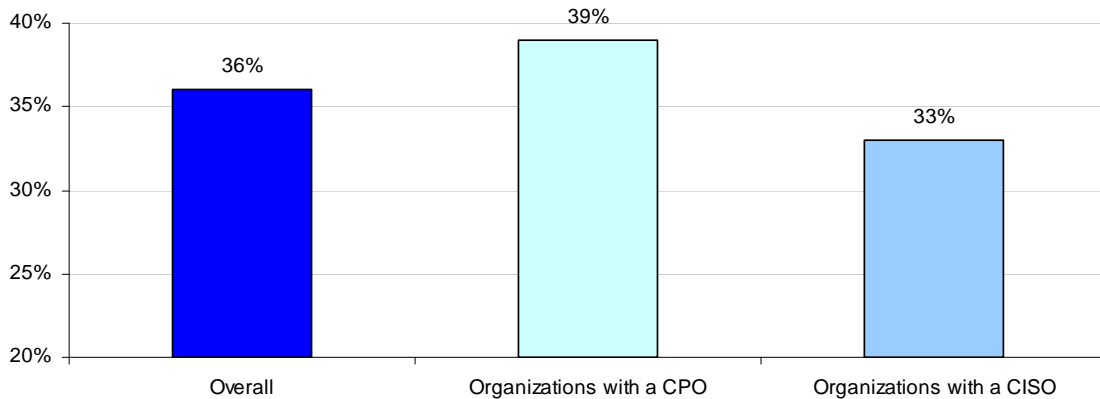
Bar Chart 2
Who is most responsible for data protection in the organization?
 Each bar shows the percentage frequency for CEOs and other C-level respondents



Executives are not confident their organizations will avoid a data breach.

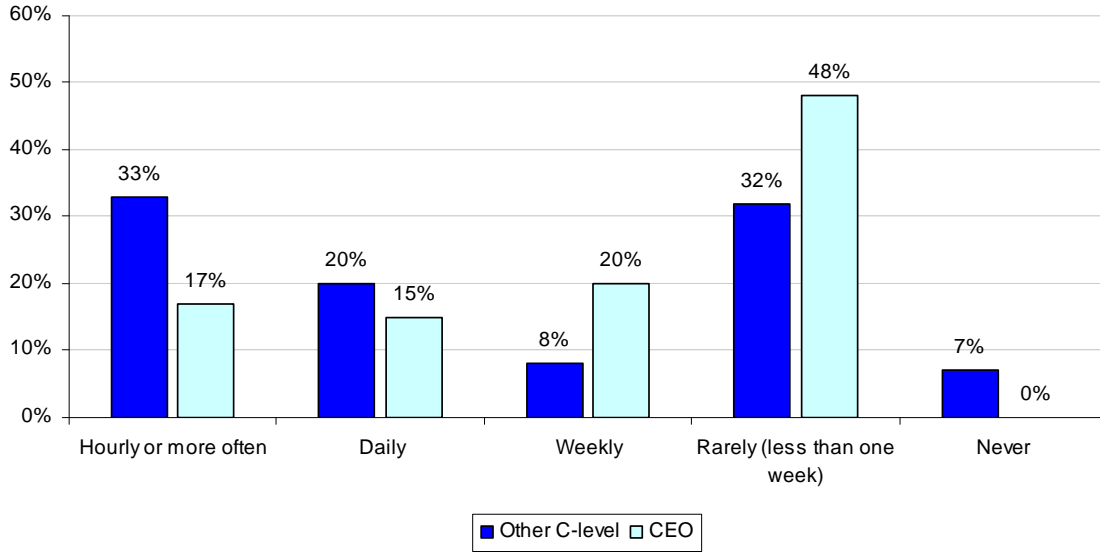
Bar Chart 3 shows that only 36% of respondents say they are confident their organizations will not suffer a data breach within the next 12 months. Respondents whose organization has a CPO in-charge of data protection enjoy a slightly higher level of confidence at 39%. Organizations with a CISO in-charge of data protection experience a slightly lower confidence level at 33%.

Bar Chart 3
Confidence that the organization will not suffer a data breach within the next year
 Each bar shows the combined very confident & confident response



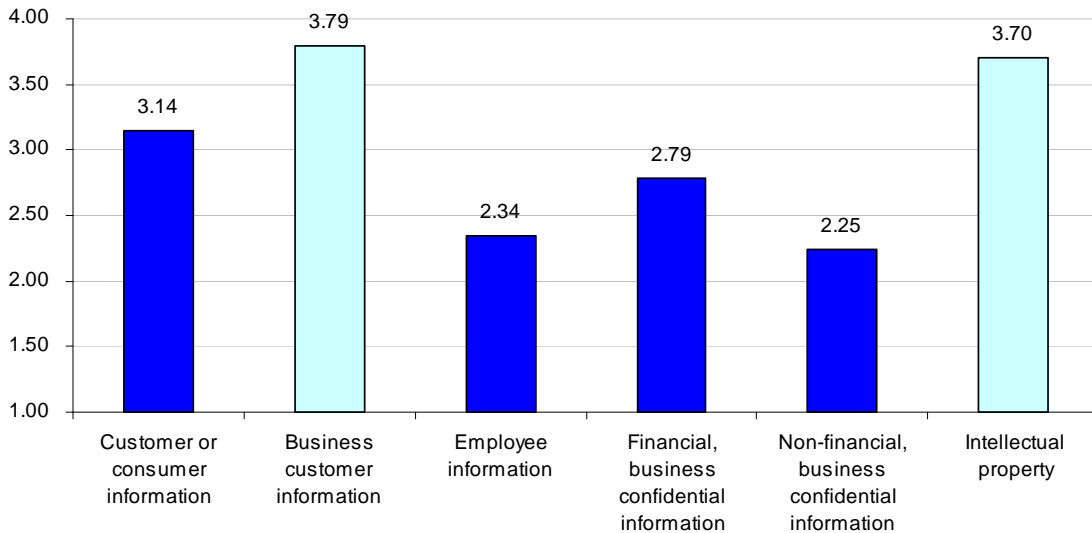
Bar Chart 4 reports the frequency of attacks against the company’s confidential or sensitive data experienced over the past year. As shown, CEOs believe that the frequency of attacks is less severe than other C-level executives.

