

Sponsored by:

Varonis

Independently Conducted by



Presents

Survey on the Governance of Unstructured Data

Published by Ponemon Institute LLC

Draft: May 22, 2008

Private & Confidential Document. Please Do Not Quote Without Express Permission.

Survey on the Governance of Unstructured Data

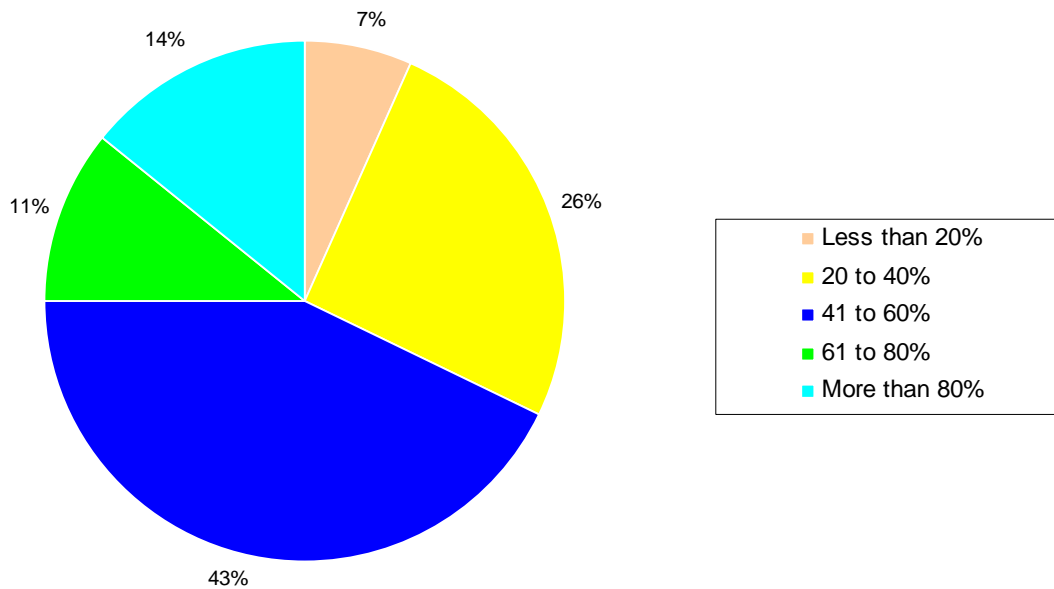
Prepared by Dr. Larry Ponemon, May 22, 2008

The purpose of this study is to better understand organizations' governance procedures for unstructured data. Protection of an organization's unstructured data from overly permissive access is becoming increasingly important because a typical business or government organization stores many thousands of files containing sensitive data in shared folders on file servers and NAS devices. Sponsored by Varonis, the study surveyed 870 individuals who work in IT operations and have an average of approximately 10 years IT and business experience.

In this study, unstructured data refers to electronic information on file servers and Network Attached Storage (NAS) devices that is not stored in a database or in a document/content management system. Examples may include electronic spreadsheets, PowerPoint and Word documents, audio files, videos, blueprints, software source code, instant messages, Web pages and so forth. Ensuring that employees, temporary employees and third-parties have appropriate access to unstructured data is not only critical to an organization's ability to be efficient and competitive but also to be in compliance with data protection regulations.

According to respondents, a significant percentage of their organizations' data is unstructured. As shown in Pie Chart 1, the sample's smallest segment (only 7%) believes that the amount of unstructured data within their organization represents less than 20% of total data. The sample's largest segment (43%) reports that 41% to 60% of their organization's data is unstructured. Fourteen percent of the sample reports that organizational data represents more than 80% of the total data available.

Pie Chart 1: How much organizational data is unstructured?



The three top data categories to be considered most at risk are customer/consumer at 54% of respondents, employee (37%) and sales (35%). Not considered by many respondents to be at risk is research and development (4% of respondents), legal and compliance (4%), finance and development (4%) and executive/board (2%).

In the past 12 months, 26% of respondents report that their organizations had a data breach and 30% report two to more than five breaches. Twenty-five percent were unsure. Of those who had

at least one breach, 57% report that the breach involved the loss or theft of unstructured data containing personal information about people or their households.

In trying to understand current perceptions and practices about the governance of unstructured data, Ponemon Institute sought to find answers to the following questions:

- How much data is unstructured and how well are organizations securing and protecting unstructured data?
- Is governance of unstructured data considered a critical business objective?
- Do individuals in an organization have access to unstructured data that is not pertinent to their role and responsibility?
- How good are organizations at governing access to structured and unstructured data?
- What are the critical success factors for governance of unstructured data?
- How confident are respondents that their organizations have the same visibility to all users of unstructured data as they do to users of structured data?
- Is the ability to control access to unstructured data going to increase in importance?
- What would be the optimal solution to preventing unauthorized access?
- How much money will organizations spend on unstructured data governance solutions?

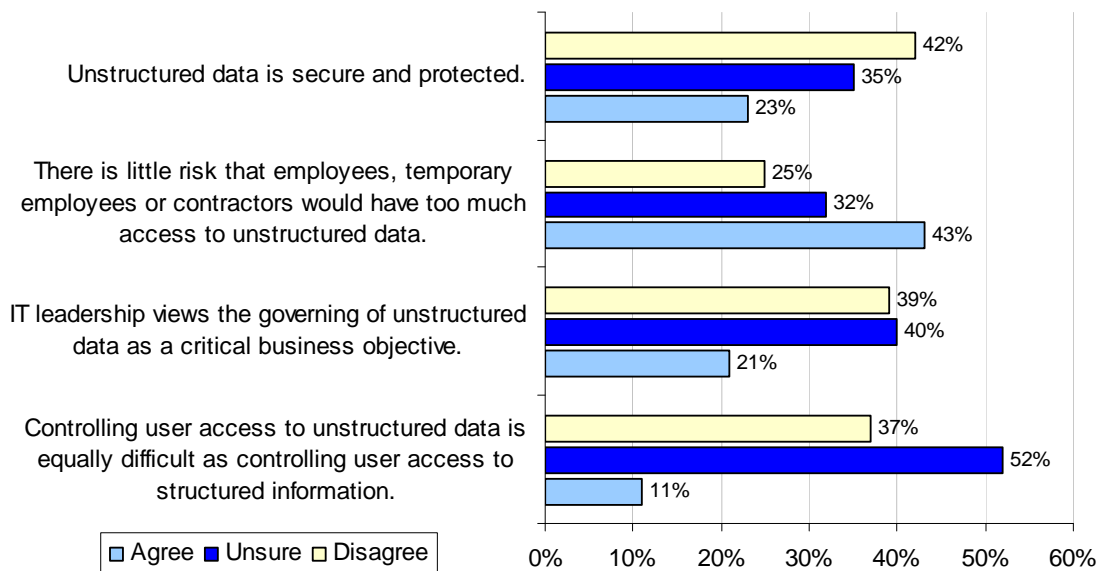
Key Findings

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

1. Unstructured data is at risk in most organizations.

Bar Chart 1 provides respondents' ratings of their organizations.¹ The four attributions reported concern the governance of unstructured data. The pattern of response to these four attributions suggests most respondents hold negative opinions about the protection of unstructured data. For example, only 23% of respondents agree that unstructured data is secure and protected. In contrast, 42% disagree or strongly disagree that protections are adequate and 35% are unsure. This perception that unstructured data is at risk can be in part attributed to the fact that only 21% of respondents report that their IT leadership views the governing of unstructured data as a critical business objective. Another 40% are unsure, and 39% disagree with this attribution. Controlling user access to unstructured data is equally difficult as controlling user access to structured information. 52% disagree, 37% are unsure, and 11% agree.

