

Sponsored by

ORACLE®

Independently Conducted by



Presents

**What Worries IT & Compliance
Practitioners Most about Privacy and
Data Security?**

2007 US Survey

Published by Ponemon Institute LLC

June 1, 2007

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 Please Do Not Quote Without Express Permission.

What Worries IT & Compliance Practitioners Most about Privacy and Data Security?

By Dr. Larry Ponemon, June 1, 2007

1. Executive summary

This study is about how more than 1,000 IT and compliance practitioners perceive the plethora of privacy and data protection risks that might seriously impact their organizations. In most organizations, these two separate functions are accountable for identifying and managing data risks, such as the theft of information assets, missing laptops and other portable storage devices, and the negligent loss of customer or employee records that require legal notification.

We decided to conduct this study to better understand:

- a. How prepared are organizations to counter the threat of privacy and security breaches?
- b. Do IT and compliance practitioners, despite differences in expertise and responsibilities, hold similar views and priorities regarding data risk management? In other words, can they be in sync on objectives and goals for reducing or mitigating privacy or data protection risks?

Our study utilized a case study approach involving 10 commonly encountered data risk scenarios for two independent samples involving highly experienced IT practitioners and corporate compliance professionals (including both internal and system auditors). Our most salient findings are summarized as follows:

- *42% of IT practitioners believe that their organizations are doing an inadequate job in diminishing the loss or theft of confidential information.* They also believe their companies lack the necessary security tools or internal controls to prevent, detect and correct data security breaches.
- *Nearly half (45%) of the IT respondents believe they would be unable to notify users and customers impacted by a data breach.* This is also evident in the fact that an incredible 68% feel there is too much Personally Identifiable Information (PII) scattered across their systems, hindering their ability to audit the use of such.
- *IT practitioners (including IT security professionals) are much more pessimistic about their organization's ability to detect and control data risks than their compliance counterparts.* Only 33% of the compliance group believes that they are vulnerable to data breaches compared to 42% of the IT group. This was a surprising result given that compliance experts and auditors are expected to constantly push for stronger security controls within their organizations.
- *Compliance practitioners in many cases lack the knowledge or expertise to recommend IT security tools for mitigating or reducing data risk.* IT practitioners, on the other hand, consistently view the need for automated audit management and security control tools to combat data security and privacy risks.
- Both groups believe that the situation is going to get worse in the next 12-18 months, and isn't getting better.
- Audit Management and User Access Control tools rank highest in the technologies expected to see increased adoption in the next 12-18 months.

These first four findings have disturbing implications for any organization collecting, using and sharing sensitive information. It suggests that the IT and compliance practitioners who are

required to deal with IT security and privacy issues see the potential for catastrophic data loss. They also believe that their organizations are grossly inadequate in curbing this potential risk.

We recommend that organizations, as part of their governance structure, present opportunities for IT and compliance practitioners to work together and address data security risks. In other words, eliminate the silo approach to governance that is pervasive in so many organizations. Second, decision-makers should listen to those individuals in the trenches who are closest to the risks that threaten organizations. It is our hope that the results of this study will help business leaders understand the need to address these risks in a holistic rather a piecemeal approach.

The remainder of this paper is organized as follows:

Part 2: Introduction, with an analysis of our most salient survey findings

Part 3: Samples, also describing key organizational characteristics of our study

Part 4: Detailed results of all survey questions asked for both the IT and Compliance samples

Part 5: Caveats about Web-based research methods used in this study

Part 6: Conclusion

2. Introduction

Are corporate IT and compliance professionals in the United States (US) concerned about their organizations' ability to prevent, detect and correct situations that compromise their organization's ability to prevent privacy or data protection incidents? Do they believe their organizations' controls and data security tools are sufficient to protect confidential or sensitive information? The present study, which was independently conducted by Ponemon Institute and sponsored by Oracle, seeks to answer the following questions.

- What types of privacy-related incidents do IT and compliance practitioners worry about?
- Are organizational controls and systems sufficient to prevent or reduce the risk of a privacy or data protection incident?
- What manual and IT controls do companies have today to prevent or reduce privacy and data protection risk?
- What manual and IT controls do respondents hope to acquire in the future to prevent or reduce privacy and data protection risk?
- Do respondents believe that the state of privacy and data protection within their organizations is getting worse over the next 12 to 18 months?

In this study, we survey two independent panels. Our first sample includes 610 experienced respondents who are employed in corporate IT departments located in the US. Our second panel includes 456 experienced respondents who work in either the corporate compliance or internal auditing fields. We use scientific sampling methods and Web-based survey methods to capture individual responses. The final response rate for both samples is over 6%. The overall margin of error for all objective survey items is $\pm 3\%$.

The survey instrument contains scenarios about 10 common privacy and data security threats faced by most major organizations. Survey scenarios are based on actual case histories that result in a material or catastrophic data breach for companies over the past two years. In addition, the survey captures information about the privacy and data security controls respondents view as most important to reduce or mitigate each one of the 10 threat areas presented. Finally, the survey captures organizational characteristics and other individual demographics.

Our two guiding hypotheses for this research are:

H₁: IT and compliance practitioners will hold differing views (a.k.a. **expectation gap**) about the presented scenarios, suggesting that the individual's role, experience and expertise will affect their perceptions and beliefs about certain privacy and data security threats.

H₂: IT and compliance practitioners will hold differing views about the types of security controls most appropriate for reducing or preventing each privacy or data security threat.

Why do we believe these hypotheses are important? Simply stated, an effective data security program requires both IT and compliance practitioners to be on the same page; that is, holding consistent views about risk priorities and mitigation methods. An incoherent strategy or approach to managing privacy and data security creates serious vulnerabilities for organizations, including gaps in controls and the misapplication of data security methods.

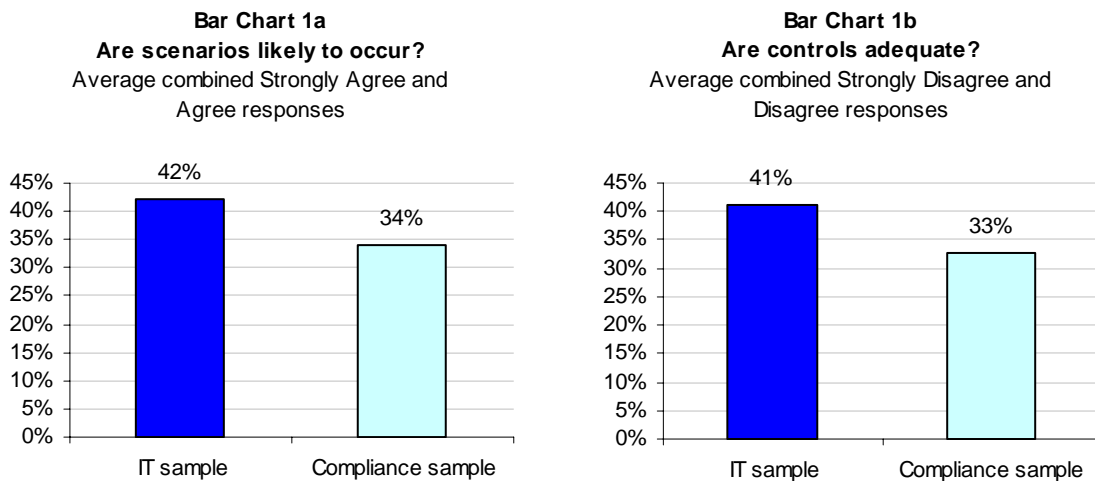
What did we find?

Responses from 10 different scenarios were used to define the expectation gap between the IT and compliance samples. Following is a summarized list of the incidents used in the survey:

- Employee negligence resulting in the loss of employee data from a home computer
- Lack of controls to revoke access privileges after an employee leaves a company
- Data spill of names and email addresses of people who registered on a website
- Backup tape containing customer information is lost in transit
- Database containing unprotected credit card information is hacked by criminals
- A data breach involving customer data is not communicated to individuals (as required by law)
- A data breach results in significant churn or turnover of customers
- Employee data is moved from Europe to the US without complying with the EU privacy directive
- Too much personally identifiable information makes it nearly impossible to perform a data inventory
- Compliance audit reveals that over privilege, where system users have too much access to sensitive data

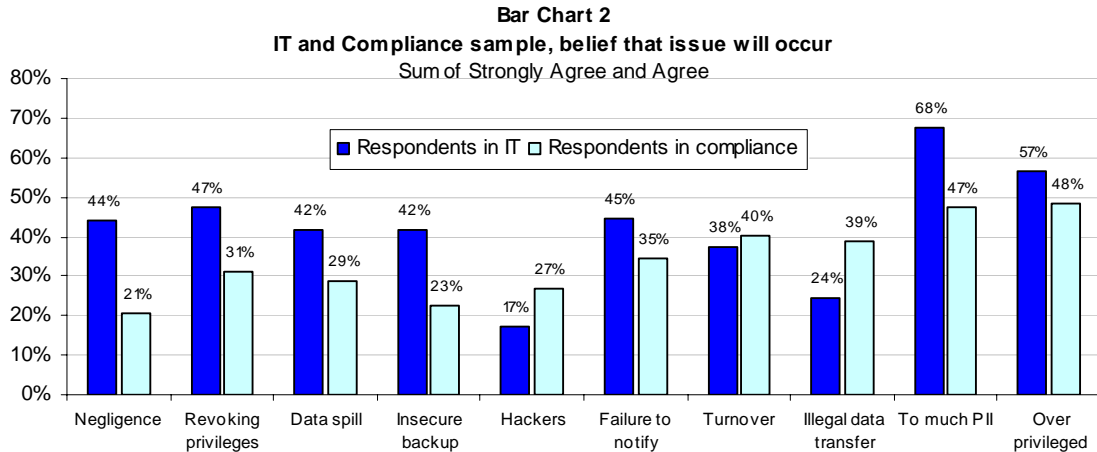
A five-point adjective scale was used for each scenario to capture the respondent's perception from "strongly agree" to "strongly disagree." The combined "agree" and "strongly agree" response for the question, "This type of incident can happen in my organization" was compiled for both samples, with the results shown in Bar Chart 1a. The combined "disagree" and "strongly disagree" response for, "My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring" is shown in Bar Chart 1b.

