



# **Business Case for Data Protection**

A Study of CEOs and other C-level Executives in the United Kingdom

---

**Sponsored by**

**IBM**

Independently conducted by Ponemon Institute LLC

Publication Date: March 2010

# **Business Case for Data Protection: A Study of CEOs and other C-Level Executives in the United Kingdom**

By Dr. Larry Ponemon, March 2010

## **I. Executive Summary**

We are pleased to present *The Business Case for Data Protection: A Study of CEOs and other C-Level Executives in the United Kingdom*. This research was independently conducted by Ponemon Institute and sponsored by IBM. The presented research follows a similar study of CEOs and C-Level executives conducted in the United States. We believe these are the first studies to determine what senior executives think about the value proposition of privacy and data protection efforts within their organisations.

The research focused on how aware CEOs and other senior executives are about their organisation's data protection efforts, what they believe is the economic justification for investment in a data protection program, how data protection programs support organisational 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 times of shrinking budgets, it is important for those individuals charged with managing a data protection program to understand how key decision makers in organisations perceive the importance of safeguarding sensitive and confidential information.

This research of 115 C-level business executives located in the UK included 26 chief executives or managing directors. By design, none of these individuals were practitioners in the privacy, data protection or information security fields. In our study, we learned that C-level executives believe good data protection practices can support important organisational 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 organisational goals. For example, CEOs are more likely to believe that data protection increases corporate value. They also are more likely to believe their organisations 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 organisation, perceived value of a data protection program, and perception gaps between CEOs and other C-level executives.

### **1. C-level executives in the UK are concerned about threats to sensitive and confidential consumer and business customer data.**

Seventy-seven percent of C-level executives in our study report that their organisation has experienced a data breach and many are not confident that they can prevent future breaches. Further, all respondents report that they have had their data attacked in the last 12 months. In general, CEOs are more confident than others that their organisations are able to prevent data breaches.

Non-financial business confidential information, business customer information and customer or consumer information appear to be the most difficult to secure. Intellectual property information

seems to be easier to safeguard against loss or theft. In the last 12 months, all of the respondents acknowledge that their organisations' information assets have been attacked at least once.

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

In the study, 75 percent 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. This is considered by 69 percent to be a full time position. It is interesting to note that the organisations really don't hold these individuals accountable. Specifically, the overwhelming majority (82 percent) do not believe a failure to stop a data breach under their watch would cause them to lose their position.

The data protection function is located in corporate law (28 percent), followed by corporate ethics (18 percent) or information security (16 percent). The organisational level that best describes the position is director or manager.

## **3. Data protection programs help organisations achieve their business goals.**

C-level executives believe data protection programs should have the following impact on an organisation: increasing or maintaining marketplace reputation and brand (51 percent), ensuring regulatory and legal compliance (40 percent) and increasing customer trust and loyalty (30 percent). Decreasing employee turnover and safeguarding critical infrastructure are goals not considered dependent upon good data protection efforts.

When asked what are the most important activities for a data protection program, 76 percent believe it is reducing potential security flaws within business-critical applications, 71 percent say training of employees, temporary employees and contractors and 67 percent of respondents believe it is a data protection strategy.

In order to achieve organisational goals, it is important to collaborate with corporate IT followed by human resources and legal. Logistics is not considered an important function with which 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 £11 million is substantially higher than the extrapolated value of data protection spending of £1.9 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, decrease the risk of regulatory actions, and reduce the inefficient uses of data for operational purposes. Increasing employee trust is not considered as important a goal.

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 decrease in regulatory action from fines and lawsuits.

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

including the protection of intellectual properties; asset performance, including increasing the value of customer information and reputation management.

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

Twenty-six respondents (23 percent) in this study are CEOs. The remaining 89 respondents are C-level executives who report to their company’s CEO, such as chief operating officers, division presidents, general managers, chief information offices and other titles.

In general, CEO responses track closely to the overall sample. However, CEOs are more likely to see data protection as reducing potential security flaws within business-critical applications, developing a data protection strategy for the organisation and identifying and responding to data breach (loss or theft of personal information). 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 organisation	67%	89%
Training employees, temporary employees and contractors	71%	58%
Reducing potential security flaws within business-critical applications	76%	94%
Establishing and managing a crisis management, disaster management, and business continuity plan	61%	76%
Identifying and responding to data breach (loss or theft of personal information)	64%	87%
Conducting due diligence on transactions and relationships that involve the sharing of personal and confidential information	71%	55%
Protecting personal or confidential information shared with vendors, business partners and other third parties	41%	65%
Ensuring record retention requirements are met	57%	46%
Monitoring new legal and regulatory requirements	45%	28%
Preventing cyber and malicious insider attacks	60%	47%
Conducting data vulnerability or privacy impact assessments for new products	35%	48%
Auditing business processes for compliance with data protection and privacy policies	38%	48%
Mapping data flows and conducting a data inventory	50%	41%
Implementing customer access and redress programs	45%	48%
Deploying enabling data protection technologies	44%	62%
Creating policies and SOPs for the handling and use of personal information	40%	63%
Complying with employee data protection and privacy laws	36%	30%
Analyzing data collection, use and sharing	36%	19%
Complying with marketing data protection and privacy laws	30%	57%
Implementing employee access and redress programs	34%	23%
Responding to e-discovery requests	45%	42%
Performing background checks on employees, temporary employees and contractors	29%	21%
Average	49%	52%

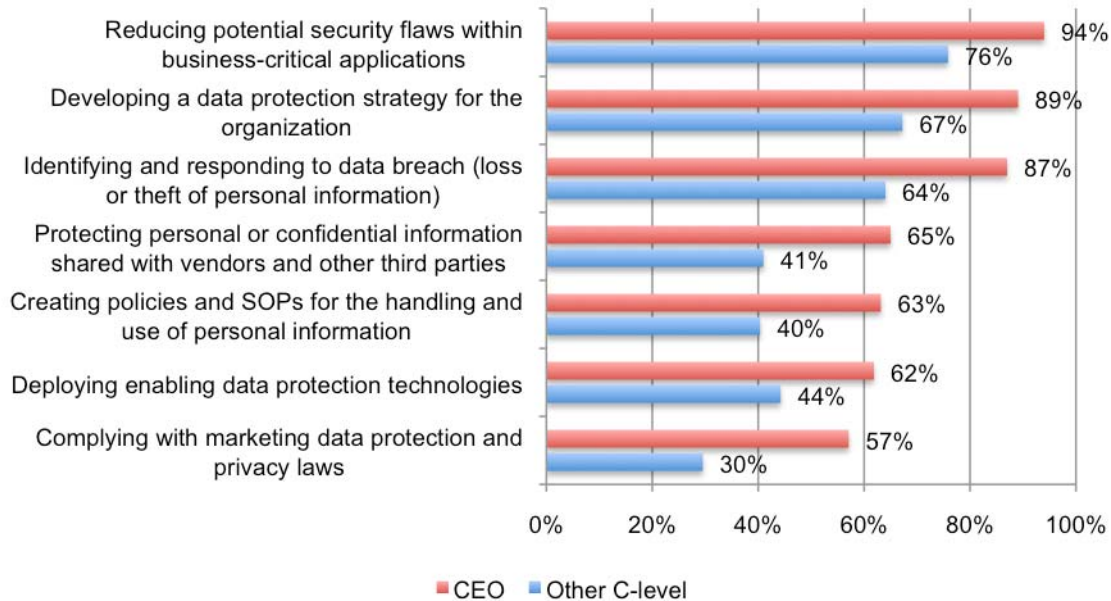
Bar Chart 1 reports those priorities with the largest differences or gaps between CEOs and other C-level executives. As can be seen, CEOs perceive complying with marketing data protection and privacy laws, protecting personal or confidential information shared with vendors, business

partners and other third parties, identifying and responding to data breach and creating policies and SOPs for the handling and use of personal information as more important than other C-level executives.