Bar Chart 4
In the past year, how often does your organization's data been attacked
 Each bar represents the percentage frequency provided by respondents



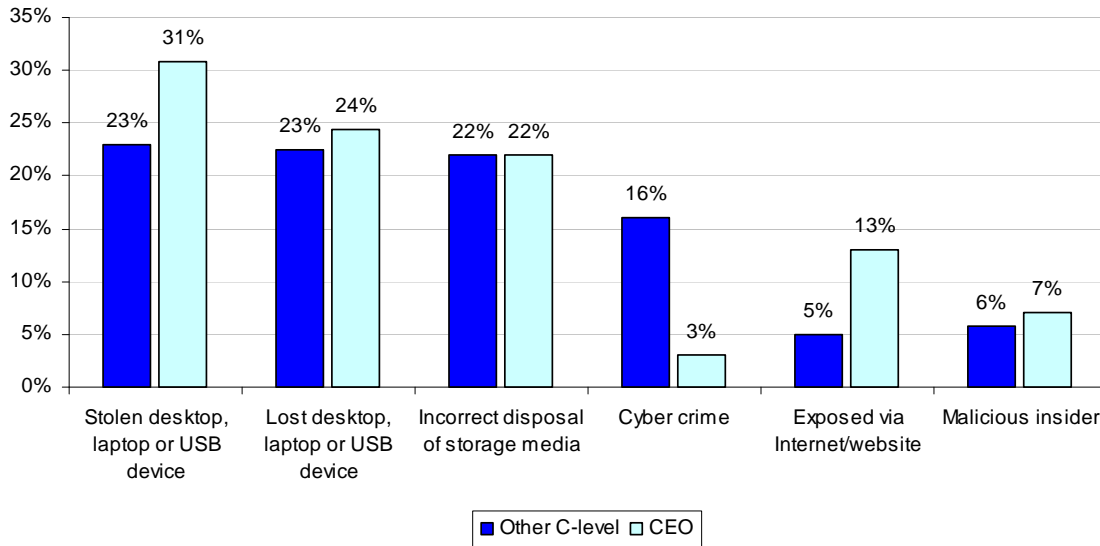
Bar Chart 5 reports the priority ranking by all executives. Clearly, the top two most critical data types are business customer information and intellectual property. This is followed by customer or consumer information and financial business confidential information. Of least importance to organization’s operations, is data about employees and non-financial business information.

Bar Chart 5
Average rank of data believed to be most critical to the organization's operations
 C-level average rank ordering from 5 = most important to 1 = least important



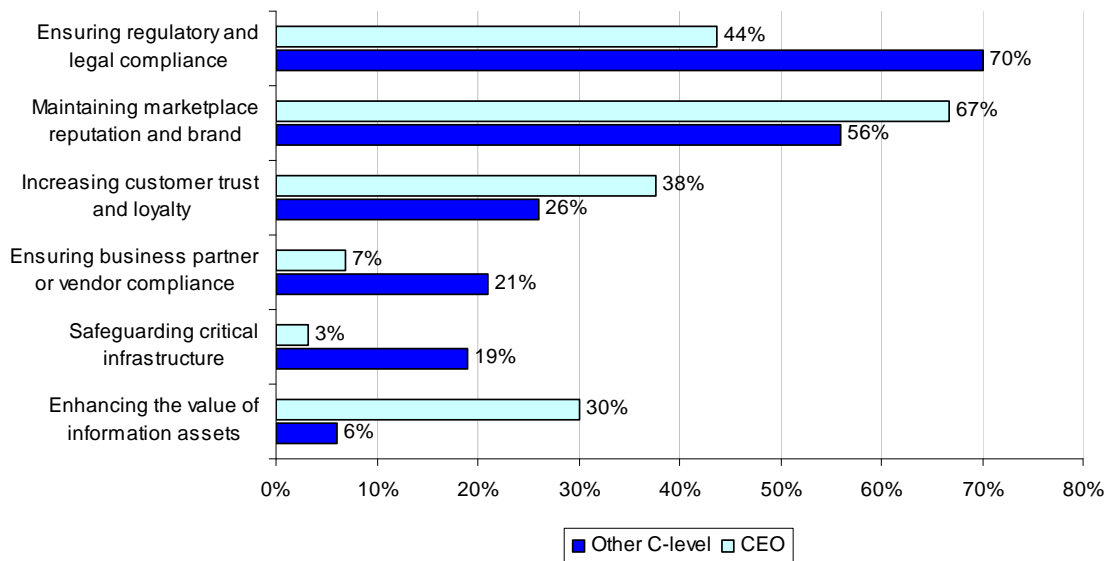
According to Bar Chart 6, both CEOs and other C-level executives believe the source of greatest risk to sensitive and confidential data come from employees who have their mobile devices either stolen or lost. The third source of greatest risk is the incorrect disposal of hard or soft data files

Bar Chart 6
Sources of greatest risk to sensitive data
 Each bar represents the percentage frequency provided by respondents



As shown in Bar Chart 7, ensuring regulatory and legal compliance is the number one organizational goal dependent upon good data protection for other C-level executives. In the case of CEOs, the number one goal dependent upon good data protection efforts concerns the maintenance of marketplace reputation and brand, followed by regulatory compliance and customer loyalty.

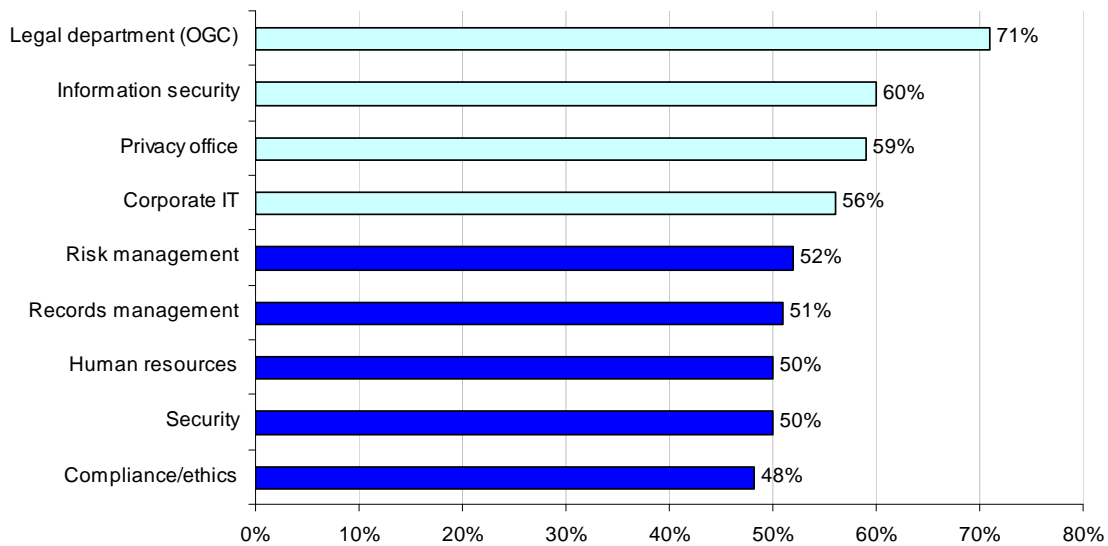
Bar Chart 7
Organizational goals that depend upon data protection
 Each bar represents the frequency of responses



Collaboration with the legal and information security departments is critical to achieving organizational data protection goals.