Bar Chart 1: Respondents' ratings of their organizations

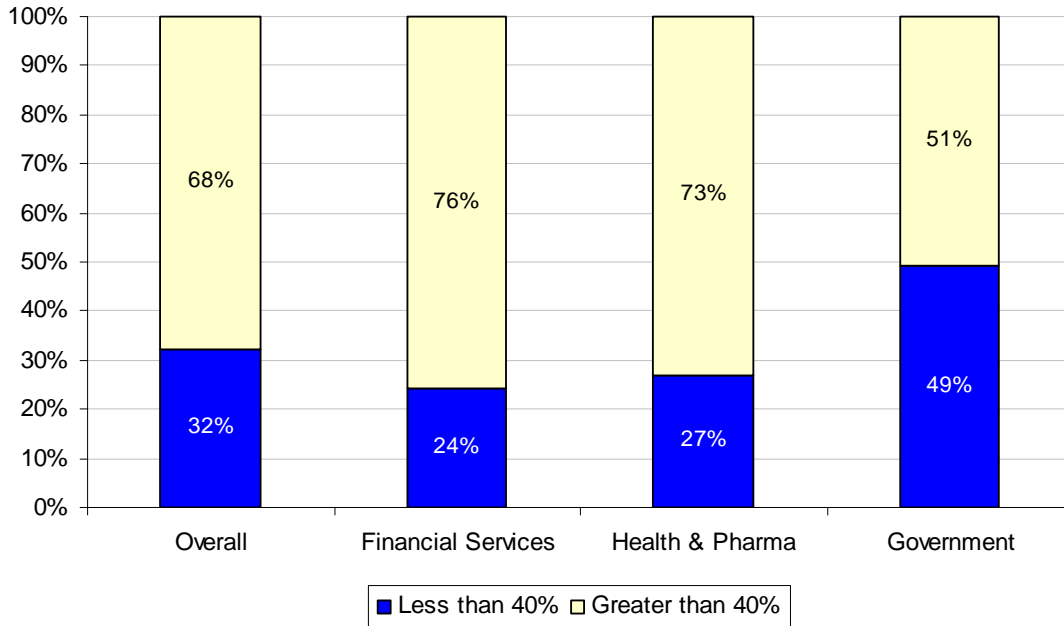


2. Organizations in the financial services and healthcare industries have more unstructured data than other industry segments.

Bar Chart 2 shows the percentage of unstructured data in relation to total data available for three industry groups: financial services (including banks, insurance, credit cards and investment), healthcare/pharma and government. As can be seen, respondents in the financial services and healthcare/pharma industries have a much higher percentage of unstructured data than respondents who are employed in government.

¹ Bar Chart 1 summarizes the results of survey questions 1 to 4. The original question provided a five-point response scale (from strongly agree to strongly disagree). The results shown in this figure combines strongly agree and agree (termed Agree) and strongly disagree and disagree (termed Disagree).

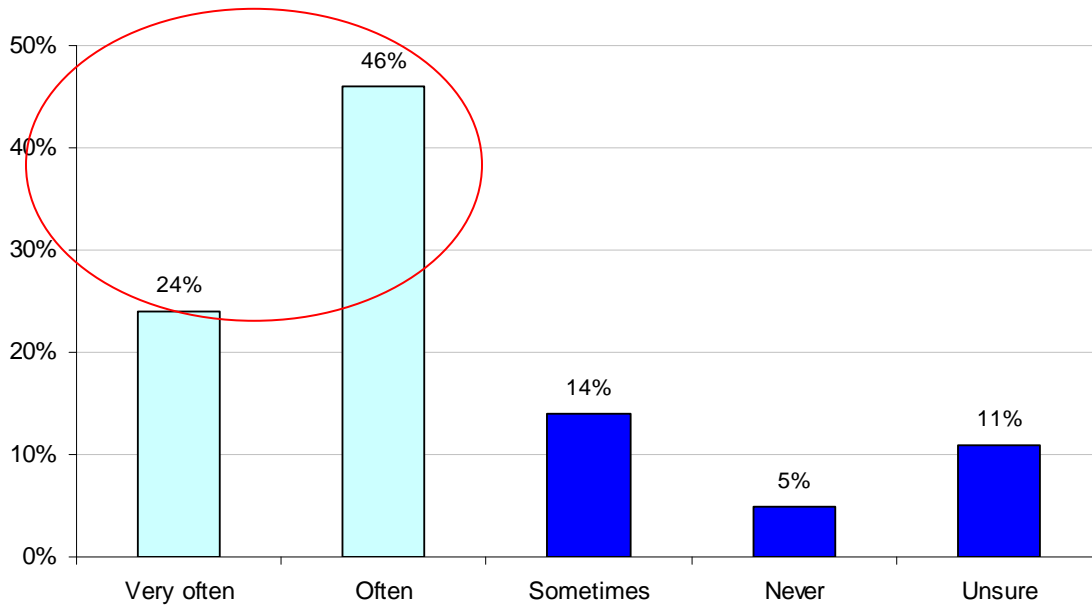
Bar Chart 2: How much organizational data is unstructured?



3. Respondents believe that their organizations are too permissive in the assignment of access privileges and accountability for access governance is questionable.

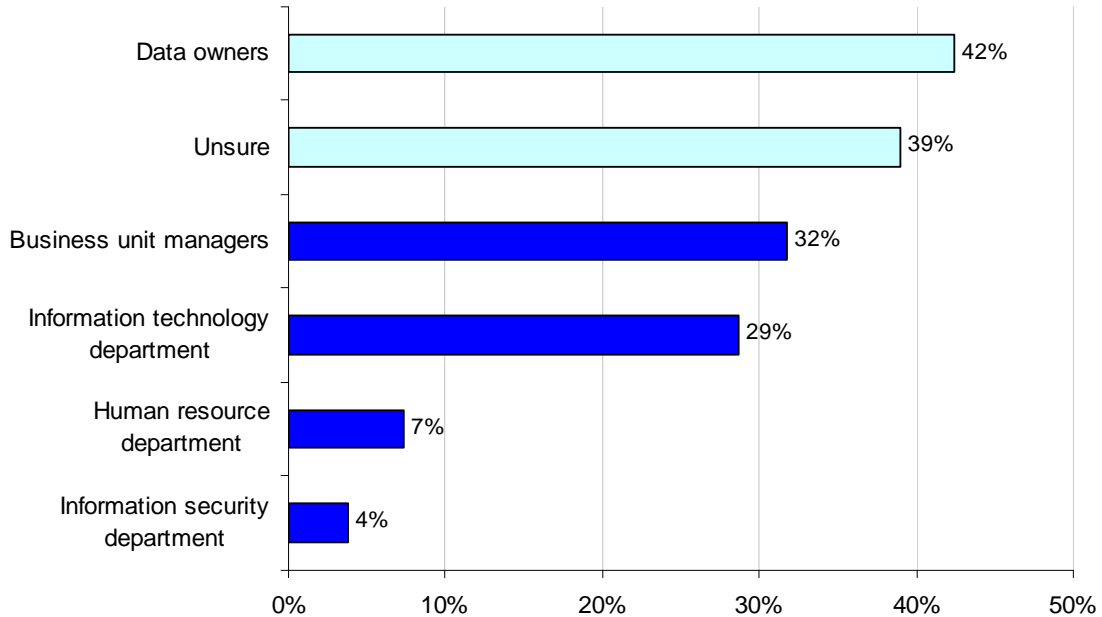
Only 5% believe that employees, temporary employees or independent contractors never have access to unstructured data that is not part of their role or responsibility. As shown in Bar Chart 3, more than 70% report that inappropriate access occurs very often (24%) or often (46%).

Bar Chart 3: How often do employees, temporary employees and independent contractors have too much access to unstructured data?



Bar Chart 4 shows only 29% believe that the IT department should be held accountable for the problem of overly permissive access rights in their organizations. Instead, they believe data owners (42%) and business unit managers (32%) should be accountable. Over 39% are unsure about who has accountability.