As shown below, 42% of IT practitioners and 34% of compliance professionals believe that the presented scenarios are likely to occur within their companies. Similarly, 41% of IT practitioners and 33% of compliance professionals believe that controls are inadequate to prevent or reduce the presented incidents. The relatively high percentage response shown in 1a and 1b suggests that both groups are concerned about their organizations' ability to reduce privacy risks. Further, the 8% difference between samples in both bar charts suggests IT practitioners are more concerned or pessimistic about their organization's ability to combat privacy-related incidents than compliance professionals.



Detailed analysis of scenarios for both samples revealed that perceptions about privacy and data security glitches vary considerably across incidents. Bar Chart 2 shows that a very high percentage of both IT and compliance respondents believe these incidents are likely to occur within their companies.

For seven scenarios, respondents in the IT sample hold more pessimistic perceptions about risk occurrence and the adequacy of controls than respondents in the compliance samples. Three scenarios where compliance practitioners hold more pessimistic views include: (1) hackers, (2) abnormal customer churn after data breach notification, and (3) data transfer that does not comply with the EU privacy directive.

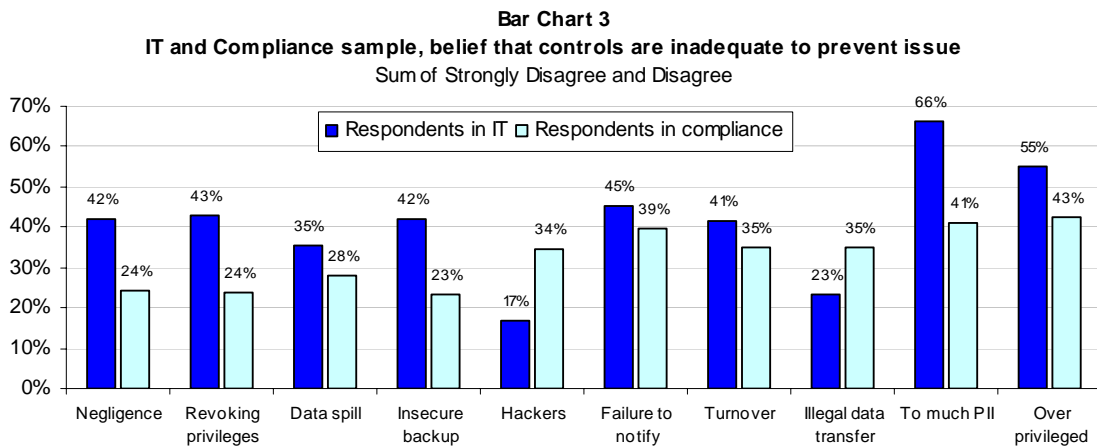


The biggest differences between the IT and compliance group in terms of likelihood of occurrence, where respondents in IT are more pessimistic than compliance, include:

- Too much PII (Difference > 21%)
- Employee negligence (Difference > 20%)
- Insecure backup (Difference > 19%)
- Revoke privileged access (Difference > 16%)

When compliance respondents are more pessimistic than IT respondents, the biggest difference concerns non-compliance with the EU privacy directive (Difference > 14%).

Bar Chart 3 reveals that many respondents see their organizations' extant controls as insufficient. Similar to the above findings, we found differences between both samples.



When IT respondents are more pessimistic than those in compliance, the most significant difference include:

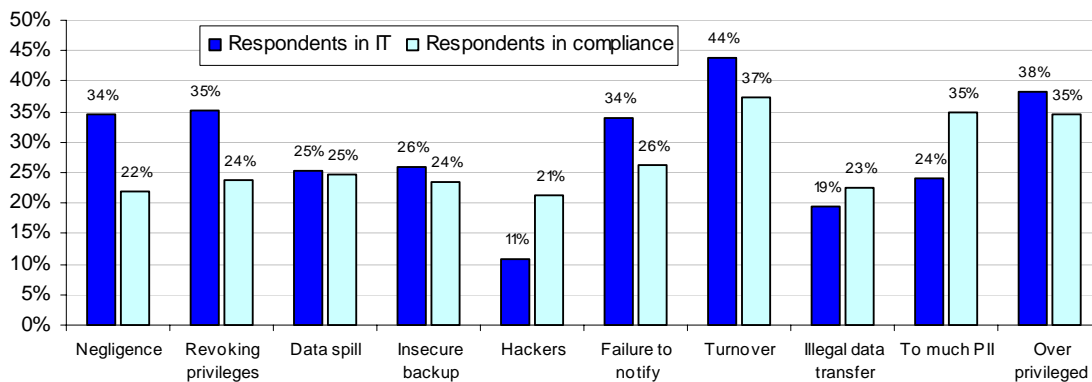
- Too much PII (Difference > 15%)
- Revoke privileged access (Difference > 19%)

- Insecure backup (Difference > 19%)
- Employee negligence (Difference > 18%)

When compliance is more pessimistic than IT, the biggest difference concerns controls that prevent or curtail hackers from accessing sensitive information (Difference > 17%). In general, IT practitioners do not see external threats from hackers as significant a vulnerability or risk area as negligent or malicious insiders. In contrast, compliance professionals appear to be much more concerned than IT practitioners about hackers.

Bar Chart 4 reports the results to a question posed for each scenario about whether or not the incident is more likely to occur within the next 12 to 18 months. In other words, is privacy and data protection getting better, staying the same or getting worse in the eyes of the respondent?

Bar Chart 4
IT and Compliance sample, belief that the issue is getting worse
 Sum of Strongly Agree and Agree



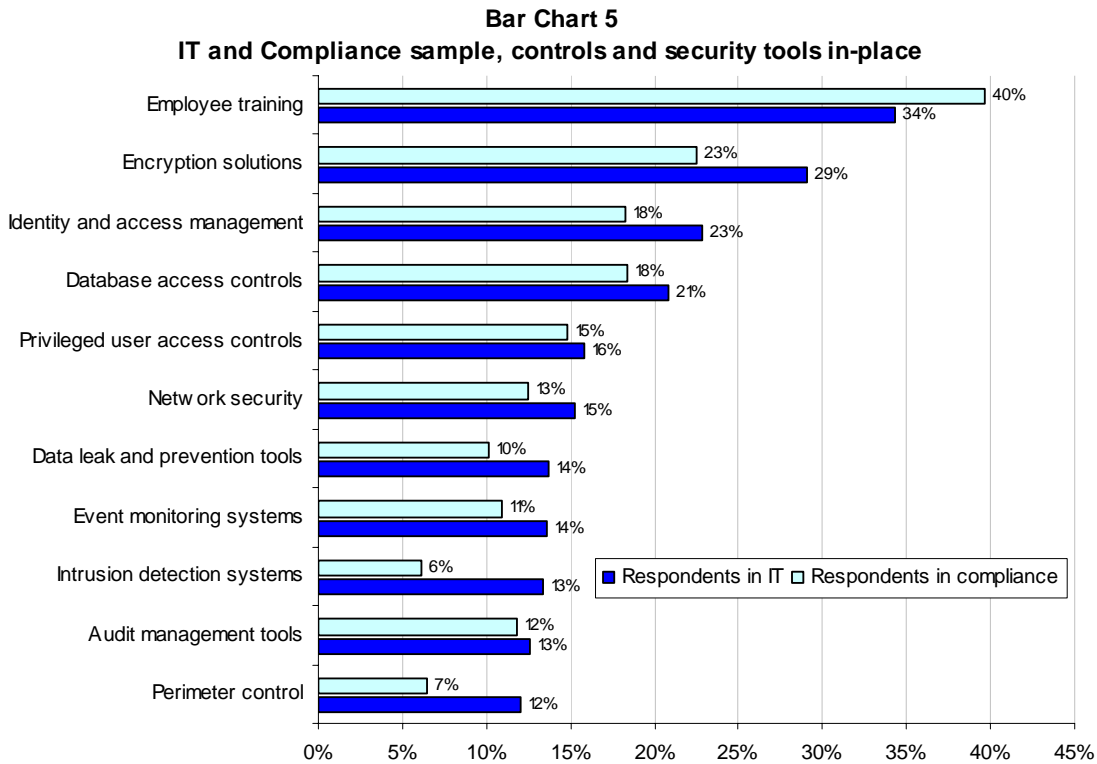
The above bar chart shows a similar pattern of results. That is, IT respondents are more pessimistic than compliance respondents about incidents becoming worse. IT rates the following incident as more likely to occur in the future: negligence (Difference > 12%) and the revoking privileged access (Difference > 11%). Respondents in the Compliance sample believe unprotected PII (Difference > 11%) and attacks by hackers (Difference > 10%) are getting worse.