To achieve organizational goals such as compliance, brand maintenance and customer loyalty, Bar Chart 8 shows that more than 71% of all respondents believe it is either very important or important to collaborate with the company's legal department. The next critical collaborations concern information security (60%) and the privacy office (59%).

Bar Chart 8
What business functions need to collaborate to achieve data protection goals?
 Each bar represents the frequency of responses



A data protection strategy, training programs and reduction of potential security flaws within business-critical applications are considered the most important activities for data protection.

As shown previously in Table 1, the most important activities to achieving good data protection are: developing a data protection strategy for the organization; training employees, temporary employees and contractors; and reducing potential security flaws within business critical applications.

Among the least important involve employee data. These are: complying with employee data protection and privacy laws; implementing employee access and redress programs and performing background checks on employees, temporary employees and contractors. Another unimportant activity is responding to e-discovery requests.

Investing in data protection is important to understanding customer and business relationships and increasing brand image.

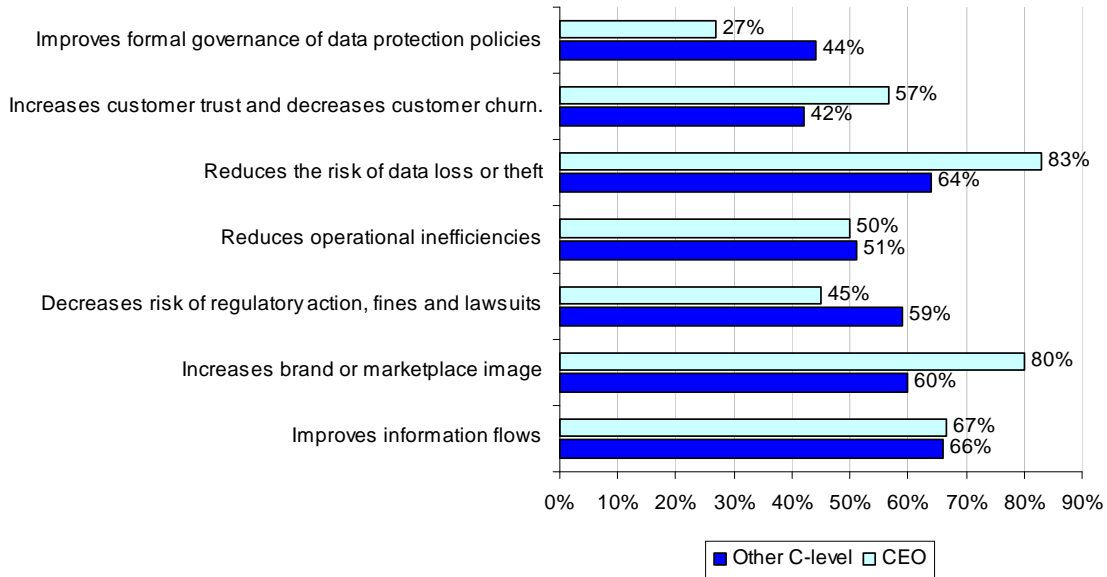
When asked whether a coherent and comprehensive enterprise data protection program increases their organization's value, 83% of CEOs and 64% of other C-level executives say it reduces or mitigates the risk of data loss or theft (see Bar Chart 9). Sixty-seven percent of CEOs and 66% of other C-level executives believe that it improves information flows about people such

as consumers, customers, business partners and other stakeholders. More than 80% of CEOs and 60% of other C-level executives believe investing in data protection increases brand or marketplace image.

Bar Chart 9

How does enterprise data protection increase organizational value?

Each bar represents the frequency of responses

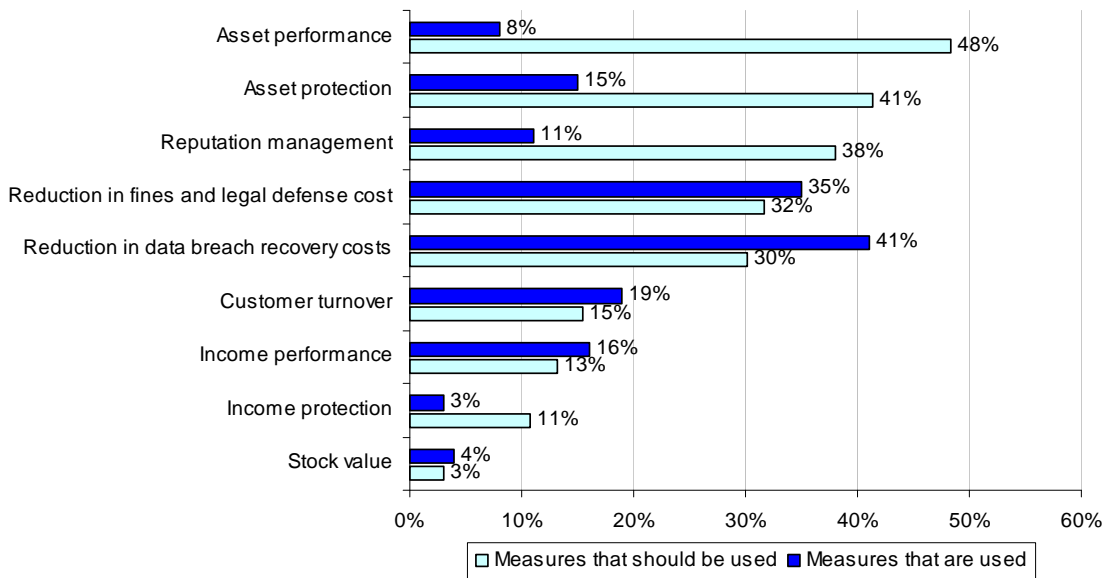


Measures of success should focus on the value of information assets and protecting the organization's reputation.