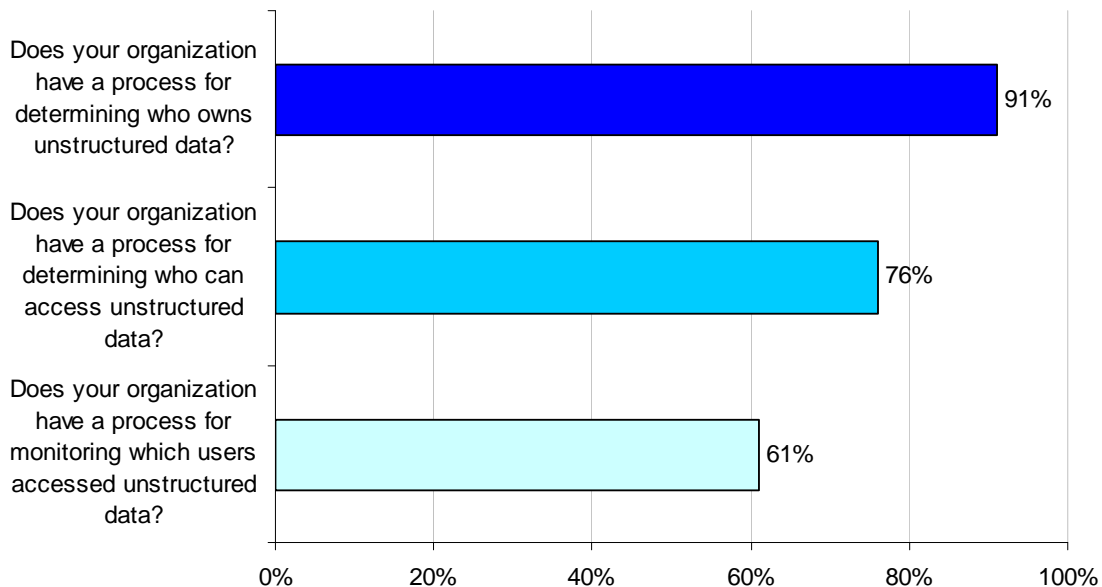
Bar Chart 4: Who has accountability for granting user access to unstructured data?



4. Most organizations do not have a data governance process.

Perhaps the reason that unstructured data is at risk and individuals have overly permissive access rights is that there are no processes in place to address governance of unstructured data.

Bar Chart 5: Is there a governance process for unstructured data?
Percentage No response to each question

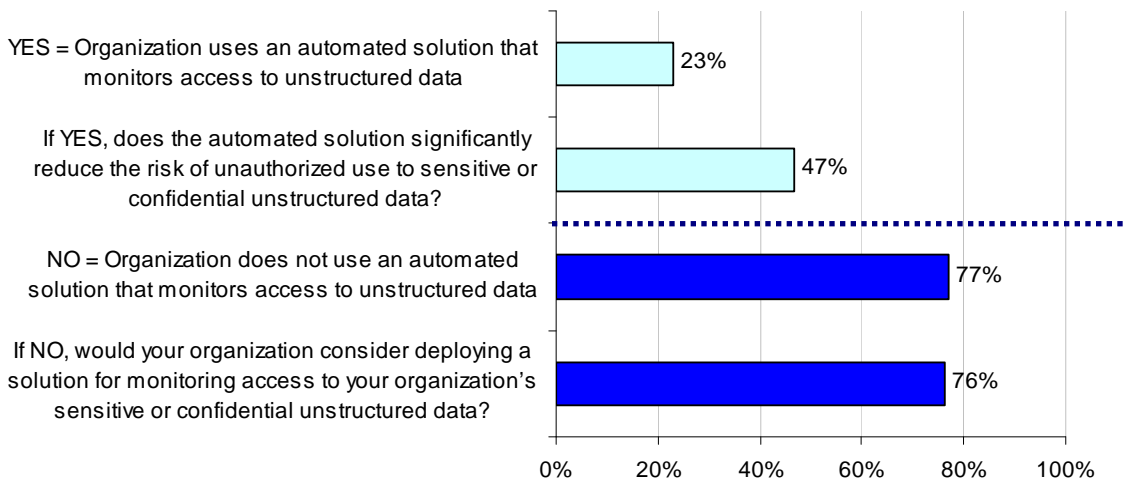


As reported in Bar Chart 5, more than 61% do not have a process for monitoring which users accessed unstructured data, 76% do not have process for determining who can access unstructured data and 91% do not have a process for determining who owns unstructured data.

5. To protect unstructured data, IT professionals need automated solutions and an ample budget.

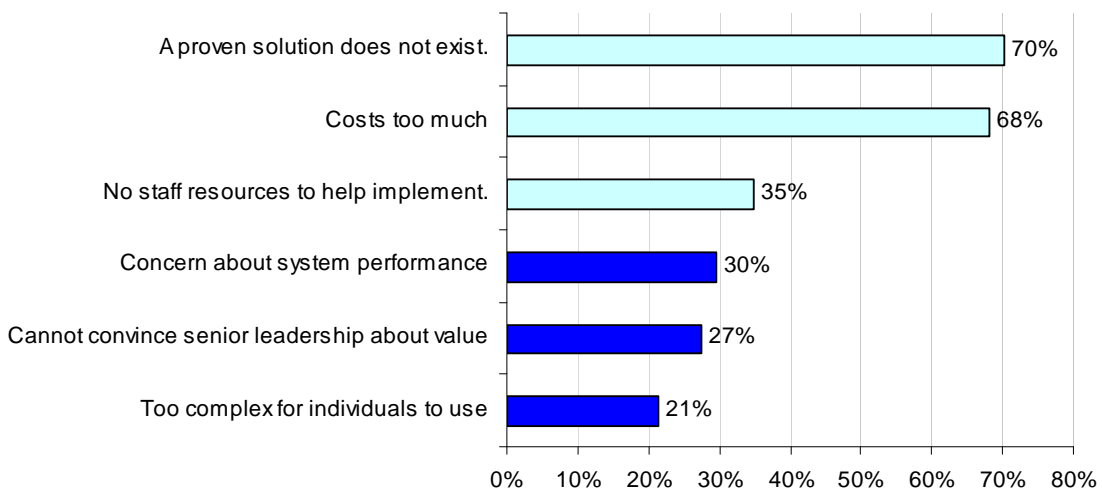
As shown in Bar Chart 6, only 23% of organizations have an automated solution that monitors access to unstructured data. Of this group, 47% are uncertain whether the automated solution significantly reduces the risk of unauthorized access to unstructured data. Seventy-six of those who report that their organizations currently do not have a solution for monitoring access to unstructured data would consider purchasing an automated solution (assuming a proven solution was available).

Bar Chart 6: Respondents' experience in deploying automated solutions for governing unstructured data



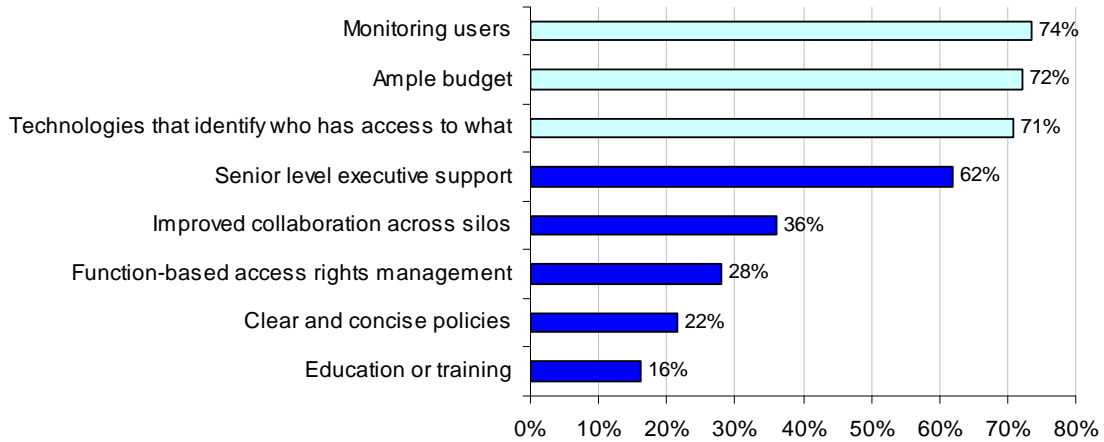
The top three reasons why respondents would not purchase an automated solution are: not aware of any proven solutions (70%), cost (68%), and insufficient staff resources (35%).

Bar Chart 7: If you would not consider using a solution to secure access to unstructured data, why not?



According to Bar Chart 8, the three most important critical success factors for establishing a governance process for unstructured data are: the ability to monitor users (74%), sufficiency of budget resources (72%) and availability of technologies that track access (71%). In addition, 62% of respondents state that senior level executive support is important to overall success.

