

Sponsored by



Independently Conducted by



Presents

**2008 Study on the
Uncertainty of Data Breach Detection**

Report of IT Practitioners in the United States

Published by Ponemon Institute LLC

June 2008



2008 Study on the Uncertainty of Data Breach Detection in the United States

Executive Summary by Larry Ponemon June 2008

A recent data breach involving Lending Tree, a mortgage lender, illustrates the risk posed by the malicious insider. According to reports of the breach, outside loan companies may have accessed information, including Social Security numbers between October 2006 and early 2008 and used this information to market their own mortgages to Lending Tree customers. It is believed that several former employees may have shared their confidential passwords with lenders that were not approved by the company. It is unknown how many consumer records were compromised.

Mainframe data security has become a critical IT issue. Typically, organizations address this risk by locking down applications to keep unauthorized outside users from accessing them. What this approach does not address is the threat of the negligent or malicious insider who is authorized to access an organization's sensitive information. Research has shown that the biggest data security threat organizations face is internal—both negligent and malicious.

Data breach notification laws and privacy regulations require organizations to inform victims of a data breach in a timely manner. These laws have placed increased importance on an organization's ability to determine the cause of the data breach and individuals affected. However, according to respondents very few companies own or use tools that could possibly be used to detect, analyze or deter inappropriate activities caused by insiders.

Understanding precisely whose personal data has been compromised can be equally important for an organization's trusted relationship with its customers. First, the process of notifying every customer of a data breach that perhaps involved only a portion of these individuals can be an unnecessary and major expense. Second, it demonstrates that the organization was not fully capable of understanding what personal data was at risk when the breach occurred. This uncertainty reflects poorly on how competent the organization is in understanding how personal information is used throughout the enterprise. Ultimately this perception could affect customer loyalty and trust.

Compuware Corporation and Ponemon Institute, LLC are pleased to report the results of the *2008 Study on the Uncertainty of Data Breach Detection*. According to 75 percent of respondents, their organizations have had data breaches caused by negligent insiders and 26 percent had a breach caused by a malicious insider. The purpose of this global study is to understand how organizations in the U.S., UK, France and Germany can detect a breach and then gather all the facts to make informed decisions about how to respond to the incident. Results of the UK, France and Germany studies are presented in separate reports.

We surveyed more than 1,112 IT practitioners with an average of almost nine years of overall experience with backgrounds in the analysis and/or response to privacy breaches. Key demographics for survey respondents are summarized at the conclusion of this report.

Our survey instrument encompassed the following issues concerning the management of the data breach event from the perspective of corporate IT practitioners:

What do IT practitioners believe are the most likely causes of data breaches in their organizations?

- Was the organization able to determine the root cause of the data breach?
- How did the organization obtain facts about the data breach?
- What facts are most important to understanding the cause of the breach?

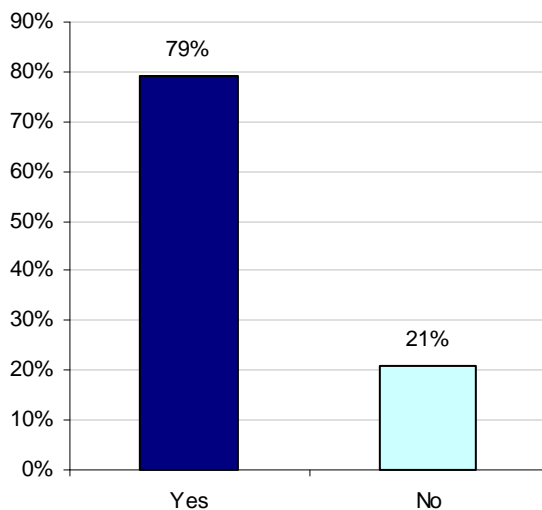
- What tools or techniques were used to determine the cause of the breach?
- What tools do organizations need to deter breaches?
- Who is accountable for detecting and responding to a breach?