**Bar Chart 1**

**Most salient differences between CEOs and other C-level executives**

Each bar represents the combined percentage of very important and important response



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 (49 percent versus 33 percent).
- CEOs are more likely to believe marketplace reputation and customer trust are dependent upon good data protection efforts than other C-level executives. CEOs are also more likely to believe that data protection programs improve information flows about people (such as consumers, customers, business partners and other stakeholders) and reduce the risk of data loss or theft.
- In contrast, CEOs are less likely than other C-level executives to believe that data protection programs decrease risk of regulatory action, fines and lawsuits and improve formal governance of data protection policies.

**II. Analysis of key findings**

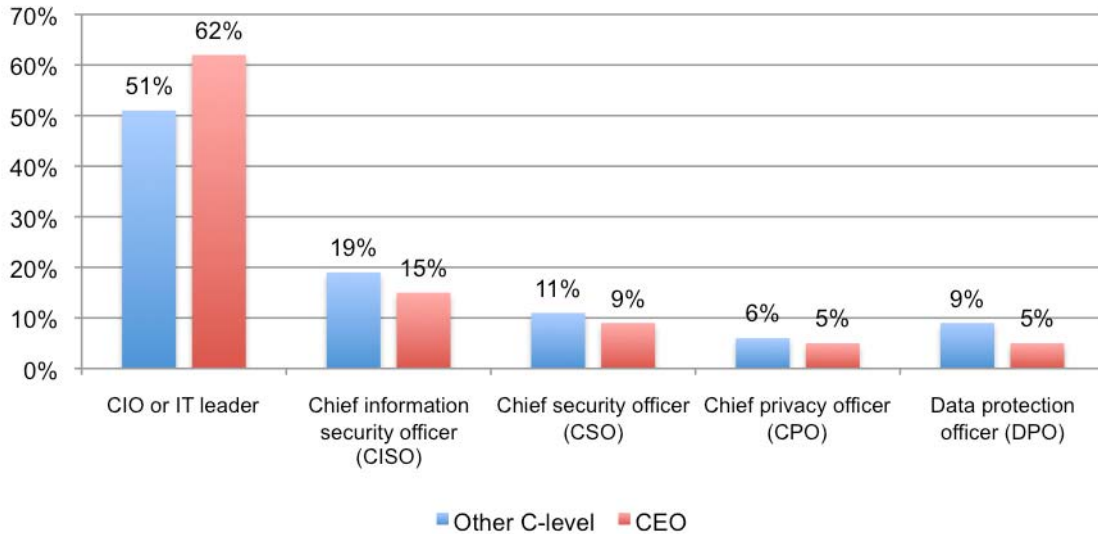
Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as the Appendix to this paper.

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

A large majority of respondents (75%) report that there is one person responsible for the overall data protection effort within their organisations.

As shown in Bar Chart 2, 62 percent of CEOs believe their company’s chief information officer (CIO) is accountable for data protection. In contrast, only 51 percent 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 security officer (CSO) are next in line in terms of individual responsibility or accountability for protecting information assets.

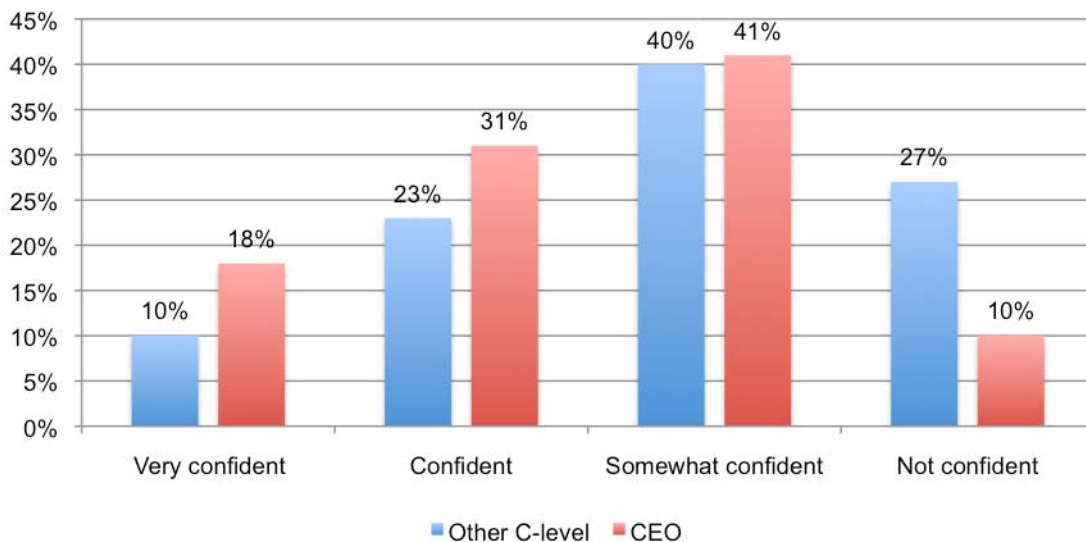
**Bar Chart 2**  
**The most responsible individuals for data protection in the organisation**  
 Each bar shows the percentage frequency for CEOs and C-level respondents



**Executives are concerned about their organisations’ ability to avoid a data breach.**

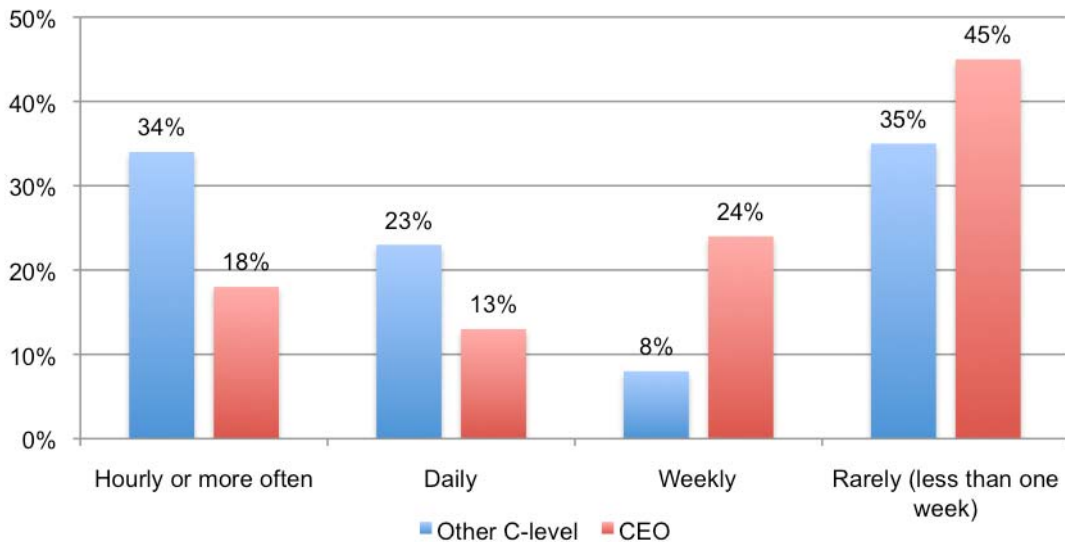
Bar Chart 3 shows that 33 percent of C-level respondents say they are very confident or confident their organisations will not suffer a data breach within the next 12 months. Forty-nine percent of CEOs say that are very confident or confident. More than 27 percent of C-level executives say they are not confident that their organisations will avoid a data breach, while only 10 percent of CEOs feel this way.