Bar Chart 10

Measures that should be used vs. that is presently used to evaluate data protection

Each bar represents the percentage frequency of respondents

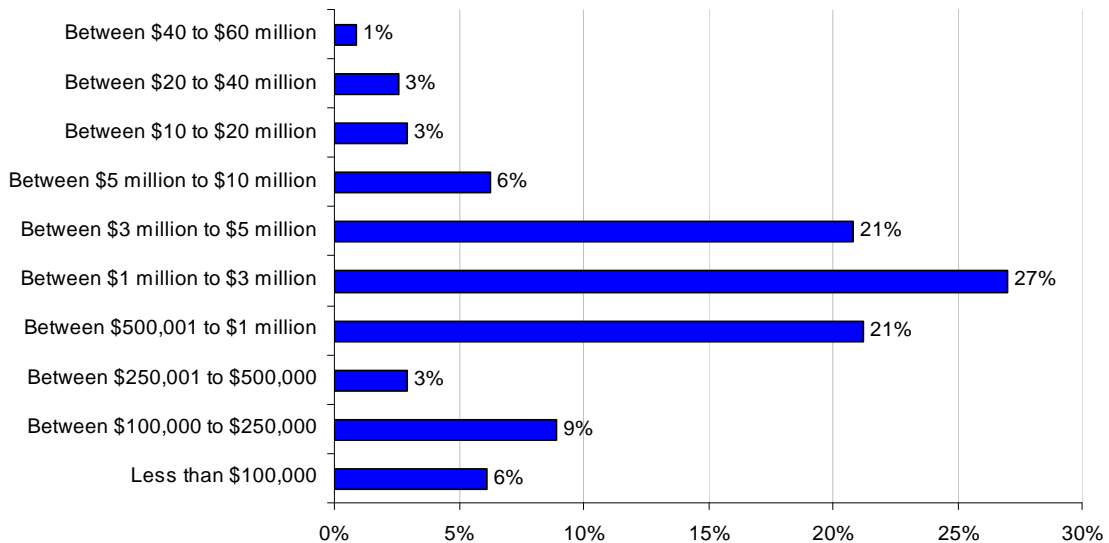


Executives in our study believe that asset performance, asset protection and reputation management measures *should be* used to measure the effectiveness of data protection efforts. However, as shown in Bar Chart 10, the most commonly used measures pertain to the reduction

of data breach and legal costs. The above chart shows differences or gaps between those measures that “should be” used versus “is” used today according to respondents.

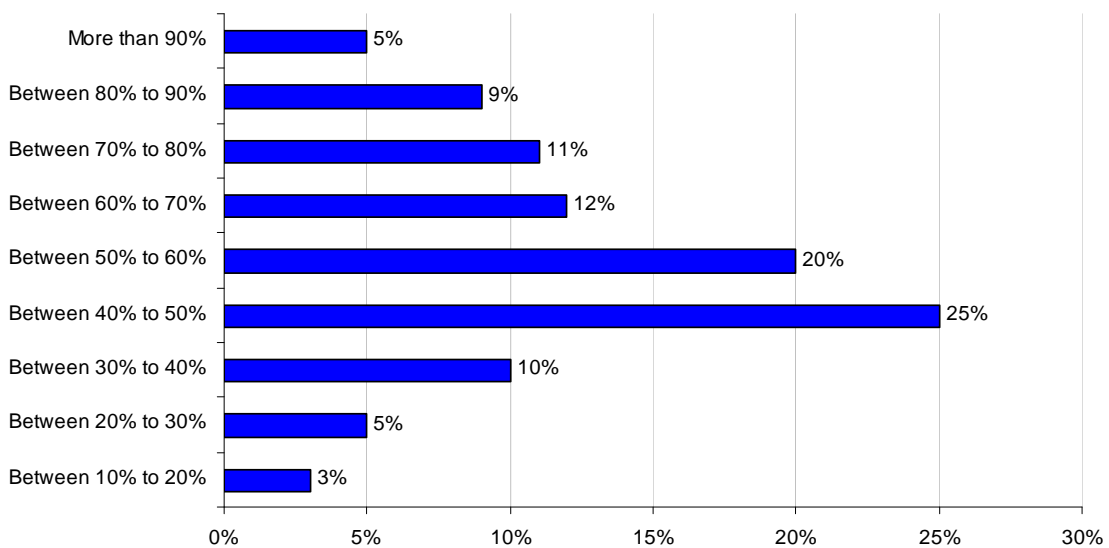
Bar Chart 11 shows the distribution frequency of annual budget dedicated to data protection. The median extrapolated value from this distribution is \$3.7 million.

Bar Chart 11
What is the approximate annual budget for enterprise data protection?
 Each bar represents the percentage frequency of respondents



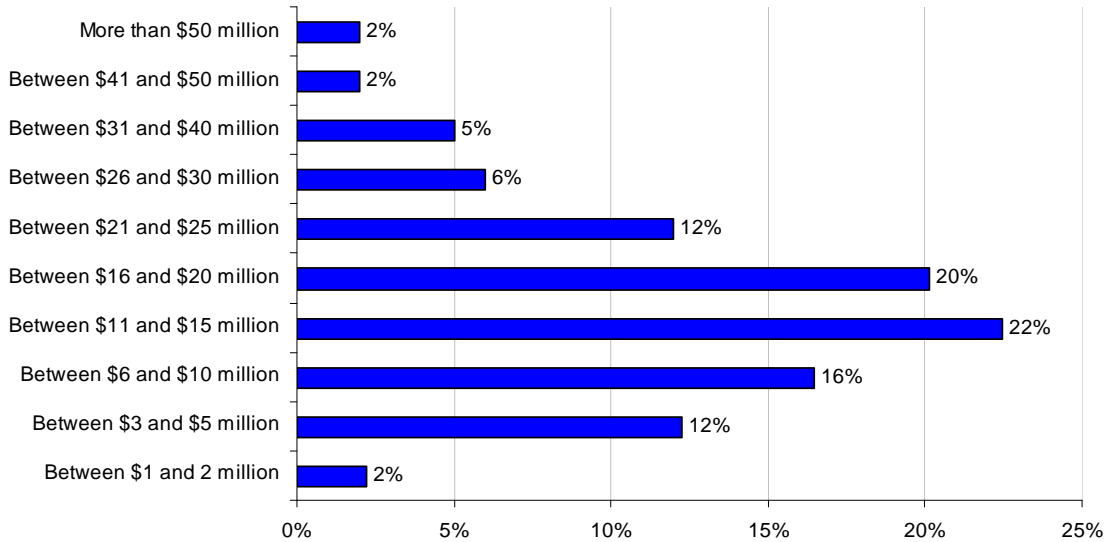
Bar Chart 12 shows the percentage distribution frequency of data protection spending dedicated to enabling technologies for privacy and data security. Accordingly, the median extrapolated median percentage spent on enabling technologies is 56% of the overall data protection budget.