Key Findings

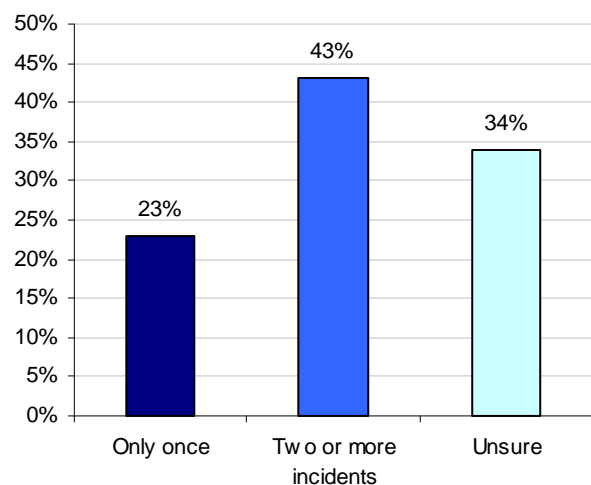
The most salient findings from the study are presented below.

The likelihood of having a data breach is significant and it may occur more than once. As shown in Bar Chart 1a, 79 percent of IT practitioners in the United States report that their organization has experienced one or more data breaches involving the loss or theft of information about individuals such as consumer data, customer information, employee records, and so forth. Of those who have experienced a breach, 43 percent say that their companies had two or more data breach incidents sometime within the past 24 months (Bar Chart 1b). Another 34 percent state they are unsure about the frequency of data breaches occurring during this two year period.

Bar Chart 1a
Has your organization experienced one or more data breaches?



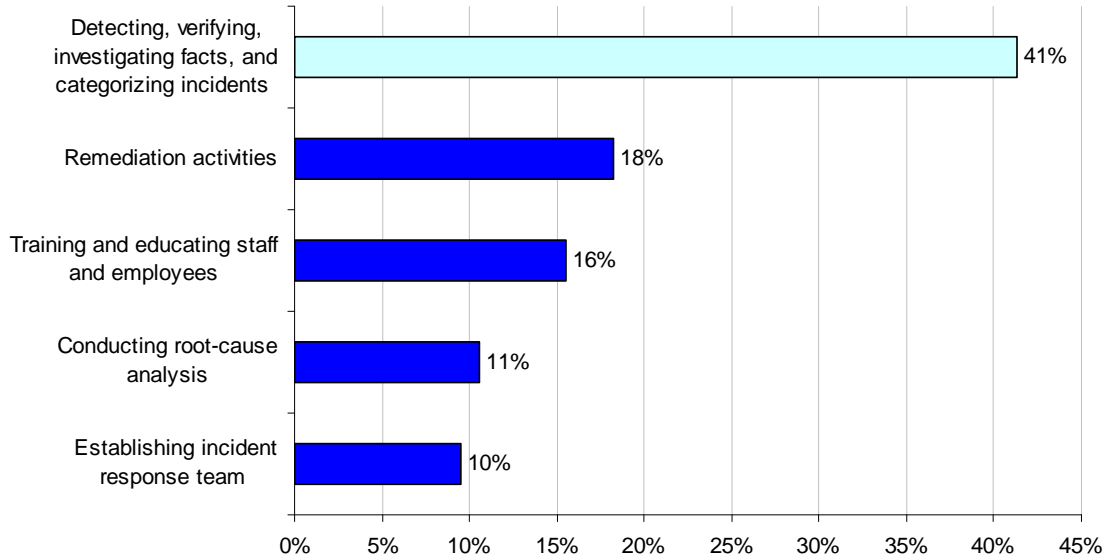
Bar Chart 1b
How many data breaches occurred within the past 24 months?



Primarily, IT practitioners detect, verify, investigate and categorize data breach incidents.

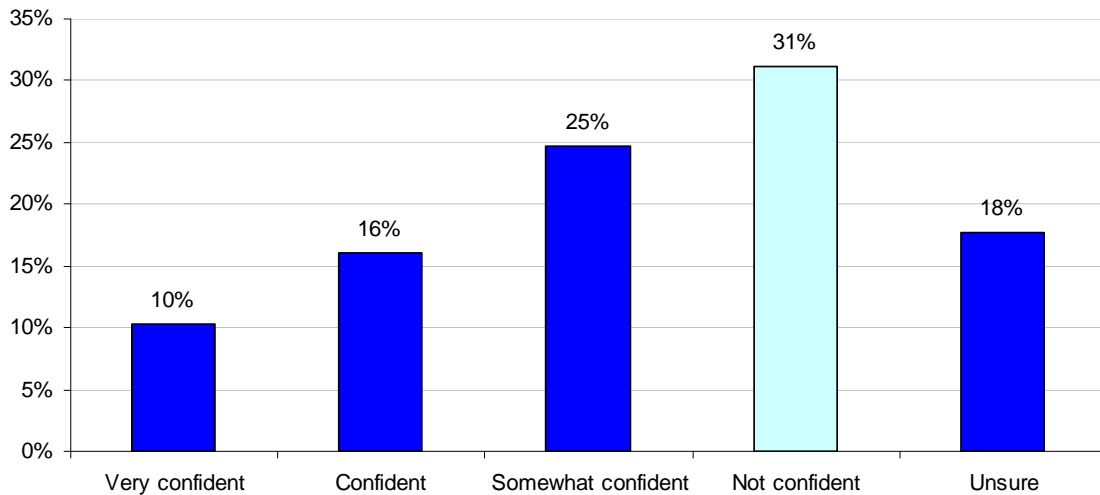
Bar Chart 2 reports the top five responses concerning respondents' involvement in their organization's data breach incidents. As shown below, detecting, verifying, investigating facts and categorizing incidents are the activities these individuals are most involved in following a breach, according to 41 percent of respondents. The second activity concerned remediation of problems identified.