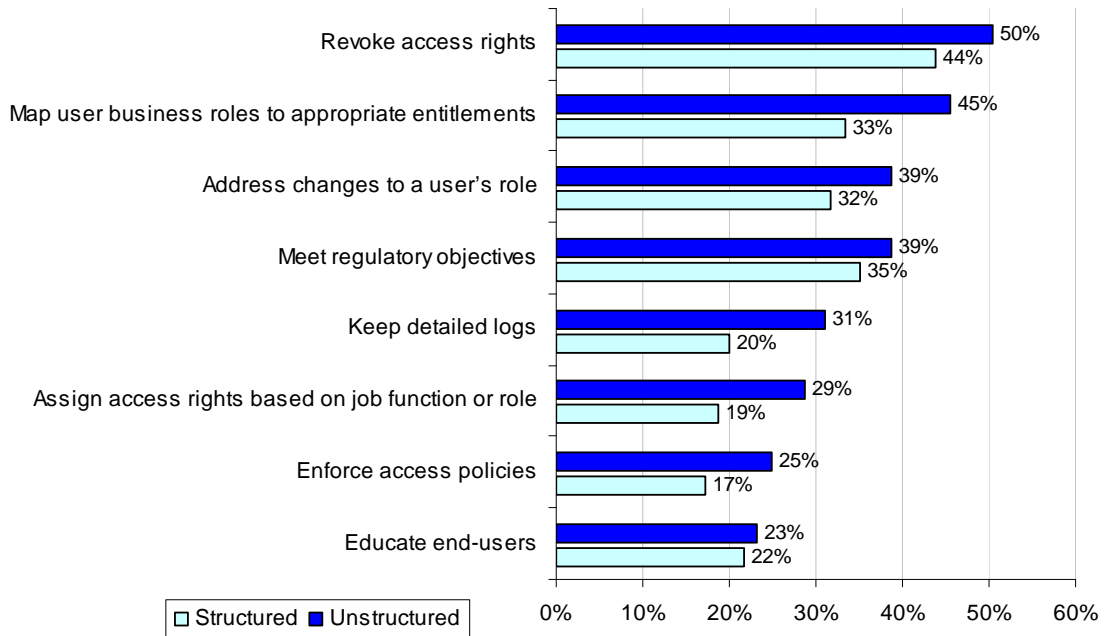
Bar Chart 8: Critical success factors to the governance of unstructured data
Percentage is the importance assigned to each attribute



6. Organizations believe they do a poor job in governing access to both structured and unstructured data.

When it comes to access governance of both structured and unstructured data, many respondents report that their organizations are doing a poor job. Bar Chart 9 shows the percentage of respondents who rated each governance activity as poor (from a graded scale including excellent, good, fair and poor).

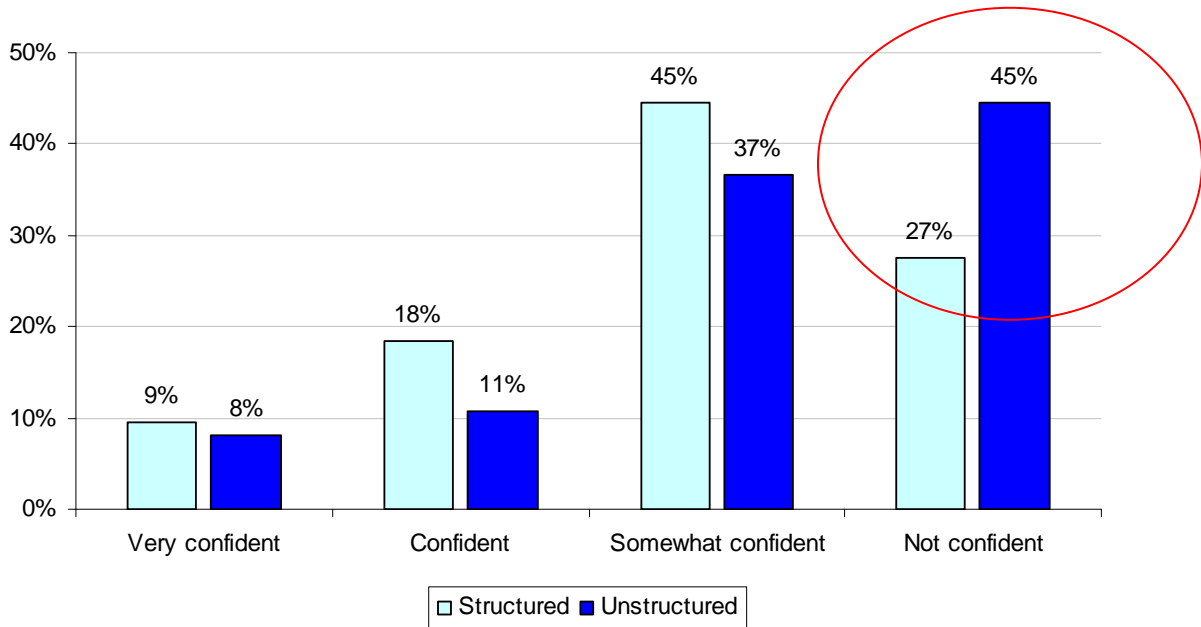
Bar Chart 9: How well do you govern access to structured and unstructured data?
Each bar reflects the percentage of responses = Poor



For all eight governance activities listed in the above chart, unstructured data activities have a higher percentage negative (poor) rating than structured data. The highest negative ratings involve the revocation of access rights, the mapping of user rights to entitlements and addressing change to the user’s role.

In support of the above results, Bar Chart 10 also shows that organizations have slightly better visibility to all users of structured data than unstructured data. It is interesting to note that 27% say they are not confident they have visibility to all users of structured data, while over 45% are not confident they have visibility to all users of unstructured data.

Bar Chart 10: How confident are you that your organization has visibility to all users of structured and unstructured data and their use of these resources?

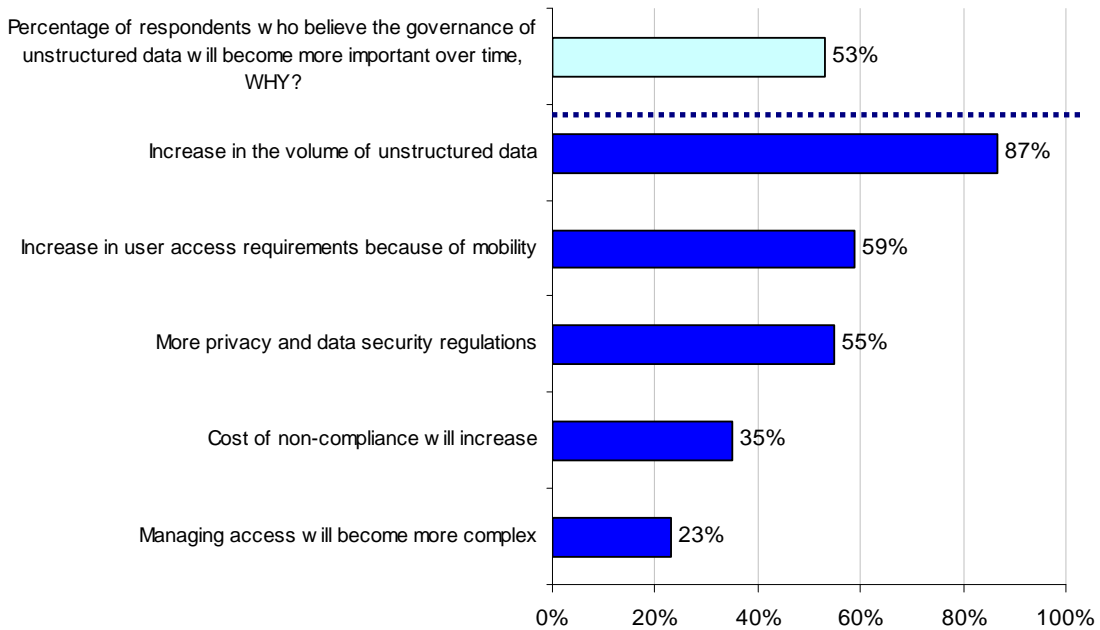


7. The importance of controlling access to unstructured data will increase.

The majority of respondents in our survey reported that their organizations had at least one data breach in the past year. They also reported that a large number of data breaches involved unstructured data about individuals. We believe this contributes to the fairly large percentage of respondents (53%) who believe that controlling access to unstructured data will most likely increase in importance over the next two years.