**Bar Chart 3**  
**Confidence that the organisation will not suffer a data breach within the next year**



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. For example, only 18 percent of CEOs believe attacks on data happen hourly or even more frequently, while 34 percent of other C-level executives believe this to be true.

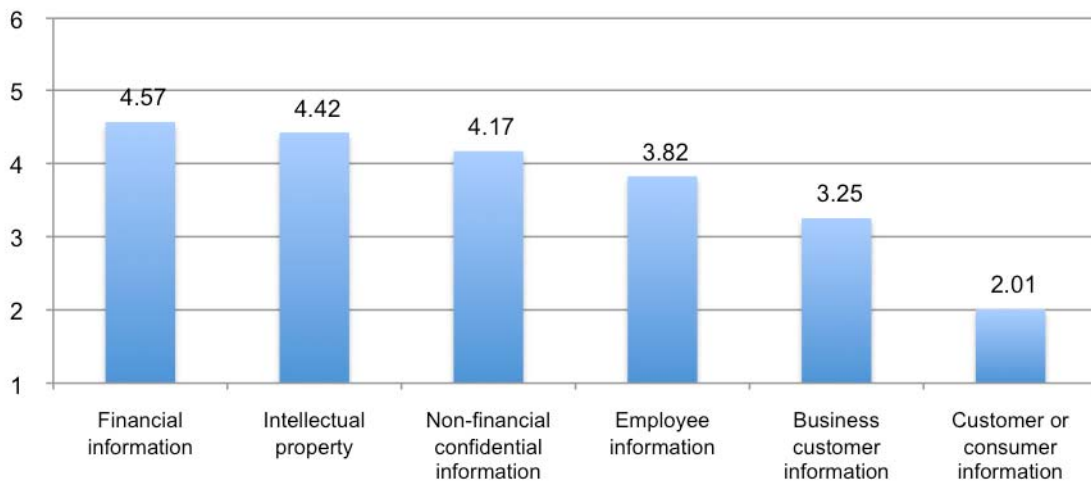
**Bar Chart 4**  
**The perceived frequency of attacks on data in the past year**



Bar Chart 5 reports the priority ranking by all executives, where a high rank defines a higher priority. Clearly, the top two most critical data types are financial information and intellectual property. This is followed by non-financial business confidential information. Of least importance to an organisation’s operations appears to be data about customer or consumer information and business customer information.

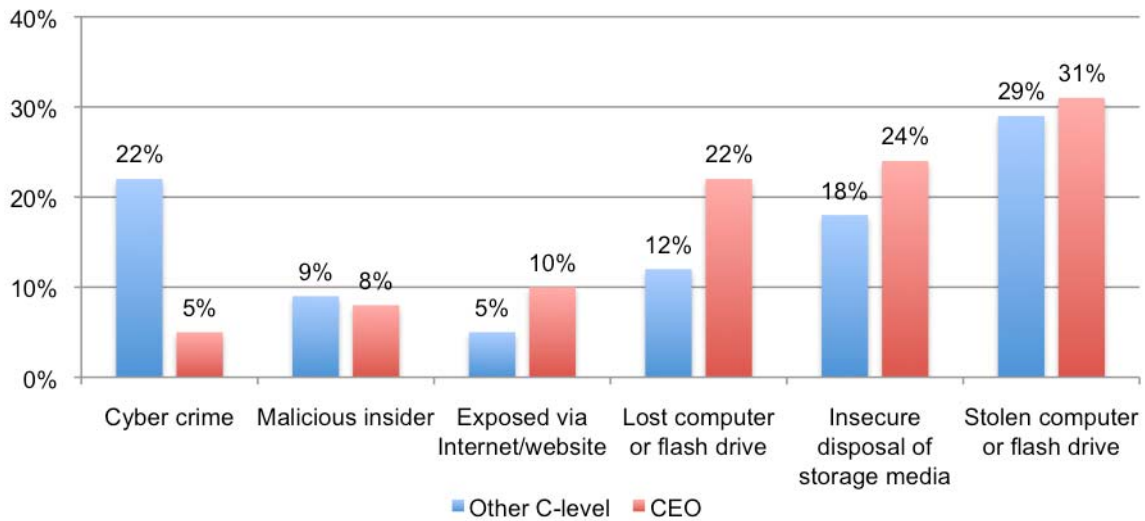
**Bar Chart 5**  
**Priority ranking of six data types believed to be most critical to business operations**

Maximum rank = 6 and minimum rank = 1



According to Bar Chart 6, both CEOs and other C-level executives believe the source of greatest risk to sensitive and confidential data comes from stolen computer/flash drives followed by the insecure disposal of storage media. The most salient difference between CEOs and other C-level executives concerns cyber crime – wherein CEOs are less likely to perceive this as a significant source of risk to sensitive data.

**Bar Chart 6**  
Sources of greatest risk to sensitive data



As shown in Bar Chart 7, maintaining marketplace reputation and brand, increasing customer trust and loyalty, and ensuring regulatory and legal compliance are the three most important organisational goals that depend upon effective data protection for both CEOs and C-level executives. Interestingly, safeguarding critical infrastructure and ensuring partner or vendor compliance is viewed as much less important.

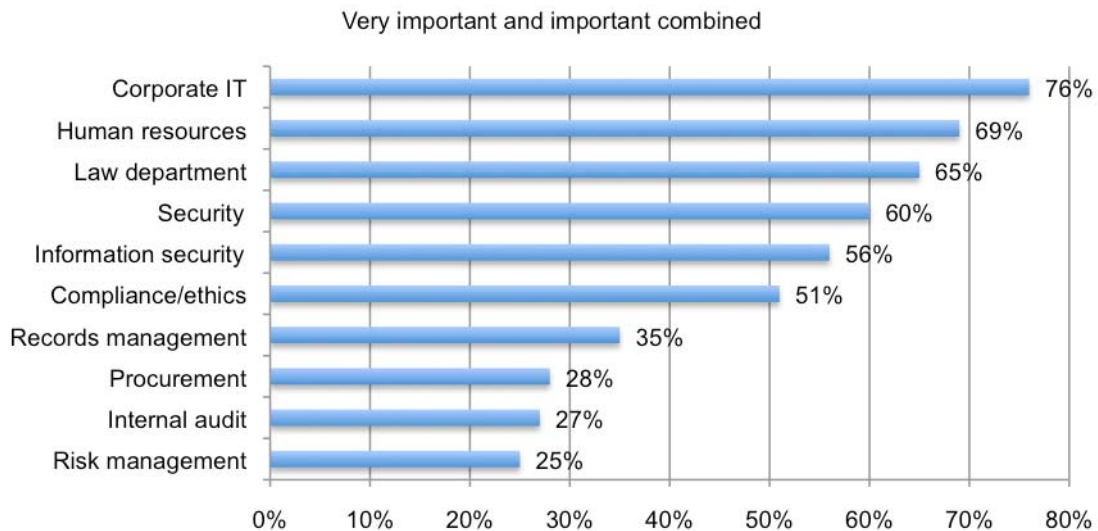
**Bar Chart 7**  
Organisational goals that depend upon data protection



**Collaboration with corporate IT, human resources, and legal is critical to achieving organisational data protection goals.**

To achieve organisational goals such as marketplace reputation, customer loyalty and compliance, Bar Chart 8 shows that more than 76 percent of all respondents believe it is either very important or important to collaborate with the company's IT department. The next critical collaborations are human resources (69 percent) legal department (65 percent) and security (60 percent).