Bar Chart 2
How were you involved? Top five answers



IT practitioners are not confident about their organization’s ability to detect the loss or theft of sensitive or confidential information. When asked how confident they are that all data breaches involving the loss or theft of personal information will be detected, only 10 percent are very confident. Thirty-one percent are not confident and 18 percent are unsure. This result is corroborated by 34 percent who are uncertain about the frequency of data breach incidents (see Bar Chart 1b).

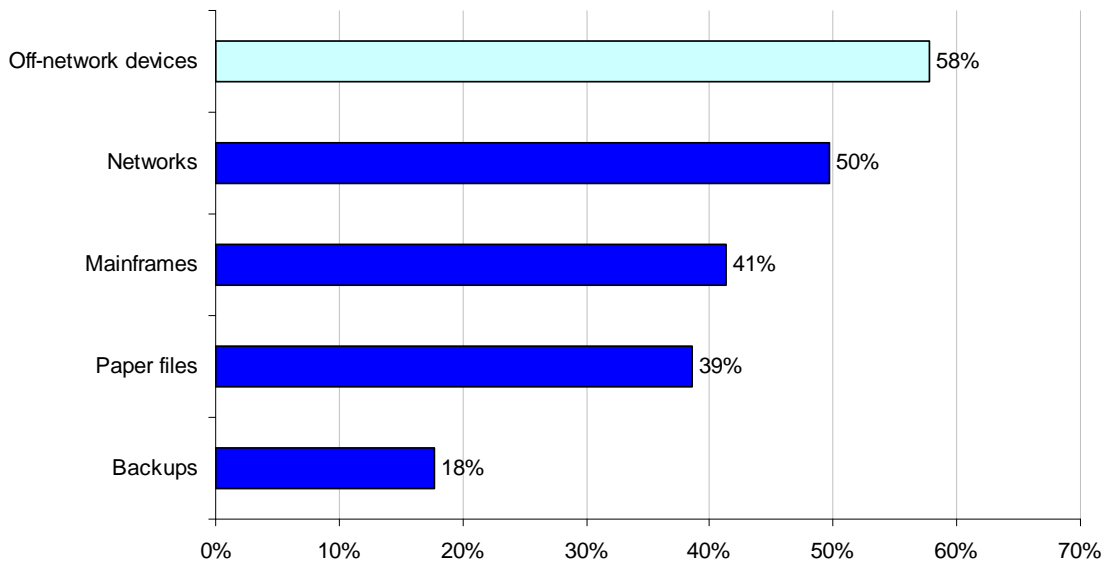
Bar Chart 3
How confident are you that all data breaches involving the loss or theft of personal information will be detected within your organization?



The cause of data breaches and the IT environment where data breaches occur are linked. According to Bar Chart 4, IT practitioners report that off-network devices--such as laptop