Our final analysis concerns the data security technologies and related manual controls organizations have in-place today (or will have in the near future) to prevent, detect or correct privacy-related incidents. The survey instrument includes a list of 15 different technology and control categories frequently used by companies to manage privacy and data protection risks. Following are the categories used in our survey:

- Anti-worm, virus, spyware and Trojan solutions
- Audit management tools
- Data leak prevention systems
- Database access controls
- Digital rights management
- Employee training and awareness
- Encryption solutions
- Event monitoring and management systems
- Identity and access management
- Incident response plan
- Intrusion detection systems
- Network security
- Perimeter controls (such as firewalls)
- Privileged user access controls

By design, some of the control or system categories are extraneous to a given scenario. For instance, perimeter controls are important when dealing with an external threat such as a hacking attack, but is not relevant when dealing with the administration of too much PII.

Bar Chart 5 lists 11 control or system categories in ascending order of relevance with respect to all 10 scenarios included in the survey.¹ As shown, the number one control for combating privacy and data protection risk concerns employee training and awareness – followed by encryption solutions, identity and access management, and database access controls.



The most significant differences between respondents, where average results for the IT sample are greater than for compliance, include: encryption solutions (Difference > 7%), intrusion detection systems (Difference > 7%), perimeter controls (Difference > 6%), and identity & access management (Difference > 5%). In contrast, for the Compliance sample, the only average result greater than for IT is employee training and awareness (Difference > 5%).

Bar Charts 6a and 6b show the net change in data security technologies that respondents in both samples believe their organizations should implement over the next 12 to 18 months to prevent or reduce the most salient areas of risk. The percentage change for each category (θ) is defined as:

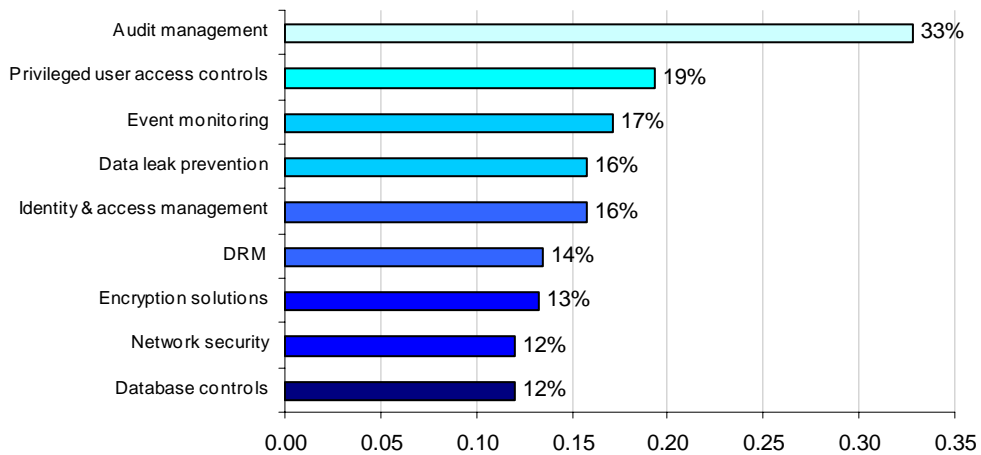
$$\text{Percentage Change } \{i\} = \{ \theta_{i[\text{future state}]} - \theta_{i[\text{current state}]} \} / \theta_{i[\text{current state}]}, \text{ for all categories } = i.$$

According to Bar Chart 6a, the largest percentage change for IT practitioners concerns audit management tools, where 33% of practitioners view this category as likely to increase over the next 12 to 18 months in response to privacy and data security threats. The percentage change in Bar Chart 6b for compliance practitioners is much lower at nine percent, suggesting they do not

¹Four controls are omitted from the analysis because of insignificant results.

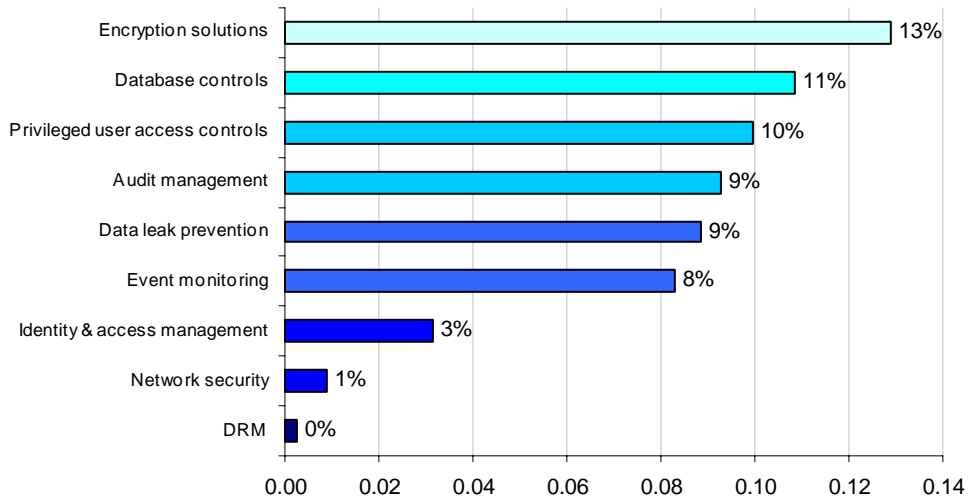
hold a comparable view or understanding about audit management tools. Other salient net changes for IT practitioners include privileged user access controls (19%), event monitoring (17%), and data leak prevention (16%). These findings suggest IT respondents view these categories of technology or controls as likely to increase over the next 12 to 18 months in response to privacy and data protection risks.

Bar Chart 6a
What security technologies are most likely to change?
 Net changes for IT practitioner sample



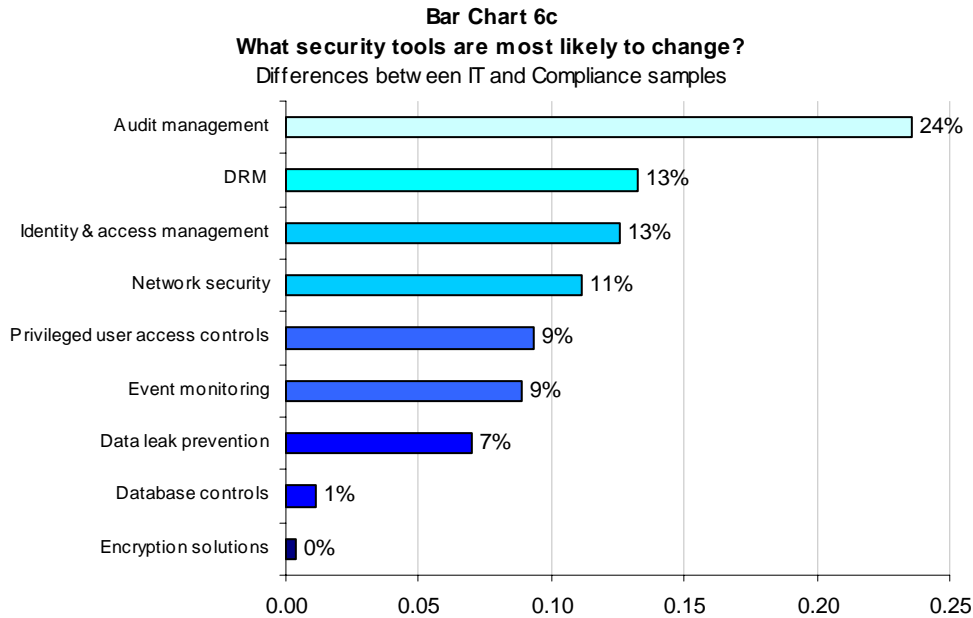
As reported in Bar Chart 6b, with the exception of encryption solutions, we observe percentage change measures for the Compliance sample are lower than those reported for IT respondents in Bar Chart 6a. This suggests compliance practitioners may be less inclined to rely on emerging technologies to prevent or reduce privacy and data protection risks than IT professionals.

Bar Chart 6b
What security technologies are most likely to change?
 Net changes for Compliance practitioner sample



Bar Chart 6c shows differences in net change measures for each category between the IT and Compliance samples. As shown, the most salient differences include audit management tools (Difference = 24%), identity & access management (Difference = 13%), digital rights management (Difference = 13%), and network security (Difference = 11%). These significant differences

confirm that IT respondents are more likely to see the need for data security tools to contain privacy and data protection risks within their organizations.