Bar Chart 8  
What business functions need to collaborate to achieve data protection goals



**Reducing potential security flaws within business-critical applications and training employees are considered the most important activities of a data protection program.**

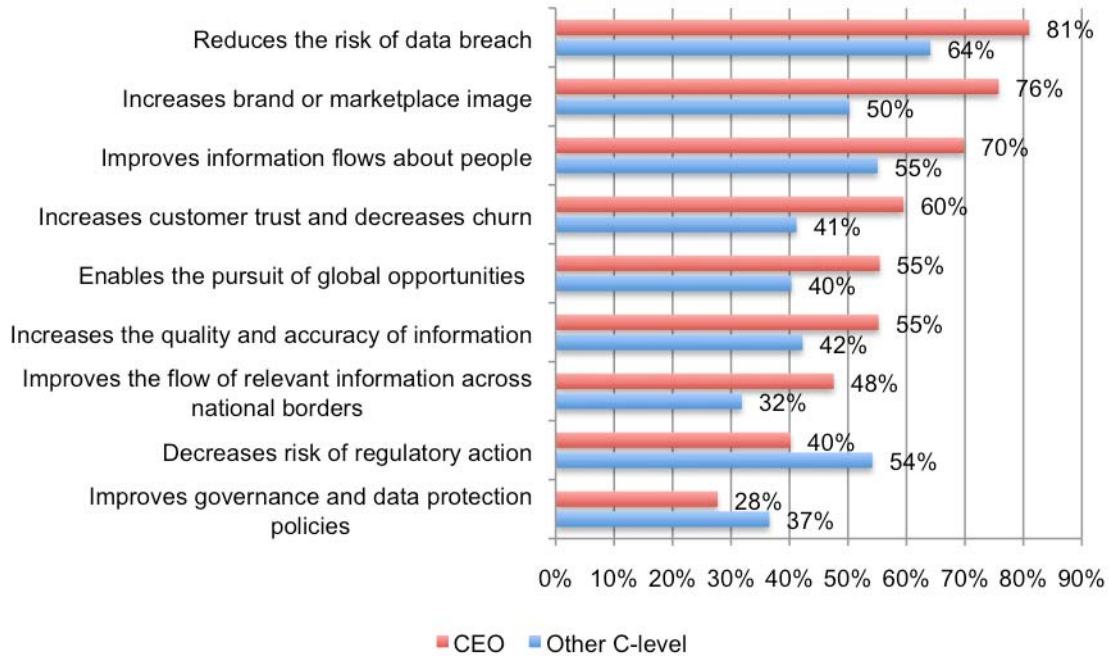
The most important and least important activities for a data protection program are shown in Table 1 (see page 4). In addition to the activities described above, developing a data protection strategy for the organisation and identifying and responding to data breaches are important activities for organisational data protection efforts. The least important activities are complying with marketing data protection and privacy laws and performing background checks on employees, temporary employees and contractors.

**Investing in data protection is important to reducing the risk of a data breach.**

When asked whether a coherent and comprehensive enterprise data protection program increases their organisation's value, 81 percent of CEOs and 64 percent of other C-level executives say it reduces or mitigates the risk of data loss or theft.

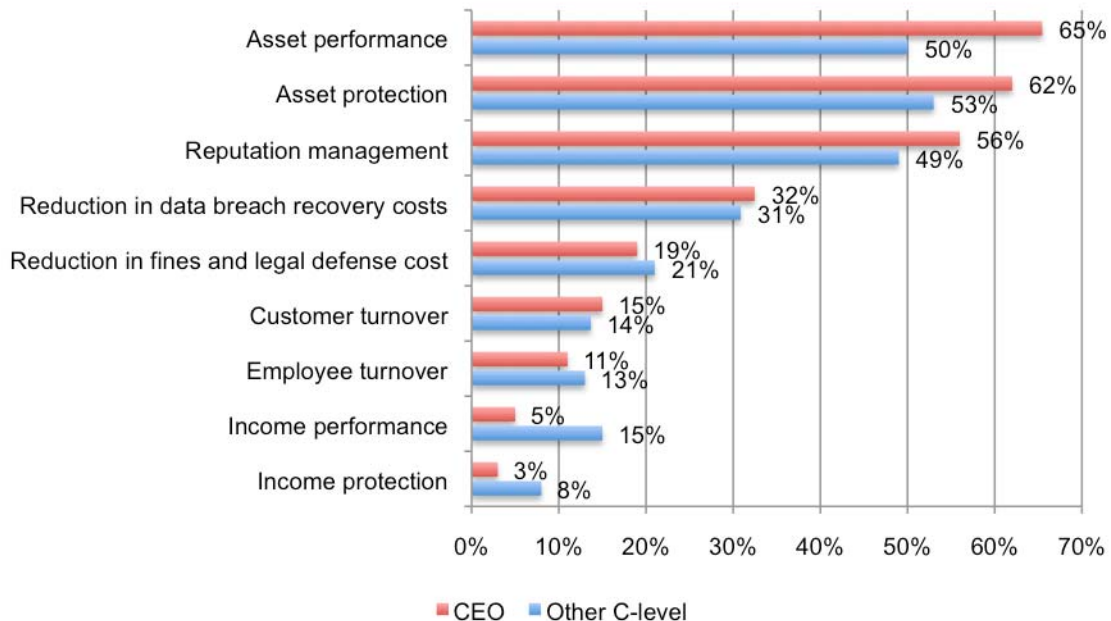
Also shown in Bar Chart 9, 76 percent of CEOs and 50 percent of other C-level executives believe that it increases brand or marketplace image followed by 70 percent of CEOs and 55 percent of other C-level executives who believe the value is improving information flows about people such as consumers, customers, business partners and other stakeholders.

**Bar Chart 9**  
**How an enterprise data protection program increases an organisation's value**



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

**Bar Chart 10**  
**Measures that should be used to evaluate the effectiveness of data protection initiatives**

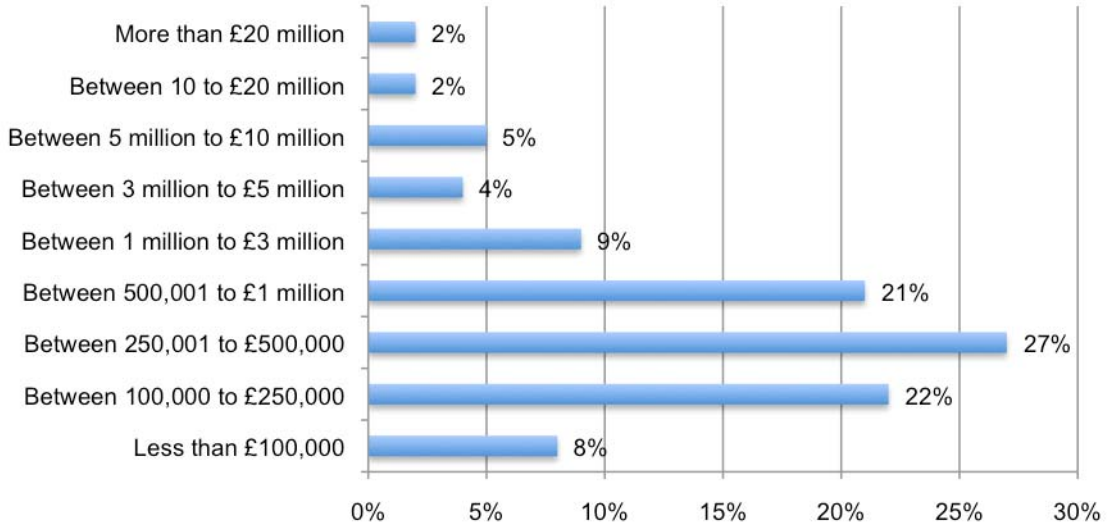


Executives in our study believe that asset protection including the protection of intellectual properties, asset performance such as increasing the value of customer information and reputation management measures *should be* used to measure the effectiveness of data protection efforts. Not shown in the above bar chart, the most commonly used measures used to

evaluate data protection program effectiveness pertain to the reduction of data breach or minimization of legal costs.