Bar Chart 12
Enterprise data protection budget earmarked for enabling technology
 Each bar represents the percentage frequency of respondents



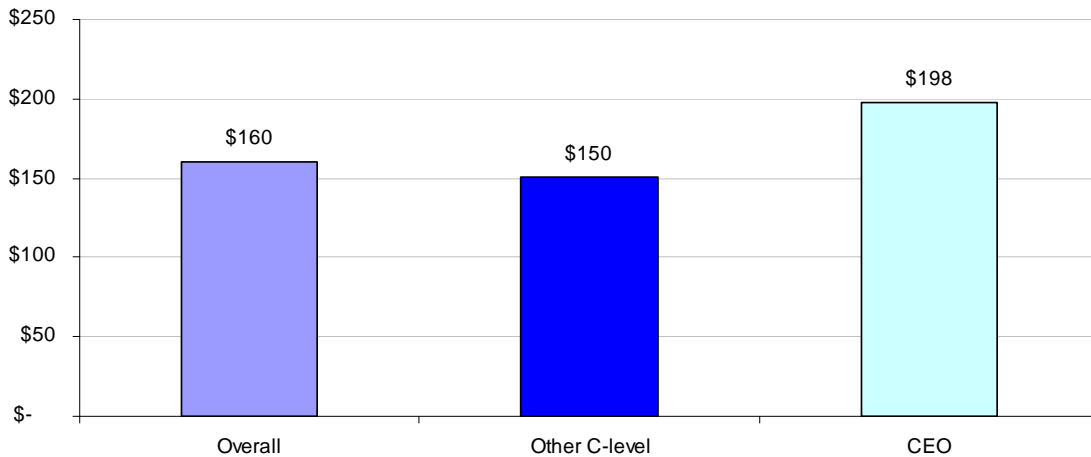
Bar Chart 13 reports the cost savings or revenue improvements realized by companies as a result of enterprise data protection efforts. The median extrapolated value from this distribution is \$16 million, which is substantially higher than the value of data protection spending of \$3.7 million mentioned above. This suggests a healthy ROI for data protection programs.

Bar Chart 13
Cost savings or revenue improvements resulting from data protection efforts
 Each bar represents the percentage frequency of respondents



Executives in this study estimated the average data breach cost per compromised record is \$160. CEOs estimated a higher amount of \$198 per compromised record, which is closer to the \$202 value reported in an earlier published report.¹

Bar Chart 14
Data breach cost on a per capita (per compromised record) basis
 Each bar represents the extrapolated median value



¹ See Ponemon Institute's [Annual Cost of a Data Breach Study](#) published in January 2009.

IV: Methods

This study was conducted over a six-month period concluding in June 2009. CEOs and other very senior executives were recruited to participate in this study.² The final survey sample consisted of 213 executives who work various industry sectors. The description of the sample according to the respondent's title is provided in Table 2.

	Freq.	Overall%
Chief executive officer	30	14%
Chief operating officer	22	10%
Division president, general manager or executive vice president	89	42%
Chief information officer	27	13%
Other C-level executives	45	21%
Total	213	100%

Respondents in this sample were selected from purchased contact lists and all voluntarily participated. All respondents were interviewed either in-person or by telephone. Only executives who responded yes to the question "Does your organization have a data protection and privacy program or initiative?" were included in the analysis.

Pie Chart 1 reports the sample distribution by industry classification. As shown, the largest segments include financial services (17%), technology and software (11%), and retail (10%).

Pie Chart 1: Sample distribution by Industry segments

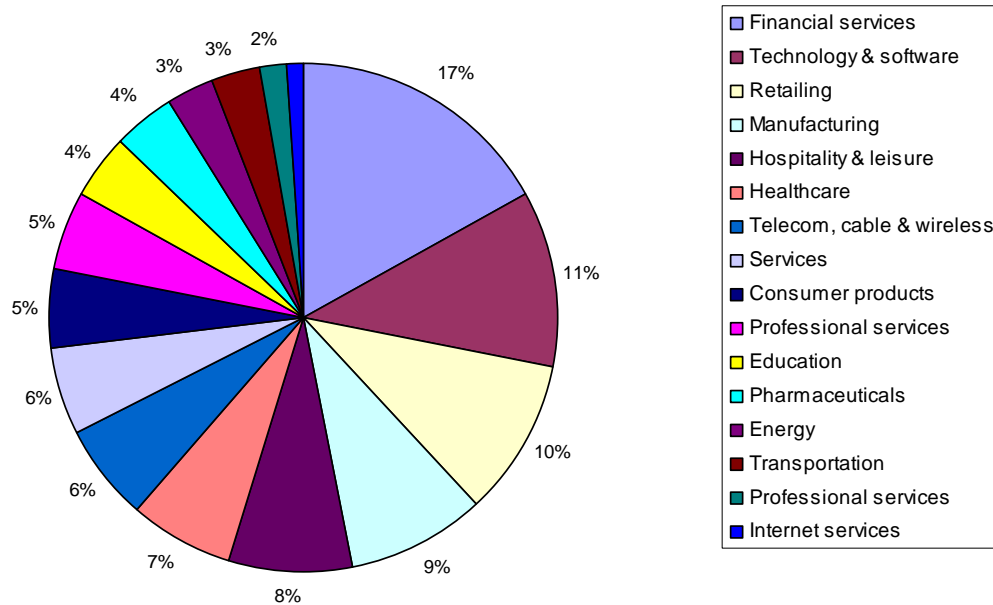


Table 3a reports the organizations' worldwide headcount showing that 41% have more than 5,000 employees Table 3b reports the organization's gross revenues or sales showing 44% have more that \$1 billion in total revenues in fiscal year 2008.