3. Samples

Two separate sampling frames consisting of 8,960 US-based IT practitioners (including IT security) and 7,095 compliance or internal audit professionals were used to recruit participants to our Web survey. Our independently constructed samples were selected from national panels using scientific selection methods. In total, 610 respondents in IT and 456 respondents in compliance completed survey results during an eight day research period in April 2007. Of the returned instruments, 114 surveys were rejected for reliability purposes. The final samples represent over a 6.8% and 6.4% response rate, respectively, for the IT and compliance samples. The margin of error on all adjective scale response items is $\leq 3\%$ for each sample.

Table 1a IT practitioners	Freq.	Pct%	Table 1b Compliance practitioners	Freq.	Pct%
Sampling frame	8,960	100.0%	Sampling frame	7095	100.0%
Invitations sent	8,208	91.6%	Invitations sent	6612	93.2%
Bounce back	944	10.5%	Bounce back	781	11.0%
Total sample	675	7.5%	Total sample	505	7.1%
Rejections	65	0.7%	Rejections	49	0.7%
Final sample	610	6.8%	Final sample	456	6.4%

Over 90% of respondents completed all survey items within 15 minutes. Respondents were given the following instruction before starting the survey.

This survey focuses on what worries you most about your organization's ability to protect the personal information it collects and uses about customers, target customers, employees, shareholders, contractors and any other individuals. In this survey, we describe 10 privacy and data security incidents. Following each incident, we ask if you believe this could occur in your organization, if you have the necessary controls to prevent or reduce the consequences of this incident, and whether you think that the likelihood of this incident occurring in your organization will increase in the next 12 months. Please note that no personally identifiable information is collected. Thank you in advance of your participation in this important study.

Table 2a reports the most frequently cited job titles of IT respondents (Top 5 list), and table 2b has the most frequently cited titles of respondents in compliance.

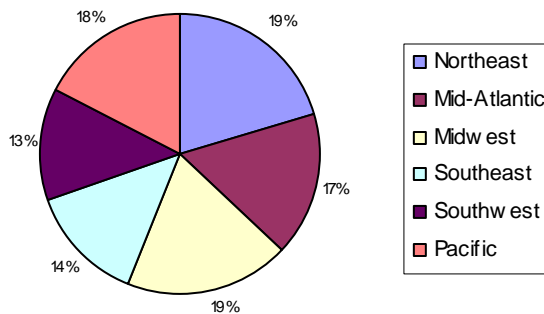
Table 2a IT practitioners			Table 2b Compliance practitioners		
	Freq.	Pct%		Freq.	Pct%
IT Operations	78	13%	Manager, internal audit	79	17%
Director, information security	71	12%	Director, systems auditor	62	14%
Manager, information security	62	10%	Director, corporate compliance	58	13%
Chief information security officer	56	9%	Manager, corporate compliance	58	13%
Director, network operations	42	7%	Compliance officer	54	12%
All other titles	301	49%	All other titles	145	32%
Total	610	100%	Total	456	100%

Table 3 provides the self-reported organizational level of respondents in both samples. As can be seen, the majority of IT respondents are at the manager (30%) or associate/technician/staff (29%) levels. The majority of respondents in compliance either are at the manager (35%) and director (34%) levels.

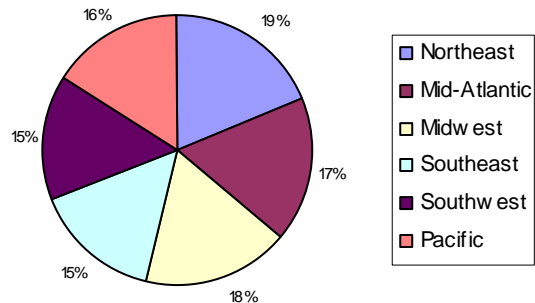
Table 3 What organizational level best describes your current position?	IT	Pct%	Compliance	Pct%
Senior Executive	12	2%	9	2%
Vice President	20	3%	16	4%
Director	161	26%	153	34%
Manager	185	30%	158	35%
Associate/Technician/Staff	176	29%	82	18%
Other	56	9%	38	8%
Total	610	100%	456	100%

Pie Chart 1a and 1b report the US distribution of respondents. Over 19% of respondents in both samples are located in the northeast region. The southwest represents the smallest regional sector for respondent in the IT and compliance samples (13% and 15%, respectively).

Pie Chart 1a
Distribution of the IT sample



Pie Chart 1b
Distribution of the Compliance sample



On average, respondents in IT have over 13 years of experience in the information technology or information security field. Respondents in compliance have almost 12 years of experience, on average, in corporate compliance, regulatory compliance or internal auditing.

Over 53% of respondents in IT report through the CIO organization, and 20% report through the organization’s CTO. About 29% of respondents in the compliance sample, report through the internal auditing department. Over 26% report through the chief compliance officer.

4. Detailed Results

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

Negligence: A junior employee in the human resources department takes his work home to complete it over the weekend. From a remote location, he is granted access to sensitive employee information such as salary levels and performance data. This violates the company’s data security policy.

Table 4a. This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	113	19%	30	7%
Agree	157	26%	64	14%
Unsure	195	32%	113	25%
Disagree	99	16%	158	35%
Strongly disagree	46	8%	91	20%
Total	610	100%	456	100%

Table 4b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	82	13%	73	16%
Agree	169	28%	166	36%
Unsure	104	17%	107	23%
Disagree	190	31%	85	19%
Strongly disagree	65	11%	25	5%
Total	610	100%	456	100%

Table 4c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring. Select top five choices only.	Freq A	Total%	Freq B	Total%
Employee training and awareness	321	53%	289	63%
Perimeter controls (firewalls)	95	16%	19	4%
Database access controls	239	39%	143	31%
Privileged user access controls	238	39%	100	22%
Identity and access management	231	38%	135	30%
Data leak and prevention tools	45	7%	25	5%
Intrusion prevention systems	57	9%	4	1%

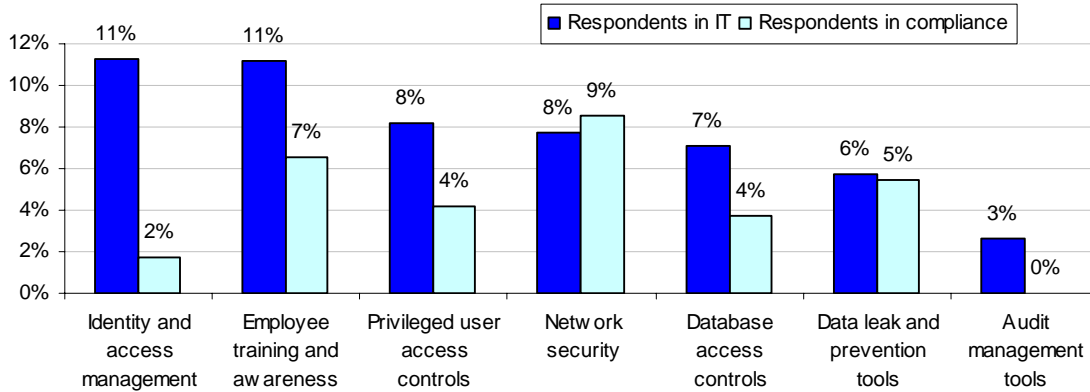
Table 4c - Continued				
Intrusion detection systems	59	10%	7	2%
Event monitoring and management systems	51	8%	4	1%
Audit management tools	59	10%	8	2%
Encryption solutions	314	51%	288	63%
Digital rights management	29	5%	40	9%
Anti-worm, virus, spyware and Trojan solutions	13	2%	2	0%
Incident response plan	14	2%	4	1%
Network security	45	7%	43	9%

Table 4d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Total%	Freq B	Total%
Employee training and awareness	389	64%	319	70%
Perimeter controls (firewalls)	95	16%	19	4%
Database access controls	282	46%	160	35%
Privileged user access controls	288	47%	119	26%
Identity and access management	300	49%	143	31%
Data leak and prevention tools	80	13%	50	11%
Intrusion prevention systems	57	9%	4	1%
Intrusion detection systems	59	10%	7	2%
Event monitoring and management systems	51	8%	4	1%
Audit management tools	75	12%	8	2%
Encryption solutions	314	51%	288	63%
Digital rights management	29	5%	40	9%
Anti-worm, virus, spyware and Trojan solutions	13	2%	2	0%
Incident response plan	14	2%	4	1%
Network security	92	15%	37	8%

Table 4e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	46	8%	36	8%
Agree	164	27%	64	14%
Unsure	115	19%	97	21%
Disagree	218	36%	203	45%
Strongly disagree	67	11%	55	12%
Total	610	100%	455	100%

Bar Chart 7 lists the top seven controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the loss of sensitive information because of employee negligence.

Bar Chart 7
Controls that prevent or reduce negligence
 Percentage change in manual & IT controls over the next 12 to 18 months



Revoking access privileges: An employee decides to terminate her employment. More than one week later, the company has still failed to revoke her access rights to all applications.