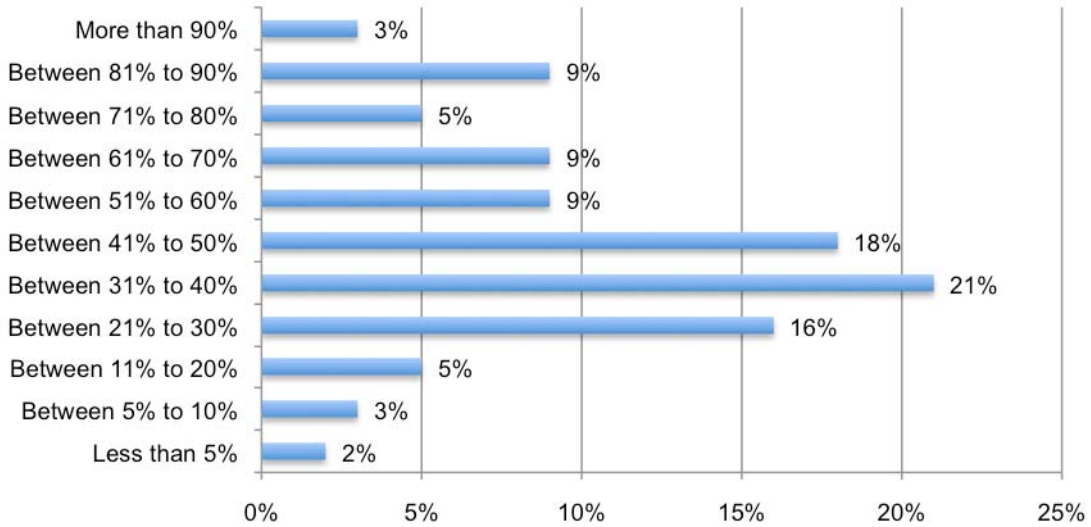
Bar Chart 11 shows the distribution frequency of annual budget dedicated to data protection. The median extrapolated value from this distribution is £1.9 million.

**Bar Chart 11**  
**The approximate annual budget for enterprise data protection**



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 approximately 45 percent of the overall data protection budget.

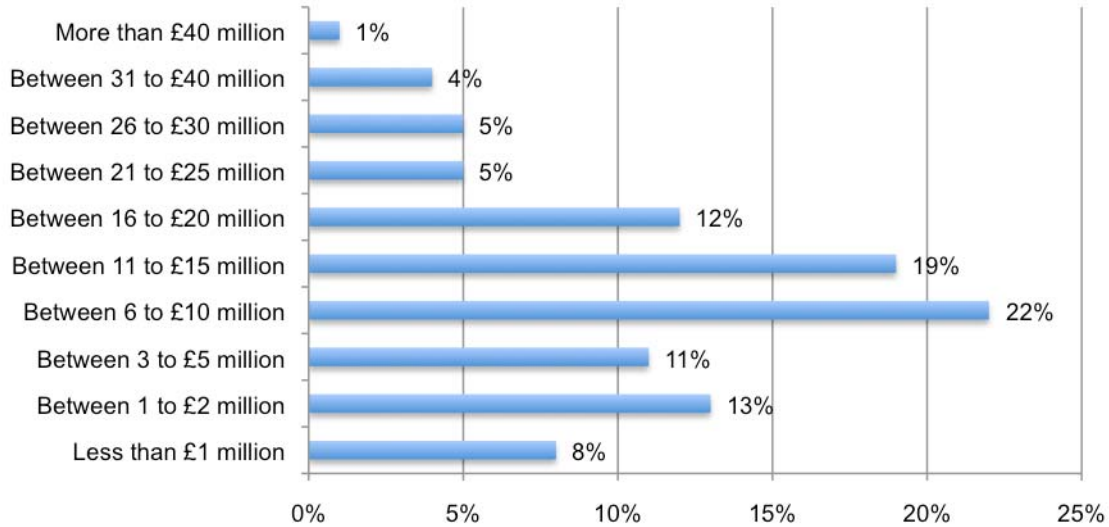
**Bar Chart 12**  
**Enterprise data protection budget earmarked for enabling technology**



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

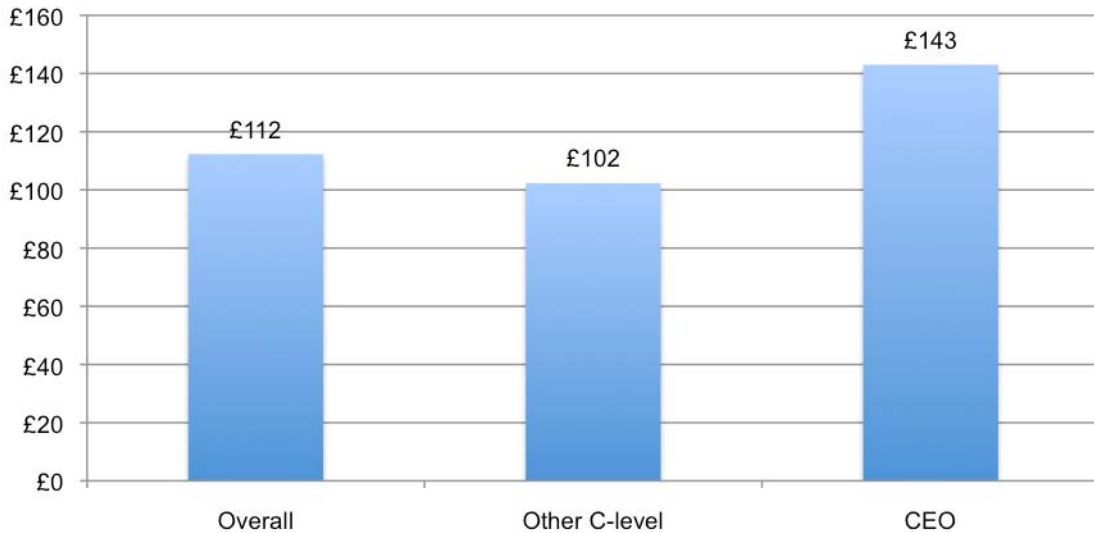
£11 million, which is substantially higher than the value of data protection spending of £1.9 million mentioned above. This suggests a healthy ROI for data protection programs.