² By design, C-level respondents who were not CEOs were no more than two steps away from the CEO or Chairman level in their organizations.

Table 3a Worldwide headcount	Overall%
Less than 500 people	22%
500 to 1,000 people	17%
1,001 to 5,000 people	20%
5,001 to 25,000 people	34%
25,001 to 75,000 people	6%
More than 75,000 people	1%
Total	100%

Table 3b Total 2008 revenues	Overall%
Less than \$100 million	21%
\$101 to \$500 million	17%
\$501 million to \$1 billion	18%
\$1.1 billion to 10 billion	35%
\$11 billion to 20 billion	6%
More than 20 billion	3%
Total	100%

Table 4a reports the frequency of companies that are publicly traded on NYSE, NASDAQ or other exchanges. Table 4c reports the geographic footprint of participating organizations.

Table 4a Is your company publicly traded?	Overall%
Yes, NYSE	24%
Yes, NASDAQ	20%
Yes, overseas exchange	5%
Yes, other minor exchange	8%
No	43%
Total	100%

Table 4b Operating locations	Overall%
United States	100%
Canada	61%
Europe	63%
Asia-Pacific	57%
Latin America (including Mexico)	42%
Total	323%

V: Concluding thoughts

We believe C-level executives understand the value propositions of good data protection. While they tend to mostly see data protection as necessary to meeting regulatory requirements, more aspirational goals such as establishing and protecting reputation and building customer trust and loyalty are emerging as a value of good data protection practices.

Currently, data protection measures of success most often focus on regulatory and compliance. To make the business case for data protection, we recommend data protection professionals begin to use measures that were ranked highest among C-level respondents. These include enhancing the value of information assets, protecting the value of corporate intellectual property, and preserving customer loyalty through trusted data protection practices.

What do these findings mean for data protection professionals concerned about their role in an organization and the ability to secure investment for the protection of sensitive and confidential information? Our research suggests C-level executives do see the importance and value of data protection and privacy in their organizations.

Despite an enthusiastic set of responses, this study finds conventional success measures – such as a focus on data breach prevention or compliance – are inadequate in justifying the full value of enterprise data protection. The value proposition of enterprise data protection that CEOs and other C-level executives would like to see relates to asset performance, asset protection and brand enhancement.

Research Caveats

There are inherent limitations to this research that need to be carefully considered before drawing inferences from our findings. First, our presented findings are based on a representative sample of 213 respondents who were carefully recruited and pre-screened before participating. Despite our attempts to select a representative sample of CEOs and other C-level executives, it is always

possible that individuals who choose not to participate are substantially different in terms of their underlying beliefs about data protection.

In addition to the possibility of sampling error, the quality of our research is based on the integrity of confidential responses provided. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a complete or truthful response.

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 e-mail:

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

Ponemon Institute LLC

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.

VI. Appendix

Following are all the questions included in the field survey instrument. The overall responses are shown in a frequency or percentage frequency format.

Q1. Does your organization have a data protection and privacy program or initiative?	Freq.
Yes	205
No (Stop)	2
Not sure (Stop)	6
Total	213

Q2a. Is there one person responsible for the overall data protection effort within your enterprise?	Overall%
Yes	79%
No	21%
Total	100%

Q2b. Who is your organization's data protection leader? That is who is responsible for the overall data protection effort within your enterprise?	Overall%
Chief information officer (CIO)	30%
Chief information security officer (CISO)	27%
Chief privacy officer (CPO)	27%
Chief security officer (CSO)	13%
Data protection officer (DPO)	2%
Other (please specify)	1%
Total	100%

Q2c. What is the organizational level that best describes the position level of your organization's data protection leader?	Overall%
EVP or SVP	2%
VP	15%
Executive Director	16%
Director	25%
Manager	30%
Supervisor	11%
Other (please specify)	1%
Total	100%

Q2d. Is this a full time position?	Overall%
Yes	73%
No	27%
Total	100%

Q2e. Who else in your organization is responsible for data protection? Please check the other executives within your organization who are responsible for data protection.	Overall%
General Counsel	62%
Cross-functional committee	54%
Chief Information Officer	51%
Compliance/Ethics Officer	43%
Human Resources VP	36%
Chief Marketing Officer	29%
Chief Risk Officer	22%
Chief Security Officer	16%
Chief Financial Officer	11%
Not sure	5%
Total	328%

Q3. What types of data are most critical to your organization's operations? Please rank order the following list from 1 = the most critical information to 5 = your least critical information.	Overall Avg Rank
Customer or consumer information	2.86
Business customer information	2.21
Employee information	3.66
Financial, business confidential information	3.21
Non-financial, business confidential information	3.75
Intellectual property	2.30

Q4. What types of data do you believe are most difficult to secure within your organization? Please check the top two choices.	Overall%
Customer or consumer information	53%
Business customer information	51%
Employee information	6%
Financial, business confidential information	16%
Non-financial, business confidential information	38%
Intellectual property	10%
Total	174%

Q5a. Has your company ever experienced a data breach?	Overall%
Yes	82%
No	18%
Total	100%

Q5b. How confident are you that your organization will not suffer a data breach in the next 12 months?	Overall%
Very confident	12%
Confident	24%
Somewhat confident	23%
Not confident	41%
Total	100%

Q5c. If your organization experienced a serious data breach, how would it affect your job security?	Overall%
I would certainly lose my job	0%
I would likely lose my job	2%
I might lose my job	13%
I would not lose my job	85%
Total	100%

Q6. In the last 12 months, how often has your organization's data been attacked?	Overall%
Hourly or more often	31%
Daily	20%
Weekly	10%
Rarely (less than one week)	33%
Never	6%
Total	100%

Q7. What is the source of greatest risk to your sensitive data? Please select only one response.	Overall%
Stolen computer/flash drive/tape	25%
Lost computer/flash drive/tape	23%
Incorrect disposal of hard/soft files	22%
Hacker/cyber crime	12%
Exposed via Internet/website	7%
Malicious insider	6%
Exposed via email	2%
Skimming	1%
Exposed via mailing	1%
Total	100%

Q8. Where within your organization is the data protection function located? Please select only one response.	Overall%
Legal	21%
Regulatory compliance	19%
Privacy office	16%
Information security department or office	13%
Corporate IT	7%
Public relations	6%
Risk management	4%
Government affairs	4%
Corporate ethics	3%
Human resources	3%
Records management	3%
Marketing	1%
Total	100%