Table 5a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	89	15%	62	14%
Agree	199	33%	81	18%
Unsure	67	11%	58	13%
Disagree	190	31%	177	39%
Strongly disagree	65	11%	78	17%
Total	610	100%	456	100%

Table 5b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	67	11%	91	20%
Agree	176	29%	174	38%
Unsure	105	17%	82	18%
Disagree	201	33%	90	20%
Strongly disagree	60	10%	18	4%
Total	609	100%	455	100%

Table 5c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	84	14%	89	20%
Perimeter controls (firewalls)	0	0%	1	0%
Database access controls	128	21%	155	34%
Privileged user access controls	99	16%	74	16%
Identity and access management	452	73%	85	19%
Data leak and prevention tools	6	1%	9	2%
Intrusion prevention systems	20	3%	0	0%

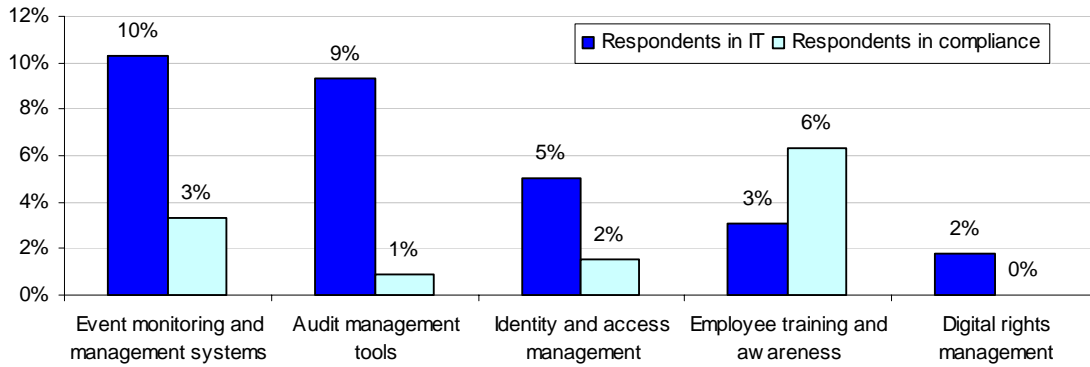
Table 5c – Continued				
Intrusion detection systems	100	16%	1	0%
Event monitoring and management systems	235	38%	74	16%
Audit management tools	142	23%	66	14%
Encryption solutions	9	1%	0	0%
Digital rights management	39	6%	1	0%
Anti-worm, virus, spyware and Trojan solutions	2	0%	4	1%
Incident response plan	1	0%	0	0%
Network security	109	18%	80	18%

Table 5d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	103	17%	118	26%
Perimeter controls (firewalls)	0	0%	1	0%
Database access controls	130	21%	167	37%
Privileged user access controls	100	16%	74	16%
Identity and access management	483	78%	92	20%
Data leak and prevention tools	6	1%	10	2%
Intrusion prevention systems	20	3%	0	0%
Intrusion detection systems	100	16%	1	0%
Event monitoring and management systems	299	48%	89	20%
Audit management tools	200	32%	70	15%
Encryption solutions	10	2%	0	0%
Digital rights management	50	8%	1	0%
Anti-worm, virus, spyware and Trojan solutions	2	0%	4	1%
Incident response plan	1	0%	0	0%
Network security	112	18%	81	18%

Table 5e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	39	6%	23	5%
Agree	176	29%	86	19%
Unsure	106	17%	39	9%
Disagree	234	38%	258	57%
Strongly disagree	55	9%	50	11%
Total	610	100%	456	100%

Bar Chart 8 lists the top five controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce failure in the revocation of privileged access to terminated employees.

Bar Chart 8
Controls that ensure revocation of privileged access rights
 Percentage change in manual & IT controls over the next 12 to 18 months



Data spill: An organization is building a national database of individuals who are using certain sensitive medical products. A personal welcoming email is sent to everyone in the database. By accident, the URL contains the email addresses of all customers in the database (i.e., a data string).

Table 6a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	68	11%	42	9%
Agree	186	30%	88	19%
Unsure	119	20%	127	28%
Disagree	154	25%	143	31%
Strongly disagree	83	14%	56	12%
Total	610	100%	456	100%

Table 6b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	79	13%	65	14%
Agree	185	30%	145	32%
Unsure	130	21%	118	26%
Disagree	177	29%	78	17%
Strongly disagree	39	6%	50	11%
Total	610	100%	456	100%

Table 6c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	71	12%	109	24%
Perimeter controls (firewalls)	157	26%	3	1%
Database access controls	89	15%	8	2%
Table 6c – Continued				
Privileged user access controls	54	9%	4	1%
Identity and access management	70	11%	4	1%
Data leak and prevention tools	179	29%	45	10%

Table 6c – Continued				
Intrusion prevention systems	14	2%	0	0%
Intrusion detection systems	98	16%	0	0%
Event monitoring and management systems	97	16%	15	3%
Audit management tools	56	9%	29	6%
Encryption solutions	194	32%	21	5%
Digital rights management	15	2%	9	2%
Anti-worm, virus, spyware and Trojan solutions	62	10%	0	0%
Incident response plan	4	1%	0	0%
Network security	168	28%	32	7%

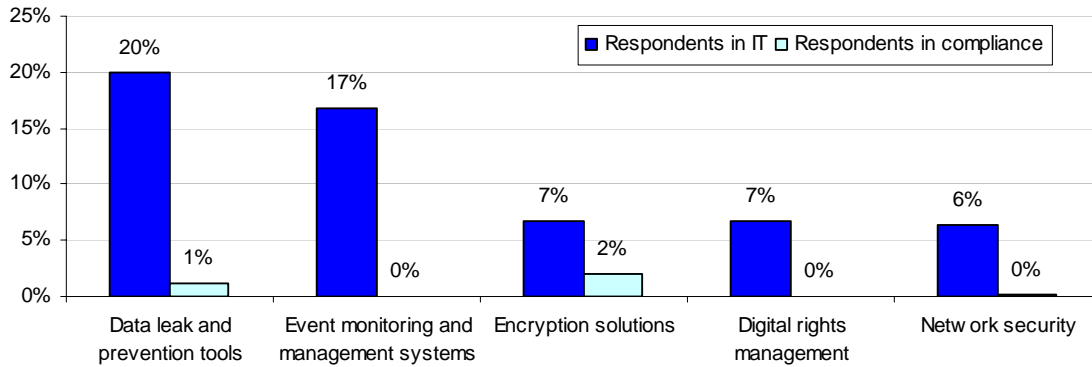
Table 6d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	71	12%	123	27%
Perimeter controls (firewalls)	157	26%	3	1%
Database access controls	96	16%	21	5%
Privileged user access controls	60	10%	5	1%
Identity and access management	75	12%	4	1%
Data leak and prevention tools	301	49%	50	11%
Intrusion prevention systems	16	3%	0	0%
Intrusion detection systems	99	16%	0	0%
Event monitoring and management systems	199	33%	15	3%
Audit management tools	64	10%	35	8%
Encryption solutions	235	39%	30	7%
Digital rights management	56	9%	9	2%
Anti-worm, virus, spyware and Trojan solutions	62	10%	0	0%
Incident response plan	4	1%	0	0%
Network security	207	34%	33	7%

Table 6e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	39	6%	23	5%
Agree	116	19%	90	20%
Unsure	106	17%	171	37%
Disagree	294	48%	128	28%
Strongly disagree	55	9%	47	10%
Total	610	100%	459	100%

Bar Chart 9 lists the top five controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce data spills from uncontrolled Internet or email communications.

Bar Chart 9
Controls that prevent data spills

Percentage change in manual & IT controls over the next 12 to 18 months



Secure backup: An organization sends its backup information to an off-site storage facility operated by a third party. An unprotected backup tape containing sensitive customer information is lost in transit.

Table 7a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	17	3%	32	7%
Agree	89	15%	90	20%
Unsure	54	9%	141	31%
Disagree	341	56%	125	27%
Strongly disagree	109	18%	68	15%
Total	610	100%	456	100%

Table 7b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	102	17%	33	7%
Agree	354	58%	98	21%
Unsure	51	8%	168	37%
Disagree	87	14%	79	17%
Strongly disagree	16	3%	78	17%
Total	610	100%	456	100%

Table 7c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	165	27%	100	22%
Perimeter controls (firewalls)	600	97%	405	89%
Database access controls	261	42%	45	10%
Privileged user access controls	79	13%	7	2%
Identity and access management	51	8%	21	5%
Data leak and prevention tools	8	1%	45	10%
Intrusion prevention systems	254	41%	126	28%