**Bar Chart 13**  
**Cost savings or revenue improvements resulting from data protection efforts**



Executives in this study estimated the average data breach cost per compromised record is £112. CEOs estimated it to be £143 per compromised record.<sup>1</sup>

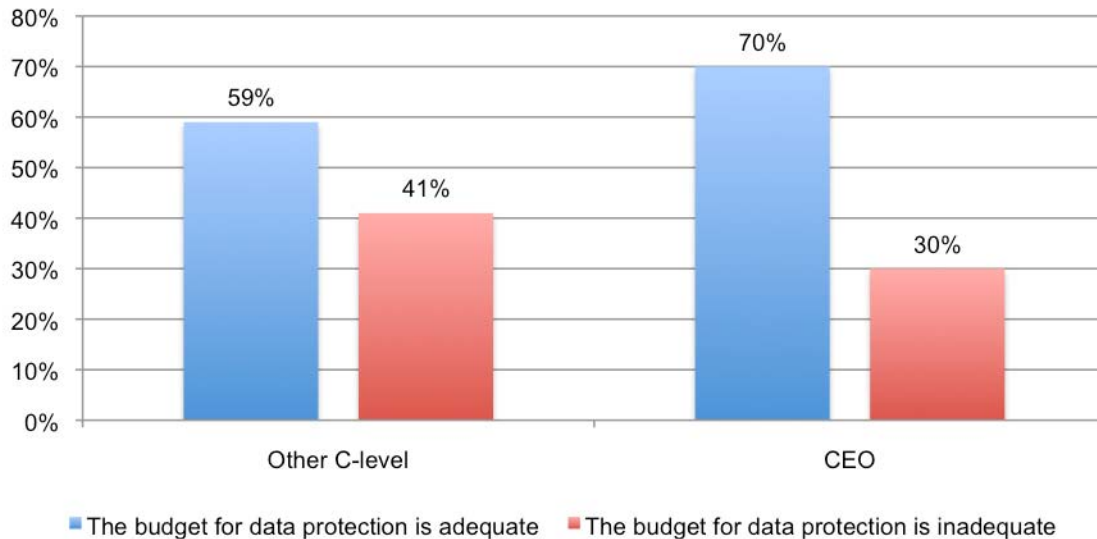
**Bar Chart 14**  
**Estimated data breach cost on a per capita (compromised record) basis**



<sup>1</sup> See Ponemon Institute's [Annual Cost of a Data Breach: UK Study](#) published in January 2009, wherein the extrapolated cost of data breach on a per capita basis is £60. This finding suggests C-level executives in the UK attach a much higher cost to a data breach involving the loss or theft of confidential information than warranted by the empirical data.

Bar Chart 15 reports how C-level executives and CEOs perceive the adequacy of organisational resources spent on data protection. More than 70 percent of CEOs believe spending on data protection initiatives is adequate. Only 59 percent of other C-level executives believe spending on data protection is adequate to meet organisational goals.

**Bar Chart 15**  
**Perceptions about the adequacy of the organisation's data protection budget**



### III. Differences between UK and US C-level executives

In July 2009, Ponemon Institute released the *Business Case for Data Protection Study* of US C-level executives. In many areas, there are similarities in perceptions held about the value proposition of corporate data protection efforts within their organisations.

The most salient similarities and differences between US and UK C-level executives are as follows:

- Responsibility for the overall data protection effort within the organisation rests with one person who is most likely to be the chief information officer (CIO) or IT leader or the chief information security officer (CISO), according to the majority of both US and UK respondents. However, C-level executives in the US also believe the chief privacy officer (CPO) is also one of the top positions responsible for data protection. This difference could be attributed to the very few CPOs in UK organisations. Both groups agree the organisation level that best describes the data protection leader is director or manager.
- The most critical data to safeguard, according to US C-level executives, includes business customer information, intellectual property and customer or consumer information. Among UK C-level executives, the most critical data is financial business confidential information, intellectual property and non-financial business confidential information.
- CEOs in both the US and UK are more confident than other C-level executives that their organisations will not suffer a data breach in the next 12 months. They are also less likely to be aware of the extent of attacks on sensitive data.

- The greatest risk to sensitive data is stolen computers/flash drives and tape, according to senior executives in both countries. US senior executives believe lost computer/flash drive and insecure disposal of data storage also are significant risks. UK senior executives rank hackers/cyber criminals and insecure disposal of data storage as serious risks.
- US C-level executives are more likely to believe that protecting personal or confidential information shared with vendors, business partners and other third parties and conducting data vulnerability or privacy impact assessments for new products are important data protection activities. UK C-level executives are more likely to see responding to e-discovery requests and performing background checks on employees, temporary employees and contractors as important activities.
- Both US and UK CEOs believe the following objective measures should be used to justify spending on data protection: asset performance, such as increasing the value of customer information; asset protection, including the protection of intellectual properties; and reputation management.

#### IV: Methods

This study was conducted over a four-month period concluding in January 2010. CEOs, managing directors and other senior executives were recruited to participate in this study.<sup>2</sup> The final survey sample consisted of 115 executives who work various industry sectors. The description of the sample according to the respondent's title is provided in Table 2.

Table 2. Description of participating executives	Freq.	Pct%
Chief executive officer or managing director	26	23%
Chief operations officer	18	16%
Division president, general manager, executive vice president	41	36%
Chief information officer	18	16%
Other C-level executives	12	10%
Total	115	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 organisation have a data protection and privacy program or initiative?" were included in this analysis.

Table 3a reports the organisations' worldwide headcount showing that 29% have more than 5,000 employees Table 3b reports the organisation's gross revenues or sales showing 23% have more that \$1 billion in total revenues in fiscal year 2008.

Table 3a. Worldwide headcount	Pct%
Less than 500 people	25%
500 to 1,000 people	21%
1,001 to 5,000 people	25%
5,001 to 25,000 people	22%
25,001 to 75,000 people	6%
More than 75,000 people	1%
Total	100%

Table 3b. Total revenues	Pct%
Less than £100 million	27%
101 to £500 million	30%
501 million to £1 billion	20%
1.1 billion to £10 billion	16%
11 billion to £20 billion	5%
More than 20 billion	2%
Total	100%

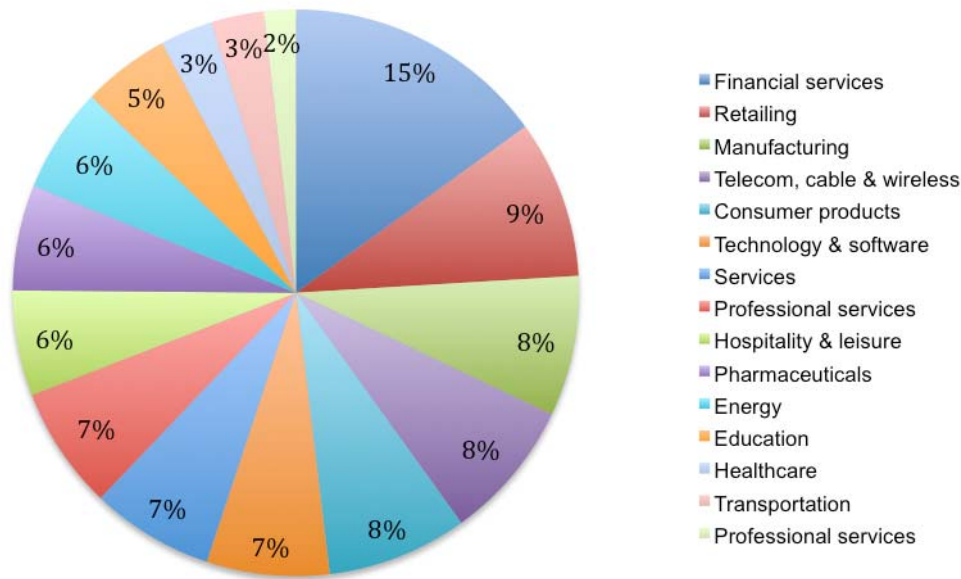
<sup>2</sup> By design, C-level respondents who were not CEOs were no more than two steps away from the CEO or Chairman level in their organisations.

Table 4a reports the frequency of companies that are publicly traded on FTSE, London or other major exchanges. Table 4b reports the geographic footprint of participating organisations.