What are the reasons why unstructured data governance will increase in important? As shown in Bar Chart 11, the three main reasons are: increase in the volume of unstructured data (87%), increase in user access requirements because of mobility (59%) and emerging privacy and data security regulations (55%). Other reasons include: the cost of non-compliance (such as fines or lawsuits) will increase (35%) and the management of access will become more complex as a result of new applications (23%).

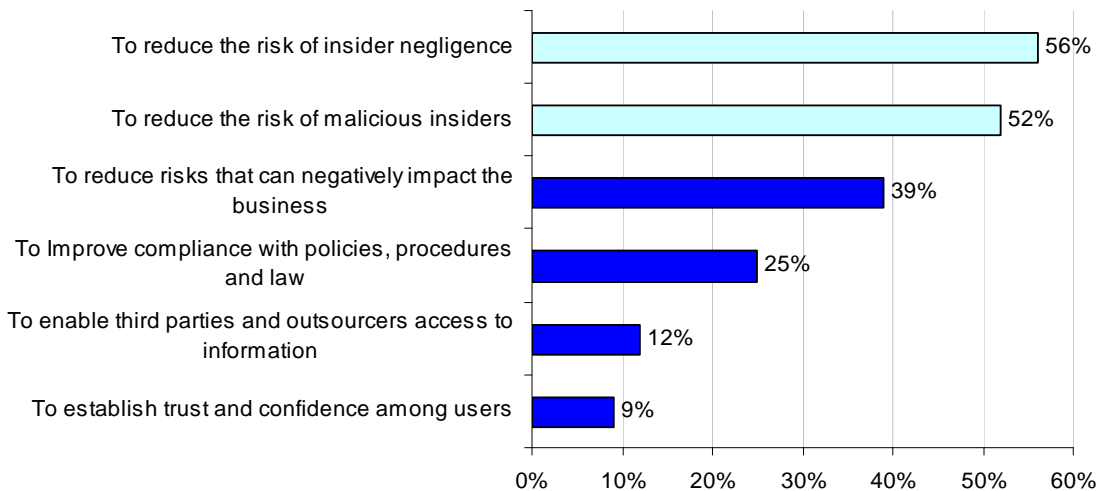
Bar Chart 11: Respondents' beliefs about the importance of unstructured data governance in the future



8. Managing user access to unstructured data will increase in importance because of employee negligence or malicious acts.

In Bar Chart 12, respondents report that the management of user access to unstructured data is important primarily for reducing the risk of insider negligence (58%) as well as insiders' malicious acts (52%). Another reason is to reduce risks that can negatively affect the business. Of least importance to respondents is the belief that unstructured data governance will establish trust and confidence among users (9%).

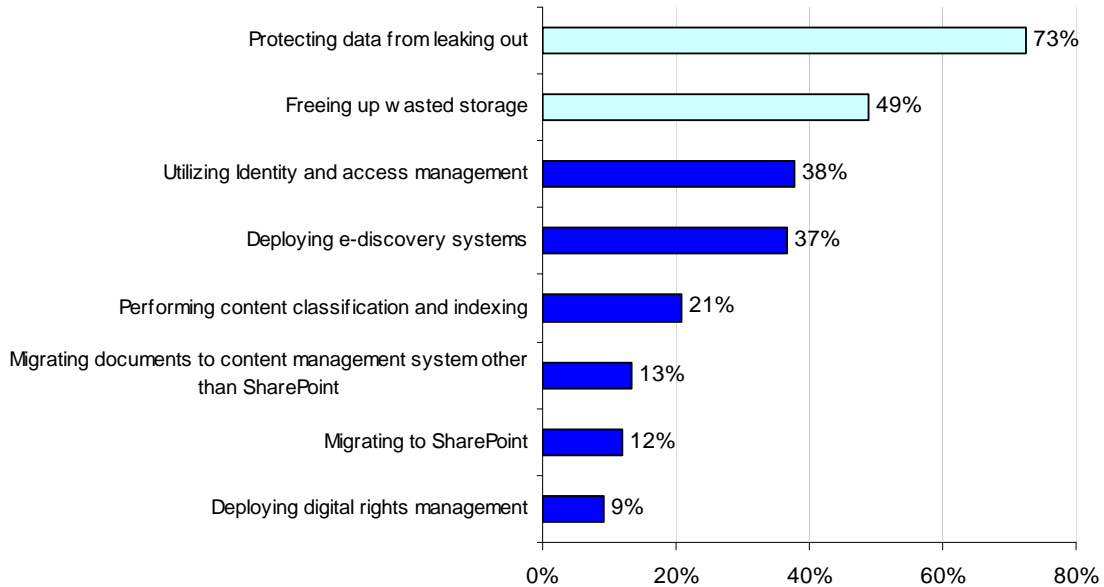
Bar Chart 12: Why is the management of user access to unstructured data important?



9. Prevention of data leakage is the top priority with respect to the management of unstructured data.

As shown in Bar Chart 13, data leakage as a priority is directly related to organizations' concerns about the employee risk to unstructured data. Other priorities also are related to employees' use of unstructured data and include freeing up wasted storage, deploying e-discovery systems and utilizing identity and access management solutions.

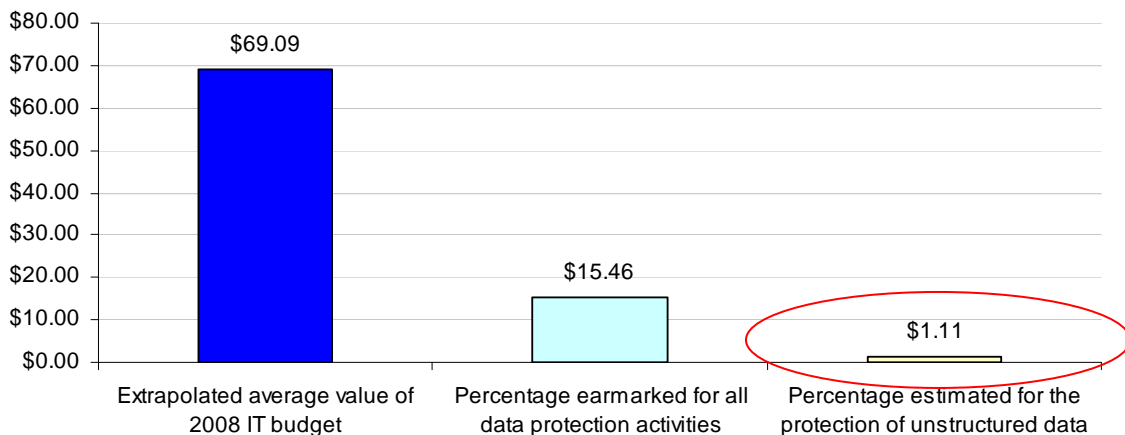
Bar Chart 13: Top priorities in the management of unstructured data
Percentage of first and second importance rating on an eight-point scale