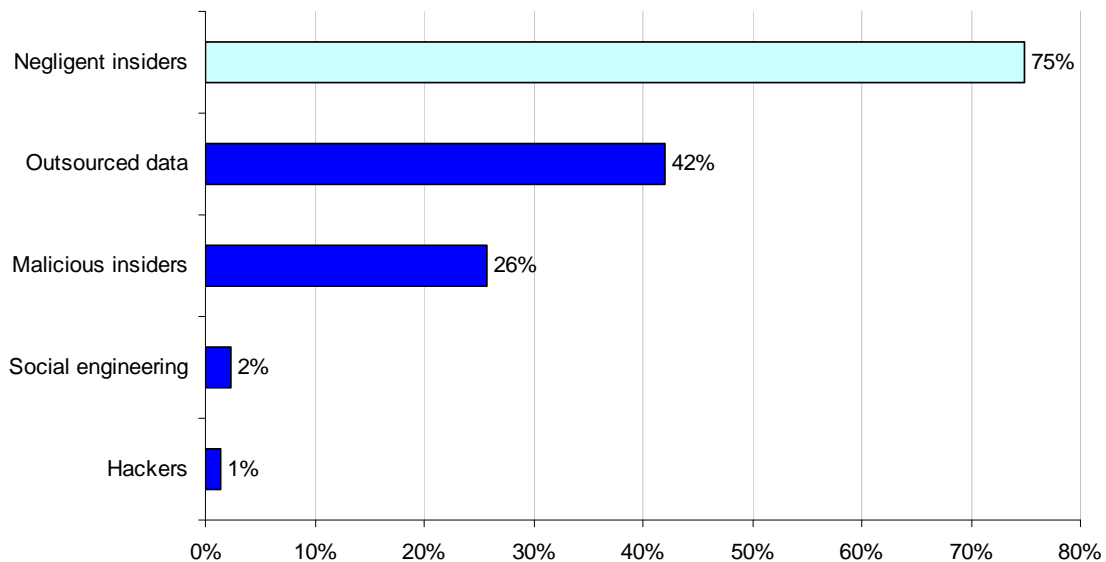
computers, PDAs and memory sticks--and networks are most vulnerable, followed by mainframes.

Bar Chart 4
IT environment where data breaches occur



When looking at the cause of data breach by individuals, the top three reasons shown in Bar Chart 5 are negligent insiders; outsourced data to vendors and other third parties; and malicious insiders. In light of mobility and convenience, organizations are allowing remote access to corporate information assets. This expansion of access rights is likely to increase the risks associated with negligent or malicious employees, temporary employees and contractors.

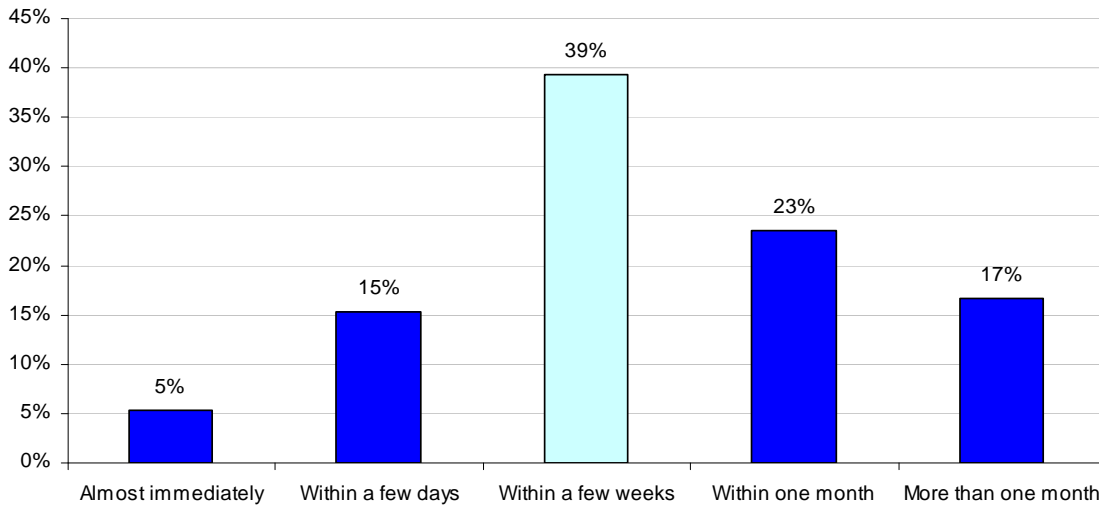
Bar Chart 5
What are the most likely causes of data breach?



Notification of victims is considered important and generally occurs within a few weeks.