Q9. Please select from the following list of organizational goals that are <u>dependent</u> upon good data protection efforts? Please select only two choices.	Overall%
Ensuring regulatory and legal compliance	65%
Increasing or maintaining marketplace reputation and brand	58%
Increasing customer trust and loyalty	28%
Ensuring business partner or vendor compliance	18%
Safeguarding critical infrastructure	15%
Enhancing the value of information assets	9%
Decreasing employee turnover	2%
Total	197%

Q10. Based on the organizational goals listed above, how important is collaboration between data protection and other business functions within your organization? Please use the following scale to indicate the importance of working closely with each of these functions to achieve data protection goals: 1 = very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Overall%*
Legal department (OGC)	71%
Information security	60%
Privacy office	59%
Corporate IT	56%
Risk management	52%
Records management	51%
Security	50%
Human resources	50%
Compliance/ethics	48%
Public relations	45%
Internal audit	44%
Government or public affairs	39%
Marketing & communications	34%
Procurement	29%
Finance & accounting	23%
Logistics	10%
Sales	2%
Average	43%

*Percentage is the combined very important and important response.

Q11. Following are typical business activities for organizational data protection efforts. Please rate the importance of each action using the following scale to indicate importance: 1 = very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Overall%*
Developing a data protection strategy for the organization	75%
Training employees, temporary employees and contractors	71%
Reducing potential security flaws within business-critical applications	70%
Establishing and managing a crisis management, disaster management, and business continuity plan	66%
Identifying and responding to data breach (loss or theft of personal information)	65%
Conducting due diligence on transactions and relationships that involve the sharing of personal and confidential information	64%
Protecting personal or confidential information shared with vendors, business partners and other third parties	57%
Ensuring record retention requirements are met	56%
Monitoring new legal and regulatory requirements	56%
Preventing cyber and malicious insider attacks	54%
Conducting data vulnerability or privacy impact assessments for new products	48%
Auditing business processes for compliance with data protection and privacy policies	47%
Mapping data flows and conducting a data inventory	46%
Implementing customer access and redress programs	43%
Deploying enabling data protection technologies	42%
Creating policies and SOPs for the handling and use of personal information	41%
Complying with employee data protection and privacy laws	39%
Analyzing data collection, use and sharing	39%
Complying with marketing data protection and privacy laws	37%
Implementing employee access and redress programs	35%
Responding to e-discovery requests	29%
Performing background checks on employees, temporary employees and contractors	18%
Average	50%

*Percentage is the combined very important and important response.

Q12. Does a coherent and comprehensive enterprise data protection program increase your organization's value? Please rate your level of agreement or disagreement with each statement about your company's data protection efforts provided below using the following scale: 1 = strongly agree, 2 = agree, 3 = unsure, 4 = disagree, 5 = strongly disagree.	Overall%*
Improves information flows about people such as consumers, customers, business partners and other stakeholders	66%
Increases brand or marketplace image	64%
Decreases risk of regulatory action, fines and lawsuits	56%
Reduces operational inefficiencies by creating more efficient uses of data	51%
Reduces or mitigates the risk of data loss or theft (i.e., data breach)	67%
Increases customer trust and decreases customer churn	45%
Improves formal governance of data protection policies	40%
Improves the flow of relevant information about customers and employees across national borders	39%
Increases the quality and accuracy of information	38%

Improves IT processes because of a better data governance structure	38%
Increases our suppliers' accountability to our data protection and privacy policies	37%
Enables the pursuit of new global business opportunities	36%
Reduces the cost of due diligence in mergers & acquisitions	32%
Reduces potential risks under e-discovery laws	25%
Increases employee trust and decreases employee churn	13%
Average	43%

*Percentage is the combined very important and important response.

Q13. Please rate each value proposition based on importance to your organization using the following scale: 1 = very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Overall%*
Reduces operational inefficiencies by creating more efficient uses of data	52%
Improves IT processes because of a better data governance structure	37%
Improves information flows about people such as targeted consumers, customers, business partners and other stakeholders	65%
Increases brand or marketplace image	62%
Improves formal governance of data protection policies	41%
Decreases risk of regulatory action, fines and lawsuits	55%
Increases our suppliers' accountability to our data protection and privacy policies	35%
Increases customer trust and decreases customer churn	45%
Increases employee trust and decreases employee churn	13%
Reduces potential risks under e-discovery laws	24%
Reduces the cost of due diligence in mergers & acquisitions	32%
Improves the flow of relevant information about customers and employees across national borders	37%
Enables the pursuit of new global business opportunities	36%
Increases the quality and accuracy of information	37%
Reduces or mitigates the risk of data loss or theft (i.e., data breach)	48%
Average	41%

*Percentage is the combined very important and important response.

Q14. What objective measures should be used to justify spending on data protection within your organization? Please choose all that apply.	Overall%
Asset performance such as increasing the value of customer information	48%
Asset protection including the protection of intellectual properties	41%
Reputation management	38%
Reduction in fines and legal defense cost	32%
Reduction in data breach recovery costs	30%
Customer turnover	15%
Income performance, such as a more effective marketing campaign	13%
Income protection	11%
Stock value	3%
Employee turnover	1%
Total	232%

Q16. How effective is your data protection leader at using objective measures to justify spending on data protection? Please state whether or not each one of the following objective measures is being used to justify your organization's data protection efforts today:	Measure is used today
Reduction in data breach recovery costs	41%
Reduction in fines and legal defense cost	35%
Customer turnover	19%
Income performance, such as a more effective marketing campaign	16%
Asset protection including the protection of intellectual properties	15%
Reputation management	11%
Asset performance such as increasing the value of customer information	8%
Stock Value	4%
Income protection	3%
Employee turnover	0%
Average	15%

Q17a. Approximately (gut feel is okay), what is the dollar range that best describes your organization's budget for data protection next year (12 months from now)?	Overall%
Less than \$100,000	6%
Between \$100,000 to \$250,000	9%
Between \$250,001 to \$500,000	3%
Between \$500,001 to \$1 million	21%
Between \$1 million to \$3 million	27%
Between \$3 million to \$5 million	21%
Between \$5 million to \$10 million	6%
Between \$10 to \$20 million	3%
Between \$20 to \$40 million	3%
Between \$40 to \$60 million	1%
More than \$60 million	0%
Total	100%