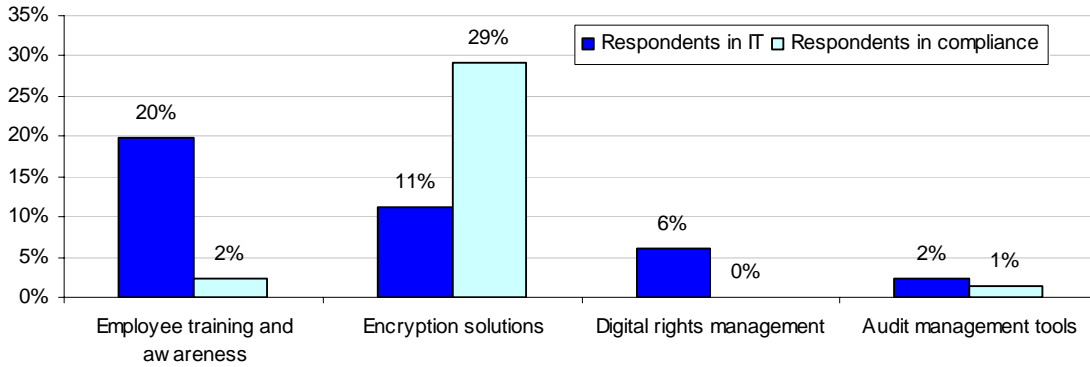
Table 7c – Continued				
Intrusion detection systems	330	53%	89	20%
Event monitoring and management systems	51	8%	4	1%
Audit management tools	81	13%	22	5%
Encryption solutions	436	70%	16	4%
Digital rights management	80	13%	2	0%
Anti-worm, virus, spyware and Trojan solutions	1	0%	4	1%
Incident response plan	110	18%	7	2%
Network security	273	44%	35	8%

Table 7d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	201	32%	100	22%
Perimeter controls (firewalls)	615	99%	441	97%
Database access controls	299	48%	68	15%
Privileged user access controls	79	13%	7	2%
Identity and access management	51	8%	21	5%
Data leak and prevention tools	45	7%	45	10%
Intrusion prevention systems	399	64%	165	36%
Intrusion detection systems	335	54%	90	20%
Event monitoring and management systems	67	11%	4	1%
Audit management tools	180	29%	50	11%
Encryption solutions	457	74%	16	4%
Digital rights management	98	16%	2	0%
Anti-worm, virus, spyware and Trojan solutions	11	2%	4	1%
Incident response plan	110	18%	7	2%
Network security	346	56%	35	8%

Table 7e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	11	2%	19	4%
Agree	55	9%	78	17%
Unsure	234	38%	170	37%
Disagree	237	39%	139	30%
Strongly disagree	73	12%	50	11%
Total	610	100%	456	100%

Bar Chart 10 lists the top four controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk of insecure data backup containing sensitive or confidential customer information.

Bar Chart 10
Controls that prevent insecure data backup
 Percentage change in manual & IT controls over the next 12 to 18 months



Hackers: An IT system’s database containing sensitive credit card information is hacked by criminals. The credit card information is not encrypted.

Table 8a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	17	3%	32	7%
Agree	89	15%	90	20%
Unsure	54	9%	141	31%
Disagree	341	56%	125	27%
Strongly disagree	109	18%	68	15%
Total	610	100%	456	100%

Table 8b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	102	17%	33	7%
Agree	354	58%	98	21%
Unsure	51	8%	168	37%
Disagree	87	14%	79	17%
Strongly disagree	16	3%	78	17%
Total	610	100%	456	100%

Table 8c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	165	27%	100	22%
Perimeter controls (firewalls)	600	97%	405	89%
Database access controls	261	42%	45	10%
Privileged user access controls	79	13%	7	2%
Identity and access management	51	8%	21	5%
Data leak and prevention tools	8	1%	45	10%
Intrusion prevention systems	254	41%	126	28%
Intrusion detection systems	330	53%	89	20%

Event monitoring and management systems	51	8%	4	1%
Audit management tools	81	13%	22	5%
Encryption solutions	436	70%	16	4%
Digital rights management	80	13%	2	0%
Anti-worm, virus, spyware and Trojan solutions	1	0%	4	1%
Incident response plan	110	18%	7	2%
Network security	273	44%	35	8%

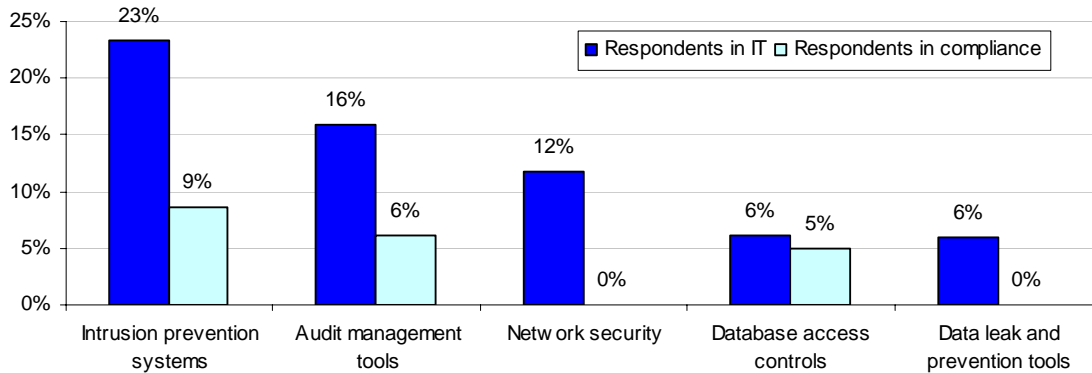
Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	201	32%	100	22%
Perimeter controls (firewalls)	615	99%	441	97%
Database access controls	299	48%	68	15%
Privileged user access controls	79	13%	7	2%
Identity and access management	51	8%	21	5%
Data leak and prevention tools	45	7%	45	10%
Intrusion prevention systems	399	64%	165	36%
Intrusion detection systems	335	54%	90	20%
Event monitoring and management systems	67	11%	4	1%
Audit management tools	180	29%	50	11%
Encryption solutions	457	74%	16	4%
Digital rights management	98	16%	2	0%
Anti-worm, virus, spyware and Trojan solutions	11	2%	4	1%
Incident response plan	110	18%	7	2%
Network security	346	56%	35	8%

The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.	Freq A	Pct%	Freq B	Pct%
Strongly agree	11	2%	19	4%
Agree	55	9%	78	17%
Unsure	234	38%	170	37%
Disagree	237	39%	139	30%
Strongly disagree	73	12%	50	11%
Total	610	100%	456	100%

Bar Chart 11 lists the top five controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk of hackers accessing sensitive or confidential credit card information.

Bar Chart 11
Controls that prevent hackers

Percentage change in manual & IT controls over the next 12 to 18 months



Failure to notify: An organization has a data breach that involves thousands of customer’s records containing sensitive information. The employees who discover the incident fail to escalate this incident to appropriate levels of management. As a result, customers do not receive notification about the breach.

Table 9a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	75	12%	29	6%
Agree	197	32%	129	28%
Unsure	155	25%	135	30%
Disagree	139	23%	94	21%
Strongly disagree	44	7%	69	15%
Total	610	100%	456	100%

Table 9b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	40	7%	30	7%
Agree	112	18%	81	18%
Unsure	183	30%	165	36%
Disagree	201	33%	118	26%
Strongly disagree	74	12%	62	14%
Total	610	100%	456	100%

Table 9c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	389	64%	285	63%
Perimeter controls (firewalls)	55	9%	2	0%
Database access controls	22	4%	25	5%
Privileged user access controls	37	6%	4	1%
Identity and access management	52	9%	7	2%
Data leak and prevention tools	6	1%	2	0%

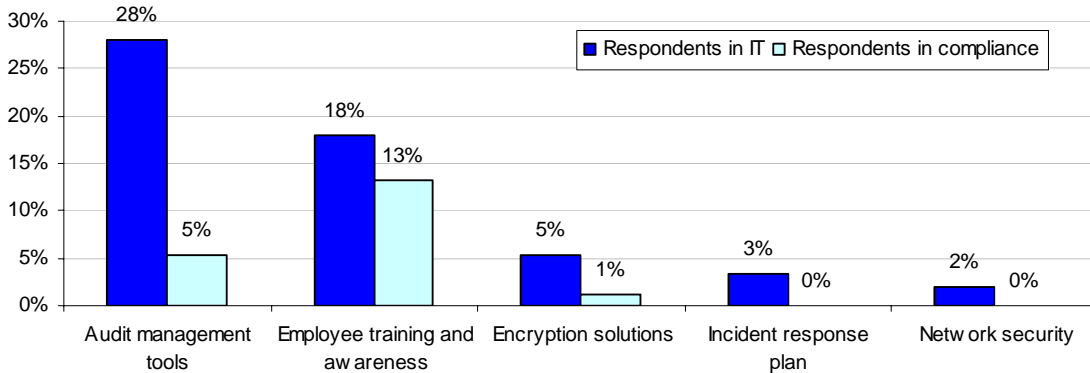
Table 9c – Continued				
Intrusion prevention systems	12	2%	0	0%
Intrusion detection systems	11	2%	0	0%
Event monitoring and management systems	6	1%	9	2%
Audit management tools	14	2%	11	2%
Encryption solutions	124	20%	87	19%
Digital rights management	3	0%	1	0%
Anti-worm, virus, spyware and Trojan solutions	11	2%	2	0%
Incident response plan	12	2%	5	1%
Network security	19	3%	16	4%

Table 9d Please check the controls your organization plans to have over the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	499	82%	345	76%
Perimeter controls (firewalls)	55	9%	2	0%
Database access controls	22	4%	31	7%
Privileged user access controls	37	6%	4	1%
Identity and access management	52	9%	7	2%
Data leak and prevention tools	6	1%	2	0%
Intrusion prevention systems	19	3%	0	0%
Intrusion detection systems	18	3%	0	0%
Event monitoring and management systems	6	1%	9	2%
Audit management tools	185	30%	35	8%
Encryption solutions	156	26%	92	20%
Digital rights management	3	0%	1	0%
Anti-worm, virus, spyware and Trojan solutions	11	2%	2	0%
Incident response plan	32	5%	5	1%
Network security	31	5%	16	4%

Table 9e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	31	5%	40	9%
Agree	177	29%	79	17%
Unsure	163	27%	145	32%
Disagree	172	28%	126	28%
Strongly disagree	67	11%	65	14%
Total	610	100%	455	100%

Bar Chart 12 lists the top five controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk that a data breach is not communicated to breach victims in accordance with various US state laws.