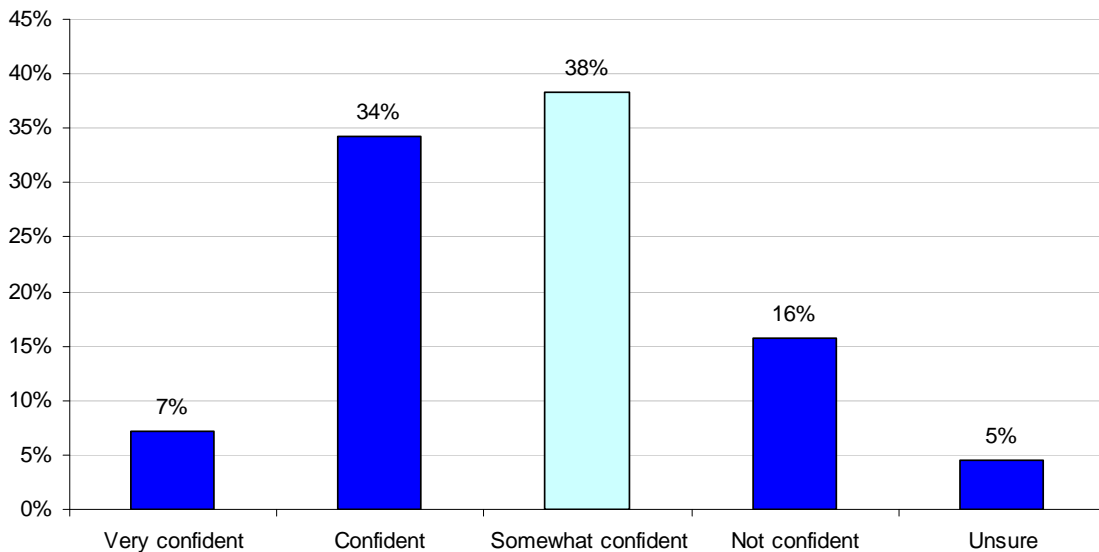
According to the survey, 53 percent of participants in our study report that the data breach incident required the organization to notify possible victims after the event (as required by a majority of US state laws). While 77 percent consider quick notification to be important, Bar Chart 6 shows that only 20 percent sent notifications within a few days after discovering the incident.

Bar Chart 6
How long after discovering the data breach are victims notified?



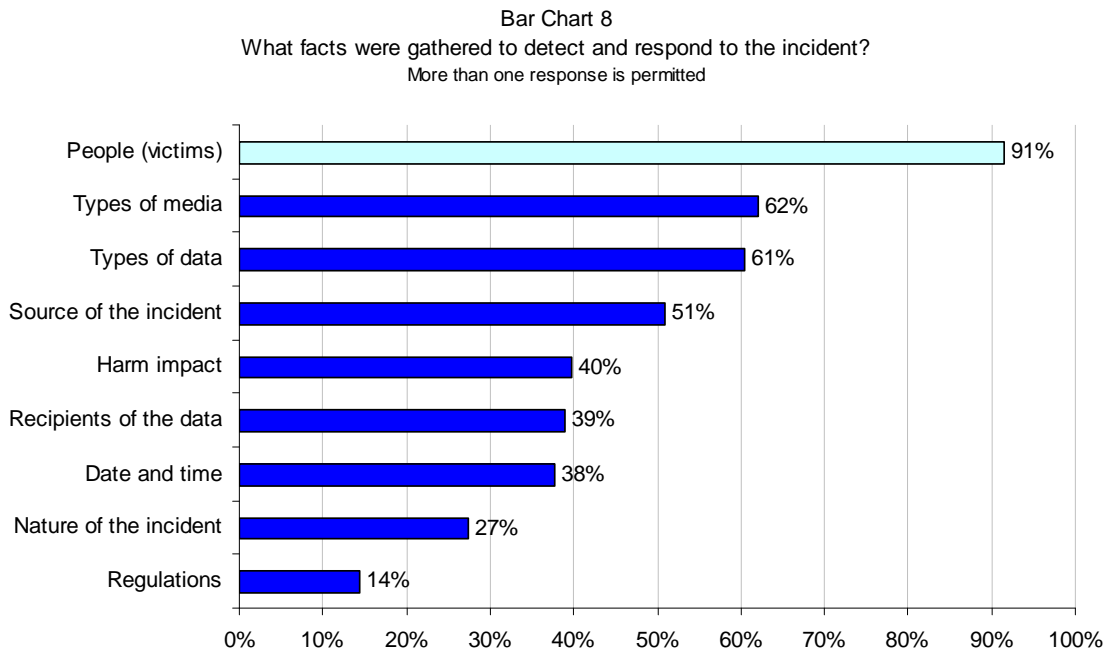
IT practitioners are not very confident of their ability to learn all the facts about the data breach. It's very important to understand not only how a breach occurred, but also to be able to take the necessary steps so the breach doesn't occur again.