Q17b. Is the budget for data protection adequate?	Overall%
Yes	56%
No	44%
Total	100%

Q17c. If no, how much would you like to see it increased?	Overall%
More than 50%	14%
Between 40 and 50%	17%
Between 30 and 40%	18%
Between 20 and 30%	14%
Between 10 and 20%	21%
Less than 10%	15%
Total	100%

Q18a. Is spending on compliance initiatives diverting resources from other security initiatives?	Overall%
Yes	8%
No	64%
Unsure	28%
Total	100%

Q18b. If yes or unsure, is this causing your data to be less secure?	Overall%
Yes	50%
No	43%
Not applicable	7%
Total	100%

Q19. Approximately (gut feel is okay), what percentage of the 2009 data protection budget is dedicated to such technology solutions as application security, DLP and encryption?	Overall%
Less than 5%	0%
Between 5% to 10%	0%
Between 10% to 20%	3%
Between 20% to 30%	5%
Between 30% to 40%	10%
Between 40% to 50%	25%
Between 50% to 60%	20%
Between 60% to 70%	12%
Between 70% to 80%	11%
Between 80% to 90%	9%
More than 90%	5%
Total	100%

Q20. Approximately (gut feel is okay), what is the dollar range that best describes your organization's cost savings or revenue improvements as a result of data protection efforts in 2009?	Overall%
Less than \$1 million	0%
Between \$1 to 2 million	2%
Between \$2 to \$5 million	12%
Between \$5 to \$10 million	16%
Between \$10 to \$15 million	22%
Between \$15 to \$20 million	20%
Between \$20 to \$25 million	12%
Between \$25 to \$30 million	6%
Between \$35 to \$40 million	5%
Between \$45 to \$50 million	2%
Between \$55 to \$60 million	2%
More than \$60 million	0%
Total	100%

Q21. If your company had a data breach involving the loss or theft of sensitive personal information about customers, employees or consumers (say 1,000 or more records), what would this incident cost your company per record lost?	Overall%
Less than \$50	12%
Between \$50 to \$100	28%
Between \$101 to \$150	21%
Between \$151 to \$200	15%
Between \$201 to \$250	9%
Between \$251 to \$300	6%
Between \$301 to \$350	1%
Between \$351 to \$400	5%
Between \$401 to \$450	0%
Between \$451 to \$500	1%
Between \$501 to \$1,000	2%
More than \$1,000	1%
Total	100%

Q22. How do you know about the success or status of your organization's data protection efforts? Please check all that apply.	Overall%
Written reports from the data protection leader	21%
Corporate communications about policy	18%
Regular presentation by the data protection leader or other person to senior management	15%
Corporate training programs about data protection (including privacy)	13%
Crisis and data breach incidents reported to management	11%
The results of data protection audits from external auditors	8%
The results of data protection audits from internal auditors	8%
Regular presentation by the data protection leader or other personal to the board	5%
No regular or formal communications (merely informal chatter)	1%
Total	100%

Q23. What organizational level best describes your current position?	Overall%
Chief executive	14%
Division or business unit president	34%
Vice president	22%
Senior or executive director	5%
Board Member	12%
Retired	12%
Other (please specify)	1%
Total	100%

Q24. In your organization, how many reporting layers or levels are there between the data protection leader and the CEO (or highest ranking executive)?	Overall%
I am the CEO	14%
One level (direct report)	46%
Two levels	30%
Three levels	10%
Four levels	0%
Five levels	0%
Total	100%

Q25a. What is your total business experience in years	29.28
Q25b. How many years have you held your current position	4.11

Q26. Gender	Overall%
Male	53%
Female	47%
Total	100%

Q27. What other job functions do you perform in your organization?	Overall%
No other function performed	60%
Corporate ethics	2%
Corporate law	20%
Corporate marketing and CRM	1%
Consulting	1%
General administration	1%
General management	12%
Governmental relations	0%
Human resources	1%
Information security	0%
IT operations	0%
Internal audit	0%
Physical security	0%
Public relations	0%
Research	0%
Regulatory compliance	1%
Records management	0%
Software development	0%
Total	100%

Q28. What is the industry or business group that best defines your organization? If your organization contains multiple industry sectors or sub-checks, please check all that apply (or write-in the space for other).	Overall%
Financial services	17%
Technology & software	11%
Retailing	10%
Manufacturing	9%
Hospitality & leisure	8%
Healthcare	7%
Telecom, cable & wireless	6%
Services	6%
Consumer products	5%
Professional services	5%
Education	4%
Pharmaceuticals	4%
Energy	3%
Transportation	3%
Professional services	2%
Internet services	1%
Total	100%

Q29. Is your organization subject to any of the following data protection or privacy regulatory requirements? Please check all that apply.	Overall%
HIPAA	8%
Sarbanes Oxley	51%
PCI	46%
Federal Privacy Act	2%
Basel II	12%
European Union Data Protection Directive	22%
Gramm-Leach-Bliley (GLBA)	10%
Data breach notification laws (various states)	6%
FACTA	4%
Total	163%

Q30 Your company has employees located in (check all that apply):	Overall%
United States	100%
Canada	61%
Europe	63%
Asia-Pacific	57%
Latin America (including Mexico)	42%
Total	323%

Q31. What is the worldwide headcount of your organization?	Overall%
Less than 500 people	22%
500 to 1,000 people	17%
1,001 to 5,000 people	20%
5,001 to 25,000 people	34%
25,001 to 75,000 people	6%
More than 75,000 people	1%
Total	100%

Q32. What is the geographical location of your data protection efforts?	Overall%
United States	99%
Canada	61%
Europe	63%
Asia-Pacific	57%
Latin America (including Mexico)	42%
Total	322%

Q33 Is your company publicly traded?	Overall%
Yes, NYSE	24%
Yes, NASDAQ	20%
Yes, overseas exchange	5%
Yes, other minor exchange	8%
No	43%
Total	100%

Q34. What is the jurisdiction of your data protection efforts (check all that apply):	Overall%
United States	100%
Canada	59%
Europe	65%
Asia-Pacific	57%
Latin America (including Mexico)	42%
Total	323%

Q. 35 2008 Total Revenues	Overall%
Less than \$100 million	21%
\$101 to \$500 million	17%
\$501 million to \$1 billion	18%
\$1.1 billion to 10 billion	35%
\$11 billion to 20 billion	6%
More than 20 billion	3%
Total	100%