Bar Chart 12
Controls that prevent the failure to notify for data breach
 Percentage change in manual & IT controls over the next 12 to 18 months



Customer turnover: An organization has a data breach that involves thousands of customer records, which triggers mandatory notification to breach victims. As a result, the organization experiences a loss of customers.

Table 10a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	64	11%	59	13%
Agree	165	27%	125	27%
Unsure	228	37%	162	36%
Disagree	109	18%	75	16%
Strongly disagree	43	7%	34	7%
Total	609	100%	455	100%

Table 10b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	12	2%	19	4%
Agree	102	17%	81	18%
Unsure	242	40%	195	43%
Disagree	205	34%	135	30%
Strongly disagree	47	8%	25	5%
Total	608	100%	455	100%

Table 10c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	151	25%	89	20%
Perimeter controls (firewalls)	23	4%	2	0%
Database access controls	40	7%	6	1%
Privileged user access controls	40	7%	9	2%
Identity and access management	19	3%	2	0%
Data leak and prevention tools	91	15%	1	0%
Intrusion prevention systems	11	2%	1	0%

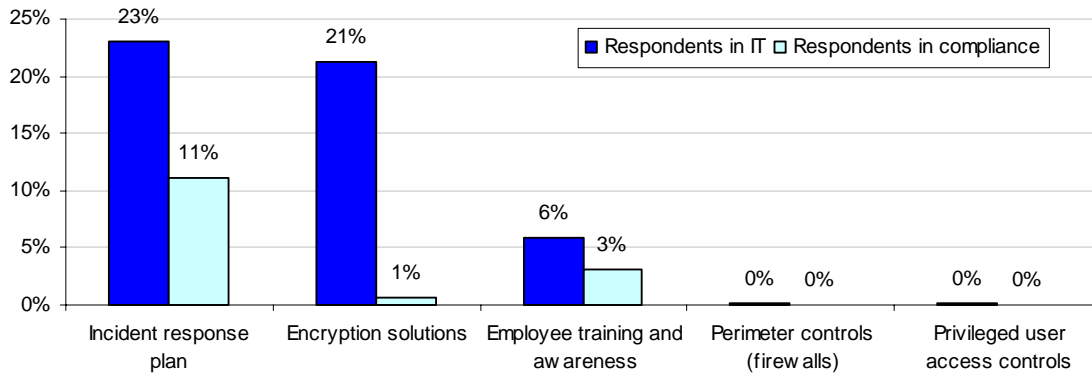
Table 10c – Continued				
Intrusion detection systems	13	2%	0	0%
Event monitoring and management systems	34	6%	49	11%
Audit management tools	15	2%	13	3%
Encryption solutions	374	61%	17	4%
Digital rights management	97	16%	8	2%
Anti-worm, virus, spyware and Trojan solutions	74	12%	7	2%
Incident response plan	258	42%	250	55%
Network security	78	13%	16	4%

Table 10d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	187	31%	103	23%
Perimeter controls (firewalls)	24	4%	2	0%
Database access controls	40	7%	6	1%
Privileged user access controls	41	7%	9	2%
Identity and access management	19	3%	2	0%
Data leak and prevention tools	91	15%	1	0%
Intrusion prevention systems	11	2%	1	0%
Intrusion detection systems	13	2%	0	0%
Event monitoring and management systems	34	6%	55	12%
Audit management tools	15	2%	15	3%
Encryption solutions	504	83%	20	4%
Digital rights management	97	16%	8	2%
Anti-worm, virus, spyware and Trojan solutions	74	12%	7	2%
Incident response plan	399	65%	301	66%
Network security	78	13%	20	4%

Table 10e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	60	10%	39	9%
Agree	207	34%	131	29%
Unsure	182	30%	136	30%
Disagree	125	21%	96	21%
Strongly disagree	35	6%	53	12%
Total	609	100%	455	100%

Bar Chart 13 lists the top five controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk that a data breach will result in the excessive loss, churn or turnover of customers.

Bar Chart 13
Controls that reduce customer churn after a data breach
 Percentage change in manual & IT controls over the next 12 to 18 months



Illegal data transfer: An organization moves employee data from a European country to the United States without complying with European (EU) privacy regulations.

Table 11a. This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	34	6%	41	9%
Agree	114	19%	135	30%
Unsure	283	46%	133	29%
Disagree	156	26%	98	22%
Strongly disagree	23	4%	48	11%
Total	610	100%	455	100%

Table 11b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	11	2%	45	10%
Agree	156	26%	136	30%
Unsure	301	49%	115	25%
Disagree	99	16%	103	23%
Strongly disagree	43	7%	56	12%
Total	610	100%	455	100%

Table 11c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	234	38%	93	20%
Perimeter controls (firewalls)	93	15%	2	0%
Database access controls	83	14%	35	8%
Privileged user access controls	15	2%	45	10%
Identity and access management	23	4%	11	2%
Data leak and prevention tools	16	3%	31	7%
Intrusion prevention systems	35	6%	1	0%
Intrusion detection systems	85	14%	1	0%

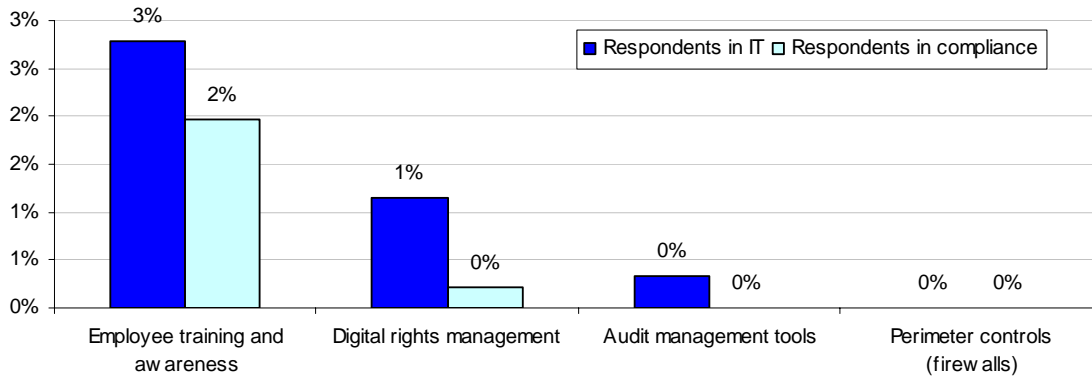
Table 11c – Continued				
Event monitoring and management systems	10	2%	14	3%
Audit management tools	78	13%	22	5%
Encryption solutions	42	7%	76	17%
Digital rights management	88	14%	2	0%
Anti-worm, virus, spyware and Trojan solutions	5	1%	1	0%
Incident response plan	9	1%	2	0%
Network security	15	2%	10	2%

Table 11d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	251	41%	102	22%
Perimeter controls (firewalls)	93	15%	2	0%
Database access controls	83	14%	50	11%
Privileged user access controls	15	2%	49	11%
Identity and access management	23	4%	13	3%
Data leak and prevention tools	16	3%	32	7%
Intrusion prevention systems	35	6%	0	0%
Intrusion detection systems	85	14%	1	0%
Event monitoring and management systems	10	2%	14	3%
Audit management tools	80	13%	22	5%
Encryption solutions	42	7%	77	17%
Digital rights management	95	16%	3	1%
Anti-worm, virus, spyware and Trojan solutions	5	1%	1	0%
Incident response plan	9	1%	2	0%
Network security	15	2%	18	4%

Table 11e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	31	5%	34	7%
Agree	87	14%	69	15%
Unsure	309	51%	217	48%
Disagree	137	22%	90	20%
Strongly disagree	46	8%	45	10%
Total	610	100%	455	100%

Bar Chart 14 lists the to four controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk that the transfer of personal information from Europe to the US does not comply with the trans-border dataflow requirements of the EU privacy directive.

Bar Chart 14
Controls that prevent illegal data transfer
 Percentage change in manual & IT controls over the next 12 to 18 months



Too much PII: The auditors require a company to perform an inventory of all the personally identifiable information (PII) it collects and uses. However, the company is unable to complete this task within a reasonable time period because of the proliferation of PII to a very large number of systems.