Bar Chart 7
How confident are you that all the facts about the breach have been obtained?



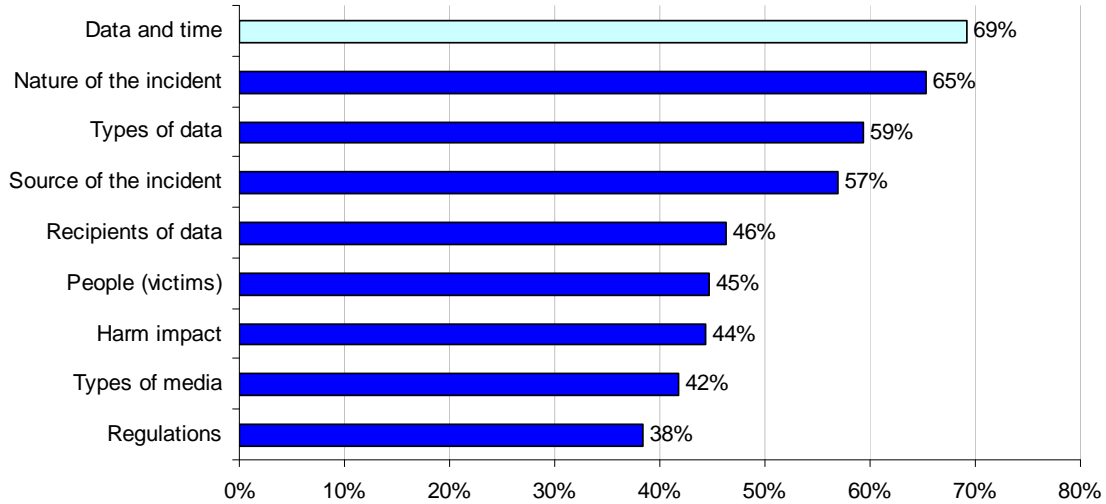
As shown in Bar Chart 7, only 7 percent were very confident and 34 percent confident about their organization's ability to determine root causes of the breach incident.

IT practitioners gather information about the people harmed by the breach event (a.k.a. victims) in order to detect and respond to the data breach. In Bar Chart 8, IT practitioners cite the following as the primary facts they gathered to detect and respond to data breach incidents: people whose information was lost or stolen (91 percent), types of files or data-bearing electronic devices lost or stolen (62 percent), types of information (i.e. customer, employee or consumer at 61 percent), source of the incident (i.e. privileged users, general employees, contractors and/or IT glitches that caused the event at 51 percent) and impact or harm resulting from the data breach (40 percent).



However, as noted in Bar Chart 9, when asked which facts are most important (i.e., very important or important) to understanding root causes, respondents report the following: date and time of the incident, nature of the incident (negligence or criminal intent), types of information lost or stolen, source of the incident and recipients of the information. Regulatory and legal requirements are considered less important.

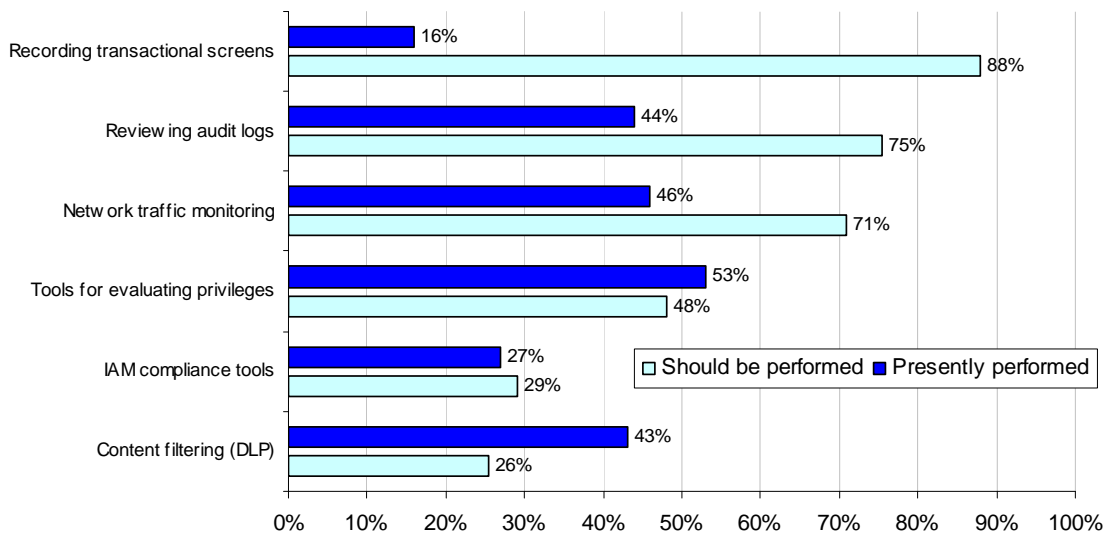
Bar Chart 9
 Very important or important to understanding the cause of the data breach incident
 More than one response is permitted