10. Organizations are expected to invest in the protection of unstructured data.

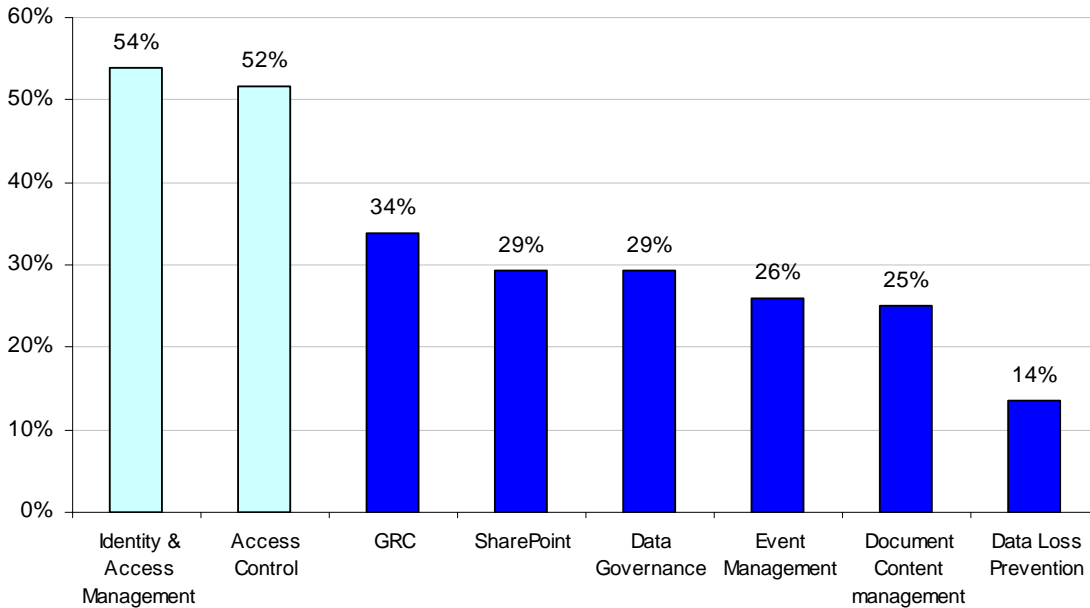
The average 2008 budget for management of unstructured data is expected to be \$1.1 million. This level of funding indicates that, in general, organizations seem committed to this area of information risk.

Bar Chart 14: Extrapolated average value of corporate spending on the the governance of unstructured data (expressed in US \$ millions)



According to Bar Chart 15, the initiatives specifically earmarked in the 2008 budget are identity and access management (54%), access control (52%) followed by governance/compliance risk (34%). While prevention of data leakage is considered a top priority, only 14% have funds designated for that initiative. This may indicate that organizations have just started to recognize the seriousness of the risk and this initiative may receive more funds in the 2009 budget.

Bar Chart 15: Data management initiatives earmarked in the 2008 IT budget



Caveats to this survey

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

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are information technology practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

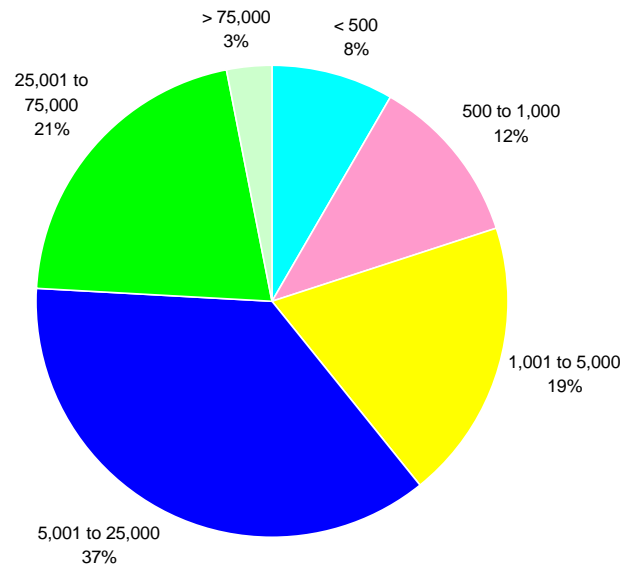
Sample

A random sampling frame of 14,559 adult-aged individuals who reside within the United States was used to recruit participants to this web survey.² Our randomly selected sampling frame was selected from three national mailing lists of professionals employed in the IT operations field.

Table 1 shows that 987 respondents elected to complete the survey results during within an eight-day research period. Of returned instruments, nine survey forms were rejected because of screening criteria to ensure that the final sample was composed of individuals who work in small to medium sized organizations.³ Another 108 were rejected because of reliability tests. A total of 870 surveys were used as our final sample. This sample represents a 6% net response rate. The margin of error on all adjective scale responses is ≤ 4 percent.

Sample description	Total	Pct%
Sampling frame	14,559	100.0%
Bounce back	2,040	14.0%
Total responses	987	6.8%
Cancellations from screening	9	0.1%
Reliability rejections	108	0.7%
Net sample before reliability checks	870	6.0%

Pie Chart 2: Organization size in global headcount



Pie Chart 1 shows that the vast majority of respondents work within larger-sized organizations as measured by worldwide headcount. Only 8% of respondents say that their organizations have fewer than 5,000 employees.

Over 95% of respondents completed all survey items within 20 minutes. Following are key demographics and organizational characteristics for U.S. respondents.

On average, respondents have 9.11 years of experience in the information technology field, and 4.01 years of experience in their current positions. In total, 78% of respondents were males and 22% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields in North America.

² Respondents were given nominal compensation to complete all survey questions.

Table 2a reports the most frequently cited job functions of respondents. Table 2b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the supervisor (25%) are at the technician/staff (37%) levels. Over 13% are at the manager level.

Table 2a: Job functions (based on top 5 titles only)	Pct%
IT operations/supervisor	20%
Systems operation/technician	16%
Manager IT operations	16%
Director, information systems	14%
Quality assurance supervisor	10%
All other titles	24%
Total	100%

Table 2b: Organizational levels	Pct %
Senior Executive	1%
Vice President	2%
Director	10%
Manager	13%
Supervisor	25%
Technician/staff level	37%
Other	12%
Total	100%

Pie Chart 3 reports the distribution of respondents by their organization’s primary industry classification. As shown, over 20% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 13% work for state or local government. Another 12% work in manufacturing industries, and 11% work for healthcare or pharmaceutical companies.

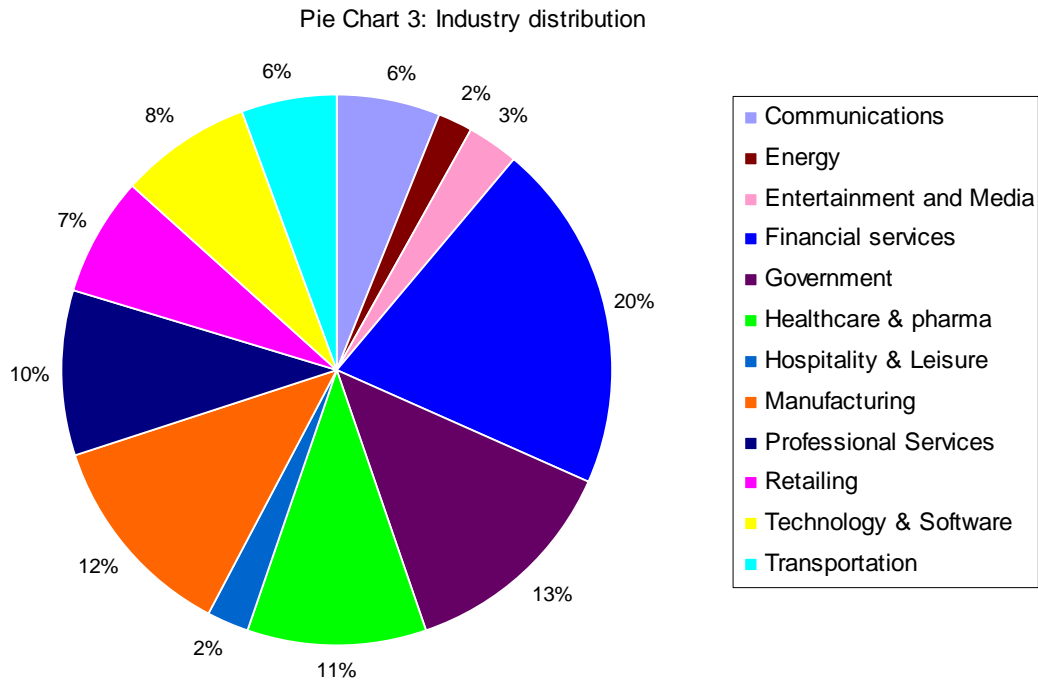


Table 3a reports the organization’s geographic footprint outside the United States, showing that the majority of respondents’ organizations have operations in Canada (79%) and Europe (61%). Table 3b provides the approximate headcounts of the IT departments within participating organizations. As can be seen, 65% of respondents are located within a larger-sized IT department with more than 500 employees.