Table 4a. Company exchange	Pct%
FTSE	16%
London	25%
NYSE	5%
NASDAQ	6%
Other overseas exchange	11%
No	37%

Table 4b. Geographic footprint	Pct%
United States	68%
Canada	59%
Europe	100%
Asia-Pacific	46%
Latin America (including Mexico)	23%
Middle East	29%

Pie Chart 1 reports the sample distribution by industry classification. As shown, participating companies include 15 industry sectors. The largest segments include financial services (15%), retail (9%), and manufacturing (8%).



## 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 organisation 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 organisations.

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 115 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, USA  
1.800.887.3118  
[research@ponemon.org](mailto: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 organisations.

As a member of the **Council of American Survey Research Organisations (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.

### Part I: Awareness about your organisation's data protection efforts.

Q1. Does your organisation have a data protection and privacy program or initiative?	Pct%
Yes	97%
No (Stop)	3%
Not sure (Stop)	0%
Total	100%

Q2a. Is there one person responsible for the overall data protection effort within your enterprise?	Pct%
Yes	75%
No	25%
Total	100%

Q2b. Who is your organisation's data protection leader? That is; who is responsible for the overall data protection effort within your enterprise?	Pct%
CIO or IT leader	51%
Chief information security officer (CISO)	19%
Chief privacy officer (CPO)	6%
Chief security officer (CSO)	11%
Data protection officer (DPO)	9%
Other (please specify)	4%
Total	100%

Q2c. What is the organisational level that best describes the position level of your organisation's data protection leader?	Pct%
EVP or SVP	0%
VP	6%
Executive Director	5%
Director	36%
Manager	42%
Supervisor	11%
Other (please specify)	0%
Total	100%

Q2d. Is this a full time position?	Pct%
Yes	69%
No	31%
Total	100%

Q2e. Who else in your organisation is responsible for data protection? Please check the other executives within your organisation who are responsible for data protection.	Pct%
General Counsel	35%
Cross-functional committee	68%
Chief Information Officer	71%
Compliance/Ethics Officer	54%
Human Resources VP	40%
Chief Marketing Officer	10%
Chief Risk Officer	19%
Chief Security Officer	18%
Chief Financial Officer (Finance Director)	26%
Not sure	2%
Total	343%

Q3. What types of data are most critical to your organisation's operations? Please rank order the following list from 1 = the most critical information to 6 = your least critical information.	Average Rank
Customer or consumer information	3.99
Business customer information	2.75
Employee information	2.18
Financial, business confidential information	1.43
Non-financial, business confidential information	1.83
Intellectual property	1.58

Q4. What types of data do you believe are most difficult to secure within your organisation? Please check the top two choices.	Pct%
Customer or consumer information	42%
Business customer information	46%
Employee information	28%
Financial, business confidential information	24%
Non-financial, business confidential information	50%
Intellectual property	8%
Total	198%

Q5a. Has your company ever experienced a data breach?	Pct%
Yes	77%
No	23%
Total	100%

Q5b. How confident are you that your organisation will not suffer a data breach in the next 12 months?	Pct%
Very confident	10%
Confident	23%
Somewhat confident	40%
Not confident	27%
Total	100%

Q5c. If your organisation experienced a serious data breach, how would it affect your job security?	Pct%
I would certainly lose my job	0%
I would likely lose my job	3%
I might lose my job	15%
I would not lose my job	82%
Total	100%

Q6. In the last 12 months, how often has your organisation's data been attacked?	Pct%
Hourly or more often	34%
Daily	23%
Weekly	8%
Rarely (less than one week)	35%
Never	0%
Total	100%

Q7. What is the source of greatest risk to your sensitive data? Please select only one response.	Pct%
Stolen computer/flash drive/tape	29%
Lost computer/flash drive/tape	12%
Incorrect disposal of hard/soft files	18%
Hacker/cyber crime	22%
Exposed via Internet/website	5%
Malicious insider	9%
Exposed via email	5%
Skimming	0%
Exposed via mailing	0%
Total	100%

Q8. Where within your organisation is the data protection function located? Please select only one response.	Pct%
Legal	28%
Regulatory compliance	8%
Privacy office	5%
Information security department or office	16%
Corporate IT	8%
Public relations	0%
Risk management	5%
Government affairs	0%
Corporate ethics	18%
Human resources	7%
Records management	5%
Marketing	0%
Total	100%

Q9. Please select from the following list of organisational goals that are dependent upon good data protection efforts? Please select only two choices.	Pct%
Ensuring regulatory and legal compliance	40%
Increasing or maintaining marketplace reputation and brand	51%
Increasing customer trust and loyalty	30%
Ensuring business partner or vendor compliance	15%
Safeguarding critical infrastructure	9%
Enhancing the value of information assets	19%
Decreasing employee turnover	10%
Total	174%

Q10. Based on the organisational goals listed above, how important is collaboration between data protection and other business functions within your organisation? 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.	Pct%
Legal department (OGC)	65%
Information security	56%
Privacy office	16%
Corporate IT	76%
Risk management	25%
Records management	35%
Security	60%
Human resources	69%
Compliance/ethics	51%
Public relations	12%
Internal audit	27%
Government or public affairs	12%
Marketing & communications	21%
Procurement	28%
Finance & accounting	12%
Logistics	7%
Sales	15%
Average	35%

Q11. Following are typical business activities for organisational 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.	Pct%
Developing a data protection strategy for the organisation	67%
Training employees, temporary employees and contractors	71%
Reducing potential security flaws within business-critical applications	76%
Establishing and managing a crisis management, disaster management, and business continuity plan	61%
Identifying and responding to data breach (loss or theft of personal information)	64%
Conducting due diligence on transactions and relationships that involve the sharing of personal and confidential information	71%
Protecting personal or confidential information shared with vendors, business partners and other third parties	41%
Ensuring record retention requirements are met	57%
Monitoring new legal and regulatory requirements	45%
Preventing cyber and malicious insider attacks	60%
Conducting data vulnerability or privacy impact assessments for new products	35%
Auditing business processes for compliance with data protection and privacy policies	38%
Mapping data flows and conducting a data inventory	50%
Implementing customer access and redress programs	45%
Deploying enabling data protection technologies	44%
Creating policies and SOPs for the handling and use of personal information	40%
Complying with employee data protection and privacy laws	36%
Analyzing data collection, use and sharing	36%
Complying with marketing data protection and privacy laws	30%
Implementing employee access and redress programs	34%
Responding to e-discovery requests	45%
Performing background checks on employees, temporary employees and contractors	29%
Average	49%

**Part II: About your organisation's data protection efforts.**

Q12. Does a coherent and comprehensive enterprise data protection program increase your organisation'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.	Pct%
Improves information flows about people such as consumers, customers, business partners and other stakeholders.	55%
Increases brand or marketplace image.	50%
Decreases risk of regulatory action, fines and lawsuits.	54%
Reduces operational inefficiencies by creating more efficient uses of data.	54%
Reduces or mitigates the risk of data loss or theft (i.e., data breach).	64%
Increases customer trust and decreases customer churn.	41%
Improves formal governance of data protection policies	37%
Improves the flow of relevant information about customers and employees across national borders.	32%
Increases the quality and accuracy of information	42%
Improves IT processes because of a better data governance structure.	42%
Increases our suppliers' accountability to our data protection and privacy policies.	38%
Enables the pursuit of new global business opportunities	40%
Reduces the cost of due diligence in mergers & acquisitions	38%
Reduces potential risks under e-discovery laws.	40%
Increases employee trust and decreases employee churn.	19%
Average	42%