Although somewhat confident they can learn all the facts, IT practitioners would use different tools and techniques to investigate.

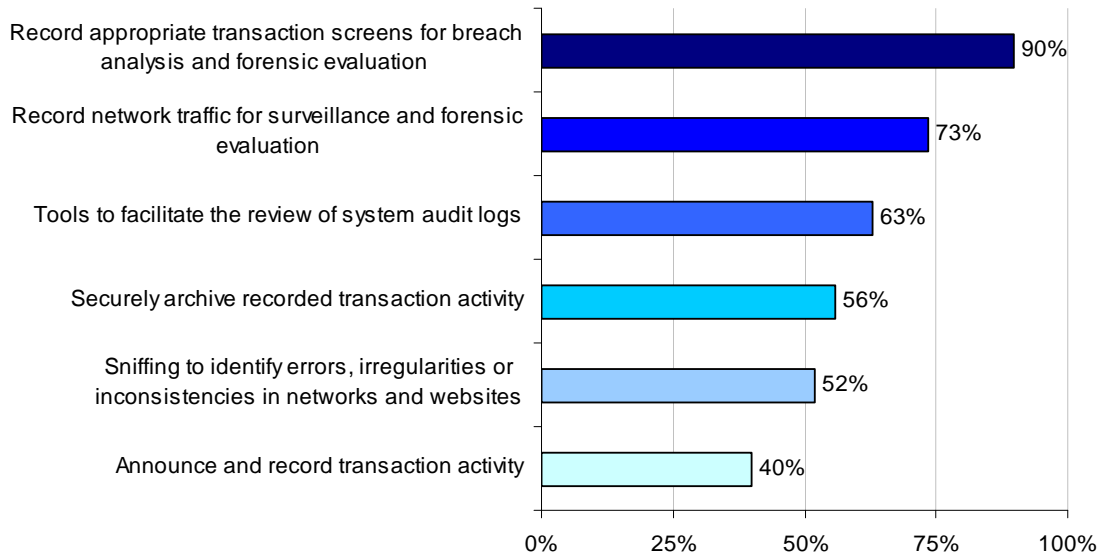
As shown in Bar Chart 10, the tools and techniques used to obtain facts about the data breach are not the same ones they perceive should be used. According to results presented in Bar Chart 10, an overwhelming majority (88 percent) believe that recording transaction screens for breach analysis is a technique that should be used to properly investigate the breach. In sharp contrast, only 16 percent state that their organizations presently record transaction screens.

Bar Chart 10
 What organizations are doing and not doing to perform a root cause analysis



Furthermore, 90 percent of respondents said that recording appropriate transaction screens for breach analysis and forensic evaluation would serve as a deterrent to potential future data breach incidents (Bar Chart 11).