Table 3a Where are your employees located?	Pct%
United States	100%
Canada	79%
Europe	61%
Asia-Pacific	32%
Latin America (including Mexico)	29%
Other	0%

Table 3b What is the approximate size of your IT department headcount?	Pct%
Less than 5 people	0%
Between 5 to 50 people	2%
Between 51 to 100 people	16%
Between 101 to 500 people	17%
Between 500 to 1,000 people	39%
Between 1,001 to 5,000 people	23%
Over 5000 people	3%
Total	100%

Concluding Observations

IT professionals, business unit managers and data owners need to work together to address the risks associated with the growing volume of sensitive and confidential unstructured data in their organizations. Although the results of our study indicate that IT professionals believe governance of unstructured data will increase in importance, they do not seem to fully understand the enormity of the problems created by overly permissive access rights, cloud computing and negligence and maliciousness in the workplace.

Responses indicate the uncertainty those in IT operations have about issues involving the protection of unstructured data. For example, 32% are unsure whether “there is little risk that employees, temporary employees or contractors would have too much access to unstructured data” while 25% strongly disagree or disagree with that statement. Also revealing is that 52% of respondents are unsure whether it is equally difficult to control user access to unstructured data as it is to control access to structured data. Only 11% strongly agree or agree that it is equally difficult to control access to unstructured data as it is to structured data. The perception that IT leadership does not seem to view the governance of unstructured data as a critical business objective could contribute to this uncertainty.

We believe the solution is dual in nature, involving both technology and individuals who understand the level of access appropriate for each role in an organization. The first step is to determine the amount of unstructured sensitive and confidential data at risk in your organization and to assess what the consequences would be if that data was misused, lost or stolen. Such an assessment could also address the wasted storage problem by determining what unstructured data is not needed and could be destroyed. The benefits of reduced risk to sensitive data and lower data storage costs should convince senior management to recognize that an effective governance strategy for unstructured data is a critical business objective.

The next section provides an Appendix that reports the percentage frequency of respondents for all survey questions included in our survey instrument.

Appendix: Survey Data

Analysis completed on May 5, 2008

The following tables provide the percentage frequencies of survey results for 870 IT practitioners who are employed by business or governmental organizations located in the United States.

Description	Total	Pct%
Sampling frame	14,559	100.0%
Bounce back	2,040	14.0%
Total responses	987	6.8%
Cancellations from screening	9	0.1%
Reliability rejections	108	0.7%
Net sample before reliability checks	870	6.0%

Part I: Issues	
Q1. {Attribute 1} In my organization, unstructured data is secure and protected.	Pct%
Strongly agree	11%
Agree	12%
Unsure	35%
Disagree	23%
Strongly disagree	19%
Total	100%

Q2. {Attribute 2} In my organization, there is little risk that employees, temporary employees or contractors would have too much access to unstructured data.	Pct%
Strongly agree	14%
Agree	29%
Unsure	32%
Disagree	16%
Strongly disagree	9%
Total	100%

Q3. {Attribute 3} In my organization, IT leadership views the governing of unstructured data as a critical business objective.	Pct%
Strongly agree	3%
Agree	18%
Unsure	40%
Disagree	26%
Strongly disagree	13%
Total	100%

Q4. {Attribute 4} In my organization, controlling user access to unstructured data is <u>equally difficult</u> as controlling user access to structured information.	Pct%
Strongly agree	6%
Agree	5%
Unsure	52%
Disagree	30%
Strongly disagree	7%
Total	100%

Q5. What types of unstructured data do you consider to be most at risk in your organization? Please provide no more than three choices.	Total%
Customer/consumer	54%
Employee	37%
Executive/board	2%
Finance & accounting	4%
Internal communications	11%
Legal & compliance	4%
Logistics/supply chain	11%
Marketing	30%
Procurement & vendor	28%
Protect design	15%
Research & development	4%
Sales	35%
Total	234%

Q6. What percentage of your organization's data is unstructured?	Total%	Median	Extrapolation
Less than 20% is unstructured	7%	0.15	1%
20 to 40% is unstructured	26%	0.3	8%
41 to 60% is unstructured	43%	0.5	21%
61 to 80% is unstructured	11%	0.7	8%
More than 80% is unstructured	14%	0.85	12%
Total	100%		50%

Q7. In your organization, estimate how often an employee, temporary employee or independent contractor has access to unstructured data (e.g., documents, spreadsheets, etc.) that is not pertinent to their job description:	Pct%
Never	5%
Sometimes	14%
Often	46%
Very often	24%
Unsure	11%
Total	100%

Q8. Who has accountability for granting user access to unstructured data? Please check only two responses.	Total%
Information technology department	29%
Information security department	4%
Legal, risk or compliance department	1%
Business unit managers	32%
Data owners	42%
Human resource department	7%
Unsure	39%
Total	154%

Q9. Does your organization have a process for monitoring which users accessed unstructured data?	Pct%
Yes	39%
No	61%
Total	100%

Q10. Does your organization have a process for determining who can access unstructured data (e.g., a permissions review)?	Pct%
Yes	24%
No	76%
Total	100%

Q11. Does your organization have a process for determining who owns unstructured data?	Pct%
Yes	9%
No	91%
Total	100%

Q12. How well is your organization able to govern access to structured and unstructured data? Please use the following scale to rate each task provided. 1 = excellent, 2 = good, 3 = fair, 4 = poor, 9 = task is not performed. Blue = unstructured, White = structured	Structured Average	Rank	Unstructured Average	Rank
Assign access rights based on job function or role	2.32	10	2.42	8
Address changes to a user's role (i.e. when a contractor becomes a full-time employee or when an employee is transferred to another department)	2.55	11	2.62	11
Revoke access rights upon an employee's termination	2.86	12	3.01	12
Enforce access policies in a consistent fashion across all enterprise information resources	1.85	6	2.04	6
Monitor and manage access rights of privileged user accounts (such as database administrators or system administrators)	1.68	2	1.74	3
Monitor segregation of duties	1.80	4	1.61	1
Keep detailed logs showing all privileged users' access (authorized or unauthorized)	2.06	7	2.18	7
Meet regulatory compliance objectives and providing evidence of compliance	2.31	9	2.48	9
Map user business roles to appropriate entitlements	2.24	8	2.52	10
Identify user entitlements that are out of scope for a particular role	1.61	1	1.61	2
Educate end-users about access control policies and procedures	1.72	3	1.88	4
Implement identity audit and roles management technologies	1.83	5	1.92	5
Average	2.07		2.16	

Q13. How confident are you that your organization has visibility to all users of **structured and **unstructured** data and their use of these resources?**

Level of confidence for structured data	Pct%
Very confident	9%
Confident	18%
Somewhat confident	45%
Not confident	27%
Total	100%
Level of confidence for unstructured data	Pct%
Very confident	8%
Confident	11%
Somewhat confident	37%
Not confident	45%
Total	100%

Q14. What are the critical success factors for implementing data governance for unstructured data across your enterprise? Please rate the following success factors using the following scale: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	Average
Senior level executive support	2.2
Ample budget	1.9
Technologies that identify who has access and audit data use	2.0
Clear and concise policies and standard operating procedures	3.4
Collaboration across different business units including IT security, business units and audit/compliance teams	3.0
Employee education or training	3.4
Access rights assigned using role or function-based methods	2.8
Rigorous compliance procedures	3.2
Strict enforcement of non-compliance	3.4
Monitoring users	2.2
Audits by an independent third-party	3.6
Average	2.8

Q15a. In your opinion, how will the importance of controlling access to unstructured data change over time?	Pct%
It will become more important for my organization	53%
It will stay the same in terms of importance for my organization	31%
It will become less important for my organization	16%
Total	100%

Q15b. If you believe data access governance will become “more important,” why do you feel this way? Please select all that apply.	Total%
Increase in the volume of unstructured data	87%
Increase in the access requirements for users because of mobility	59%
More privacy and data security regulations to comply with	55%
Managing user access at the application level with become more complex	23%
Cost of non-compliance will increase	35%
Total	259%