Table 12a This type of incident can happen in my organization.	Freq A	Pct%	Freq B	Pct%
Strongly agree	108	18%	97	21%
Agree	305	50%	119	26%
Unsure	43	7%	102	22%
Disagree	109	18%	103	23%
Strongly disagree	45	7%	34	7%
Total	610	100%	455	100%

Table 12b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Pct%
Strongly agree	41	7%	70	15%
Agree	109	18%	89	20%
Unsure	55	9%	109	24%
Disagree	205	34%	119	26%
Strongly disagree	199	33%	68	15%
Total	609	100%	455	100%

Table 12c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.	Freq A	Pct%	Freq B	Total%
Employee training and awareness	194	31%	277	61%
Perimeter controls (firewalls)	25	4%	2	0%
Database access controls	187	30%	69	15%
Privileged user access controls	33	5%	19	4%
Identity and access management	32	5%	18	4%
Data leak and prevention tools	142	23%	41	9%

Table 12c – Continued				
Intrusion prevention systems	55	9%	3	1%
Intrusion detection systems	32	5%	5	1%
Event monitoring and management systems	31	5%	7	2%
Audit management tools	54	9%	47	10%
Encryption solutions	15	2%	6	1%
Digital rights management	1	0%	0	0%
Anti-worm, virus, spyware and Trojan solutions	6	1%	1	0%
Incident response plan	34	5%	3	1%
Network security	92	15%	13	3%

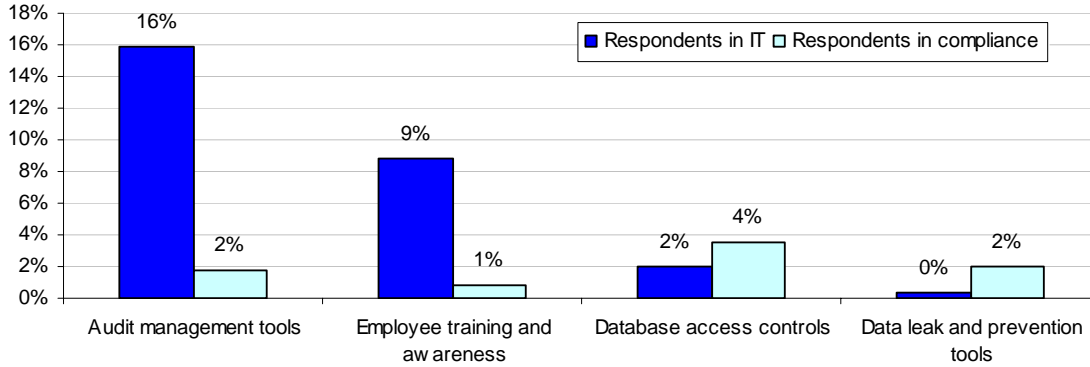
Table 12d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	245	40%	281	62%
Perimeter controls (firewalls)	25	4%	2	0%
Database access controls	196	32%	85	19%
Privileged user access controls	33	5%	19	4%
Identity and access management	32	5%	18	4%
Data leak and prevention tools	142	23%	50	11%
Intrusion prevention systems	55	9%	13	3%
Intrusion detection systems	32	5%	15	3%
Event monitoring and management systems	31	5%	27	6%
Audit management tools	150	25%	55	12%
Encryption solutions	15	2%	7	2%
Digital rights management	1	0%	0	0%
Anti-worm, virus, spyware and Trojan solutions	6	1%	1	0%
Incident response plan	34	6%	3	1%
Network security	92	15%	15	3%

Table 12e The likelihood our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	31	5%	67	15%
Agree	115	19%	92	20%
Unsure	361	59%	138	30%
Disagree	81	13%	100	22%
Strongly disagree	22	4%	58	13%
Total	610	100%	455	100%

Bar Chart 15 lists the top four controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk that an organization would collect an excessive amount of personally identifiable information (and find it nearly impossible to perform a data inventory of PII).

Bar Chart 15
Controls that limit excessive PII

Percentage change in manual & IT controls over the next 12 to 18 months



Over privileged users: A compliance audit reveals that many system users have too much access to sensitive or confidential information including sensitive data about customers.

Table 13a This type of incident can happen in my organization.		Freq A	Pct%	Freq B	Pct%
Strongly agree		102	17%	76	17%
Agree		243	40%	145	32%
Unsure		98	16%	88	19%
Disagree		139	23%	119	26%
Strongly disagree		27	4%	28	6%
Total		609	100%	456	100%

Table 13b My organization has the controls to prevent or reduce the likelihood of this type of incident from occurring.		Freq A	Pct%	Freq B	Pct%
Strongly agree		47	8%	56	12%
Agree		130	21%	82	18%
Unsure		96	16%	124	27%
Disagree		238	39%	125	27%
Strongly disagree		99	16%	69	15%
Total		610	100%	456	100%

Table 13c Please check the controls your organization has <u>today</u> to prevent or reduce the likelihood of this type of incident from occurring.		Freq A	Pct%	Freq B	Total%
Employee training and awareness		198	32%	199	44%
Perimeter controls (firewalls)		9	1%	1	0%
Database access controls		183	30%	130	29%
Privileged user access controls		177	29%	156	34%
Identity and access management		235	39%	303	66%
Data leak and prevention tools		52	9%	46	10%
Intrusion prevention systems		10	2%	2	0%
Intrusion detection systems		99	16%	1	0%

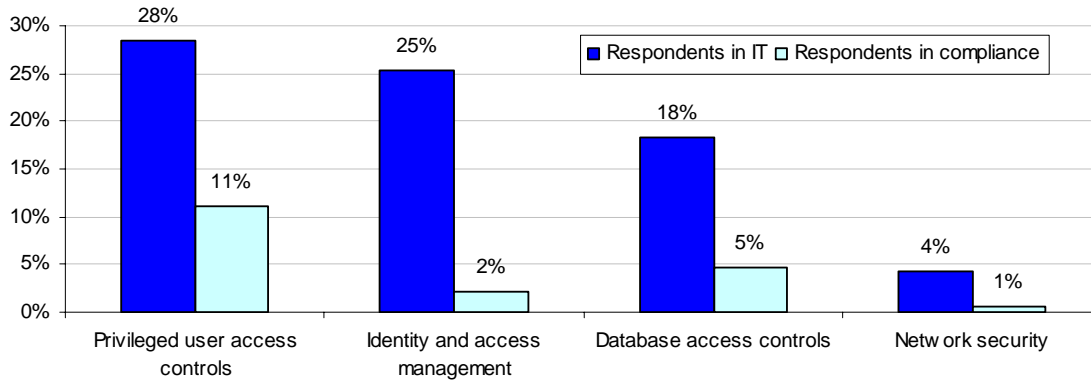
Table 13c – Continued				
Event monitoring and management systems	69	11%	50	11%
Audit management tools	78	13%	25	5%
Encryption solutions	41	7%	4	1%
Digital rights management	60	10%	2	0%
Anti-worm, virus, spyware and Trojan solutions	27	4%	0	0%
Incident response plan	77	13%	3	1%
Network security	43	7%	62	14%

Table 13d Please check the controls your organization plans to have within the next 12 to 18 months to prevent or reduce the likelihood of this type of incident from occurring.				
	Freq A	Pct%	Freq B	Total%
Employee training and awareness	198	32%	200	44%
Perimeter controls (firewalls)	9	1%	1	0%
Database access controls	295	48%	151	33%
Privileged user access controls	350	57%	207	45%
Identity and access management	390	64%	313	69%
Data leak and prevention tools	52	9%	50	11%
Intrusion prevention systems	10	2%	3	1%
Intrusion detection systems	99	16%	1	0%
Event monitoring and management systems	75	12%	54	12%
Audit management tools	89	15%	30	7%
Encryption solutions	41	7%	4	1%
Digital rights management	60	10%	2	0%
Anti-worm, virus, spyware and Trojan solutions	27	4%	0	0%
Incident response plan	77	13%	3	1%
Network security	69	11%	65	14%

Table 13e The likelihood that our organization will have this type of incident will increase over the next 12 to 18 months.				
	Freq A	Pct%	Freq B	Pct%
Strongly agree	89	15%	65	14%
Agree	145	24%	93	20%
Unsure	199	33%	135	30%
Disagree	138	23%	98	21%
Strongly disagree	39	6%	65	14%
Total	610	100%	456	100%

Bar Chart 16 lists the top four controls and IT security solutions that respondents are likely to implement over the next 12 to 18 months to prevent or reduce the risk that system users have too much access rights to sensitive or confidential information (over privilege).

Bar Chart 16
Controls that limit over privileged users
 Percentage change in manual & IT controls over the next 12 to 18 months



5. Caveats

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 of contact information and the degree to which the list is representative of individuals who are information security practitioners. Compensation was provided to ensure that respondents completed the survey task in a short holdout period. While compensation was held to a nominal amount, we acknowledge potential bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses 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.

6. Conclusion

Our research findings suggest that both IT practitioners and compliance professionals are uncertain and insecure about their organization's ability to prevent or curtail the loss or theft of information about customers, employees and other individuals. It appears that respondents in IT hold a more pessimistic view about their organization's existing state of control and security than individuals in corporate compliance or internal audit. This finding is somewhat disconcerting given that IT practitioners are usually the first line of defense against improper or illegal use of sensitive personal information.

These observations are preliminary. We believe further research is needed regarding the use of database security as well as the controls necessary to secure data at rest. If you have questions

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

About Ponemon Institute, LLC

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions. For more information, please visit <http://www.ponemon.org>.