Q13. Please rate each value proposition based on importance to your organisation using the following scale: 1 = very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Pct%
Reduces operational inefficiencies by creating more efficient uses of data.	47%
Improves IT processes because of a better data governance structure.	33%
Improves information flows about people such as targeted consumers, customers, business partners and other stakeholders.	66%
Increases brand or marketplace image.	62%
Improves formal governance of data protection policies	46%
Decreases risk of regulatory action, fines and lawsuits.	54%
Increases our suppliers' accountability to our data protection and privacy policies.	35%
Increases customer trust and decreases customer churn.	52%
Increases employee trust and decreases employee churn.	17%
Reduces potential risks under e-discovery laws.	32%
Reduces the cost of due diligence in mergers & acquisitions	30%
Improves the flow of relevant information about customers and employees across national borders.	48%
Enables the pursuit of new global business opportunities	39%
Increases the quality and accuracy of information	39%
Reduces or mitigates the risk of data loss or theft (i.e., data breach).	46%
Average	43%

**Part III: Measures for success**

Q14. What objective measures should be used to justify spending on data protection within your organisation? Please choose all that apply.	Pct%
Asset performance such as increasing the value of customer information	50%
Asset protection including the protection of intellectual properties	53%
Reputation management	49%
Reduction in fines and legal defense cost	21%
Reduction in data breach recovery costs	31%
Customer turnover	14%
Income performance, such as a more effective marketing campaign	15%
Income protection	8%
Stock value	10%
Employee turnover	13%
Total	263%

Q15 is a reliability check and thus omitted from analysis

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 organisation's data protection efforts today:	US
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 organisation's budget for data protection next year (12 months from now)?	Pct%
Less than £100,000	8%
Between 100,000 to £250,000	22%
Between 250,001 to £500,000	27%
Between 500,001 to £1 million	21%
Between 1 million to £3 million	9%
Between 3 million to £5 million	4%
Between 5 million to £10 million	5%
Between 10 to £20 million	2%
Between 20 to £40 million	2%
Between 40 to £60 million	0%
More than£ £60 million	0%
Total	100%

Q17b. Is the budget for data protection adequate?	Pct%
Yes	59%
No	41%
Total	100%

Q17c. If no, how much would you like to see it increased?	Pct%
More than 50%	6%
Between 40 and 50%	13%
Between 30 and 40%	16%
Between 20 and 30%	19%
Between 10 and 20%	19%
Less than 10%	27%
Total	100%

Q18a. Is spending on compliance initiatives diverting resources from other security initiatives?	Pct%
Yes	28%
No	52%
Unsure	20%
Total	100%

Q18b. If yes or unsure, is this causing your data to be less secure?	Pct%
Yes	65%
No	35%
Not applicable	0%
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?	Pct%
Less than 5%	2%
Between 5% to 10%	3%
Between 10% to 20%	5%
Between 20% to 30%	16%
Between 30% to 40%	21%
Between 40% to 50%	18%
Between 50% to 60%	9%
Between 60% to 70%	9%
Between 70% to 80%	5%
Between 80% to 90%	9%
More than 90%	3%
Total	100%

Q20. Approximately (gut feel is okay), what is the dollar range that best describes your organisation's cost savings or revenue improvements as a result of data protection efforts in 2009?	Pct%
Less than £1 million	8%
Between 1 to £2 million	13%
Between 2 to £5 million	11%
Between 5 to £10 million	22%
Between 10 to £15 million	19%
Between 15 to £20 million	12%
Between 20 to £25 million	5%
Between 25 to £30 million	5%
Between 35 to £40 million	4%
Between 45 to £50 million	1%
Between 55 to £60 million	0%
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?	Pct%
Less than £50	20%
Between 50 to £100	39%
Between 101 to £150	18%
Between 151 to £200	11%
Between 201 to £250	5%
Between 251 to £300	5%
Between 301 to £350	2%
Between 351 to £400	0%
Between 401 to £450	0%
Between 451 to £500	0%
Between 501 to £1,000	0%
More than £1,000	0%
Total	100%

Q22. How do you know about the success or status of your organisation's data protection efforts? Please check all that apply.	Pct%
Written reports from the data protection leader	30%
Corporate communications about policy	35%
Regular presentation by the data protection leader or other personal to senior management	41%
Corporate training programs about data protection (including privacy)	18%
Crisis and data breach incidents reported to management	6%
The results of data protection audits from external auditors	8%
The results of data protection audits from internal auditors	11%
Regular presentation by the data protection leader or other personal to the board or audit committee	28%
No regular or formal communications (merely informal chatter)	25%
Total	202%

#### Part IV: Your position and other organisational characteristics

Q23. What organisational level best describes your current position?	Pct%
Chief executive	23%
Division or business unit president	36%
Vice president	12%
Senior or executive director	18%
Board Member	6%
Retired	5%
Other (please specify)	0%
Total	100%

Q24. In your organisation, how many reporting layers or levels are there between the data protection leader and the CEO (or highest ranking executive)?	Pct%
I am the CEO	23%
One level (direct report)	56%
Two levels	21%
Three levels	0%
Four levels	0%
Five levels	0%
Total	100%

Experience	Pct% mean
Q25a. What is your total business experience in years	31.42
Q25b. How many years have you held your current position	6.80

Q26. Gender	Pct%
Male	71%
Female	29%
Total	100%

Q27. What other job functions do you perform in your organisation? Please check all that apply:	Pct%
No other function performed	78%
Corporate ethics	5%
Corporate law	6%
General management	6%
Human resources	4%
Total	100%

Q28. What is the industry or business group that best defines your organisation? If your organisation contains multiple industry sectors or sub-checks, please check all that apply (or write-in the space for other).	Pct%
Financial services	15%
Technology & software	7%
Retailing	9%
Manufacturing	8%
Hospitality & leisure	6%
Healthcare	3%
Telecom, cable & wireless	8%
Services	7%
Consumer products	8%
Professional services	7%
Education	5%
Pharmaceuticals	6%
Energy	6%
Transportation	3%
Professional services	2%
Internet services	0%
Total	100%

Q29. Is your organisation subject to any of the following data protection or privacy regulatory requirements? Please check all that apply.	Pct%
European Union Data Protection Directive	95%
National privacy laws (ICO)	56%
PCI	56%
Sarbanes Oxley	23%
Basel II	15%
Financial Services Authority (FSA)	15%

Q30. What is the geographical location of your data protection efforts?	Pct%
United States	68%
Canada	59%
Europe	100%
Asia-Pacific	46%
Latin America (including Mexico)	23%
Middle east	29%
Total	296%

Q31. What is the worldwide headcount of your organisation?	Pct%
Less than 500 people	25%
500 to 1,000 people	21%
1,001 to 5,000 people	25%
5,001 to 25,000 people	22%
25,001 to 75,000 people	6%
More than 75,000 people	1%
Total	100%

Q32 Your company has employees located in (check all that apply):	Pct%
United States	50%
Canada	50%
Europe	100%
Asia-Pacific	43%
Latin America (including Mexico)	21%
Middle east	16%
Total	280%

Q33 Is your company publicly traded?	Pct%
Yes, FTSE	16%
Yes, London	25%
Yes, NYSE	5%
Yes, NASDAQ	6%
Yes, overseas exchange	11%
Yes, other minor exchange	0%
No	37%
Total	100%

Q. 34 2008 Total Revenues	Pct%
Less than £100 million	27%
101 to £500 million	30%
501 million to £1 billion	20%
1.1 billion to £10 billion	16%
11 billion to £20 billion	5%
More than 20 billion	2%
Total	100%