Q15c. If you believe data access governance will become “less important,” why do you feel this way? Please select all that apply.	Total%
Decrease in the volume of unstructured data	0%
Increased use of SharePoint or other enterprise content management solutions	65%
Currently implementing an unstructured data governance product/solution	9%
Unstructured data is a “hot” topic now, but will be overshadowed by the next big IT issue	51%
Total	125%

Q16 In your opinion, why is the management of user access to unstructured data important? Please select your top two reasons.	Total%
To reduce the risk of insider negligence	56%
To reduce the risk of malicious insiders	52%
To enable third parties and outsourcers access to information	12%
To Improve compliance with policies, procedures and law	25%
To establish trust and confidence among users	9%
To reduce risks that can negatively impact the business	39%
Total	193%

Q17. With respect to your organization’s unstructured data management priorities, please rank the following eight (8) key activities from 1=highest priority to 8=lowest priority . If possible, please avoid tied ranks.	Average
Protecting data from leaking out	2.16
Migrating to SharePoint	4.36
Migrating documents to an enterprise content management system other than SharePoint	4.38
Deploying digital rights management	5.41
Freeing up wasted storage	3.22
Performing content classification and indexing	4.21
Deploying e-discovery systems	3.34
Utilizing Identity and access management	3.38
Total	3.81

Q18. What is your biggest threat to sensitive or confidential unprotected unstructured data? Please check one (1) choice only.	Pct%
Hackers	2%
Malicious employees	10%
Broken business processes	18%
Employee mistakes	37%
Temporary worker or contractor mistakes	12%
Third party or outsourcer management of data	12%
Not knowing where the data is	9%
Lack of key management for encrypted data	0%
Other (please specify)	1%
Total	100%

Part II: Market Factors	
Q19a. Does your organization currently use any automated solution that monitors access to unstructured data?	Pct%
Yes	23%
No	77%
Total	100%

Q19b. If yes, does the automated solution significantly reduce the risk of unauthorized use to sensitive or confidential unstructured data?	Pct%
Yes	28%
No	26%
Unsure	47%
Total	100%

Q19c. If no, would your organization consider deploying a solution for monitoring access to your organization's sensitive or confidential unstructured data?	Pct%
Yes	76%
No	24%
Total	100%

Q19d. If no, do you believe using any automated solution would increase the effectiveness and efficiency of your company's data governance activities?	Pct%
Yes	16%
No	84%
Total	100%

Q19e. If you would not consider using a solution to secure access to unstructured data, why not? Please choose your top three reasons.	Total%
Concern about system performance	30%
Too complex for individuals to use	21%
Redundancy – other data security safeguards and controls work fine	5%
No need to use it	3%
Costs too much	68%
Can't convince senior leadership about the value proposition	27%
No staff resources to help implement.	35%
To the best of my knowledge, such a solution does not exist.	70%
Total	260%

Following are questions Q20a to Q20g about your IT budget	
Q20a. Are you responsible for managing all or part of your organization's IT budget in 2008?	Pct%
Yes	45%
No (Go to Q26a)	55%
Total	100%

Q20b. Approximately, what is the dollar range best describes your organization's IT budget for 2008?	Pct%	Midpoint	Extrapolated value
Less than \$1 million	0%	0.5	0.000
Between \$1 to 2 million	4%	1.5	0.059
Between \$2 to \$5 million	3%	3.5	0.095
Between \$5 to \$10 million	6%	7.5	0.429
Between \$10 to \$15 million	2%	12.5	0.209
Between \$15 to \$20 million	4%	17.5	0.659
Between \$20 to \$30 million	8%	25	2.057
Between \$30 to \$40 million	15%	35	5.209
Between \$40 to \$50 million	21%	45	9.645
Between \$50 to \$100 million	12%	75	8.936
Between \$100 to \$200 million	19%	150	29.082
Over \$200 million	6%	201	12.709
Total	100%		\$69.09

Q20c. Approximately, what percentage of the 2008 IT budget will go to data protection activities?	Pct%	Midpoint	Estimated Pct%
Less than 5%	4%	2.5%	0.09%
Between 5% to 10%	32%	7.5%	2.37%
Between 10% to 20%	27%	25.0%	6.73%
Between 20% to 30%	17%	25.0%	4.14%
Between 30% to 40%	10%	35.0%	3.50%
Between 40% to 50%	9%	45.0%	4.05%
Between 50% to 60%	1%	55.0%	0.55%
Between 60% to 70%	0%	65.0%	0.19%
Between 70% to 80%	1%	75.0%	0.75%
Between 80% to 90%	0%	85.0%	0.00%
Between 90% to 100%	0%	95.0%	0.00%
Total	100%		22.37%

Q20d. Approximately, what percentage of the budget for data protection activities will be allocated to the protection of unstructured information?	Pct%	Midpoint	Estimated Pct%
Nothing	5%	0.0%	0.00%
Less than 1%	2%	0.5%	0.01%
Less than 3%	6%	2.0%	0.12%
Less than 5%	37%	4.0%	1.49%
Between 5% to 10%	27%	7.5%	2.03%
Between 10% to 20%	16%	15.0%	2.40%
Between 20% to 30%	2%	25.0%	0.47%
Between 30% to 40%	1%	35.0%	0.32%
Between 40% to 50%	0%	45.0%	0.04%
Between 50% to 60%	0%	55.0%	0.12%
Between 60% to 70%	0%	65.0%	0.20%
Between 70% to 80%	0%	75.0%	0.00%
Between 80% to 90%	0%	85.0%	0.00%
Between 90% to 100%	0%	95.0%	0.00%
Total	100%		7.19%

Q20e. Please check the initiatives that are specifically earmarked in the 2008 budget?	Total%
Data Loss/Leakage Prevention	14%
SharePoint	29%
Document/Content Management	25%
e-Discovery	2%
Identify & Access Management	54%
Security Information/Event Management	26%
Data Governance	29%
Governance/Compliance/Risk (GRC)	34%
Access Control	52%
Other (please specify)	420%

Q20f. If Data Governance, GRC or Access Control management is specifically earmarked in the 2008 budget for IT then what is its approximate percentage of this within the total 2008 security budget?	Pct%	Midpoint	Estimated Pct%
Nothing	0%	0.0%	0.00%
Less than 1%	0%	0.5%	0.00%
Less than 3%	2%	2.0%	0.05%
Less than 5%	5%	4.0%	0.19%
Between 5% to 10%	2%	7.5%	0.11%
Between 10% to 20%	18%	15.0%	2.72%
Between 20% to 30%	12%	25.0%	2.97%
Between 30% to 40%	31%	35.0%	10.82%
Between 40% to 50%	13%	45.0%	5.92%
Between 50% to 60%	12%	55.0%	6.68%
Between 60% to 70%	5%	65.0%	3.45%
Between 70% to 80%	0%	75.0%	0.00%
Between 80% to 90%	0%	85.0%	0.00%
Between 90% to 100%	0%	95.0%	0.00%
Total	100%		32.91%

Q20g. Approximately, what percentage of the Data Governance, GRC or Access Control management budget will be allocated for controlling access to unstructured information?	Pct%	Midpoint	Estimated Pct%
Nothing	2%	0.0%	0.00%
Less than 1%	1%	0.5%	0.00%
Less than 3%	10%	2.0%	0.20%
Less than 5%	9%	4.0%	0.35%
Between 5% to 10%	10%	7.5%	0.73%
Between 10% to 20%	17%	15.0%	2.54%
Between 20% to 30%	12%	25.0%	3.10%
Between 30% to 40%	26%	35.0%	9.17%
Between 40% to 50%	12%	45.0%	5.26%
Between 50% to 60%	1%	55.0%	0.40%
Between 60% to 70%	1%	65.0%	0.41%
Between 70% to 80%	0%	75.0%	0.00%
Between 80% to 90%	0%	85.0%	0.00%
Between 90% to 100%	0%	95.0%	0.00%
Total	100%		22.17%

About data breach	
Q26a. Did your experience a data breach in the past 12 month period?	Pct%
Yes, only one incident	26%
Yes, two to five incidents	27%
Yes, more than five incidents	3%
No	19%
Unsure	25%
Total	100%

Q26b. If you said yes, did the breach involve the loss or theft of unstructured data containing personal information about people or their households?	Pct%
Yes	57%
No	43%
Total	100%

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