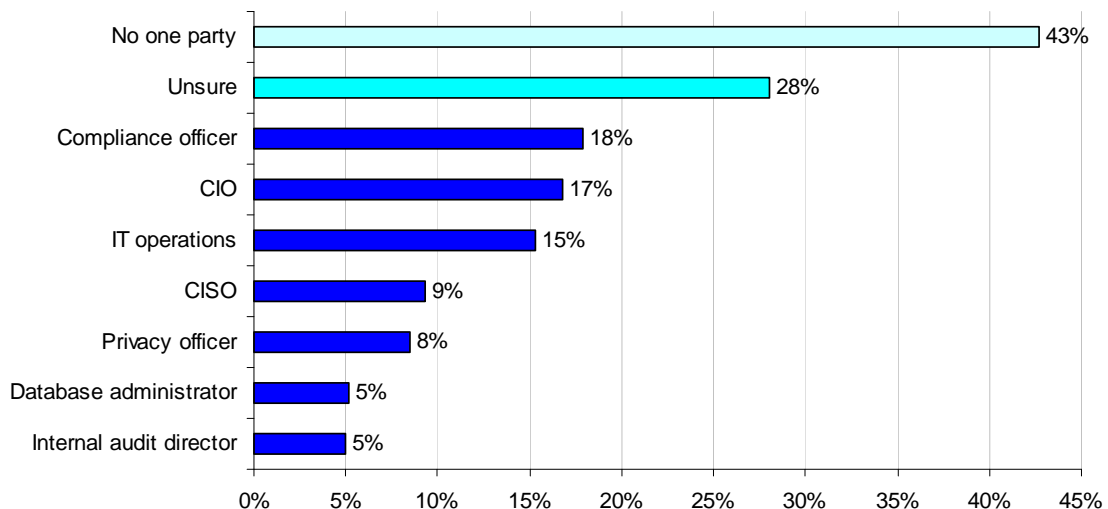
Bar Chart 11
What tools or techniques do you believe could serve as a deterrent to potential future data breach incidents? Top six responses



Who is responsible for detecting and responding to a data breach?

Over 43 percent of IT practitioners report that no one in their organization is accountable for data breach management. Another 23 percent state they are unsure who is responsible. This obvious lack of accountability can have a negative affect not only on detecting data breaches but preventing them as well.

Bar Chart 12
Who is responsible for detecting and responding to data breach incidents?
More than one response is permitted



A lack of leadership in data breach management could explain respondents' lack of confidence in the ability to detect data breaches. It could also contribute to the misallocation of resources and as a result not having the appropriate tools to detect and investigate data breaches. As shown above, IT practitioners believe they would use different tools and techniques to better understand the cause of the data breach. Better understanding of the root cause would lead to better approaches to deterring and preventing data breaches in the future.

Comparison of US Practices to Three European Countries

Are there significant differences in how organizations in the U.S. and those in three European countries – namely, France, United Kingdom and Germany – are addressing the problems associated with data breaches? This research was conducted in four countries to better understand how each country addresses the detection and prevention of data breaches.

As shown in Bar Chart 13a, the US and France have the most reported data breaches but the UK, by a slightly greater percentage, has the highest percentage of two or more breaches (Bar Chart 13b). IT practitioners in the US are more uncertain about how many data breaches their organizations have had followed by France.

Table 13a
At least one or more data breach incidents by country

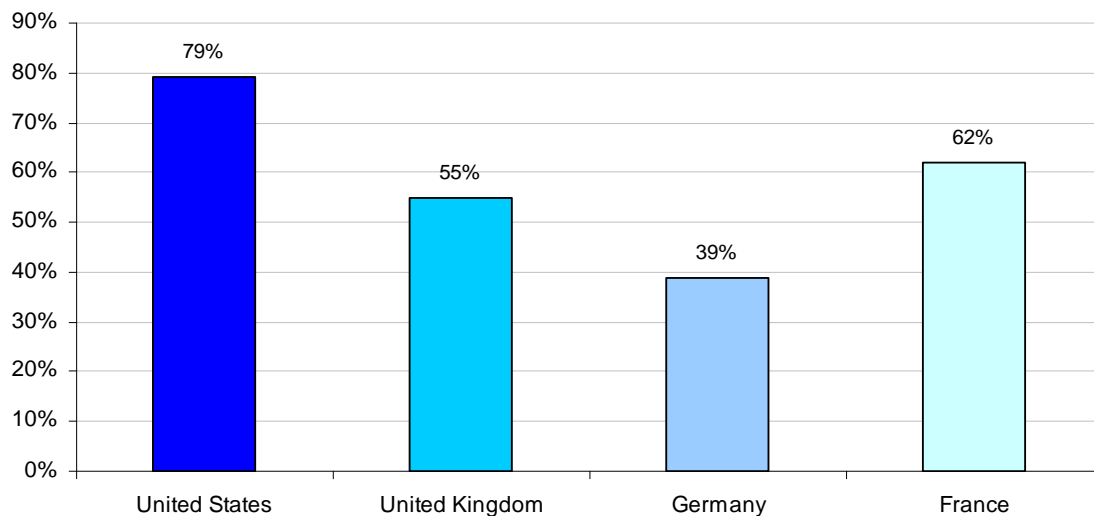
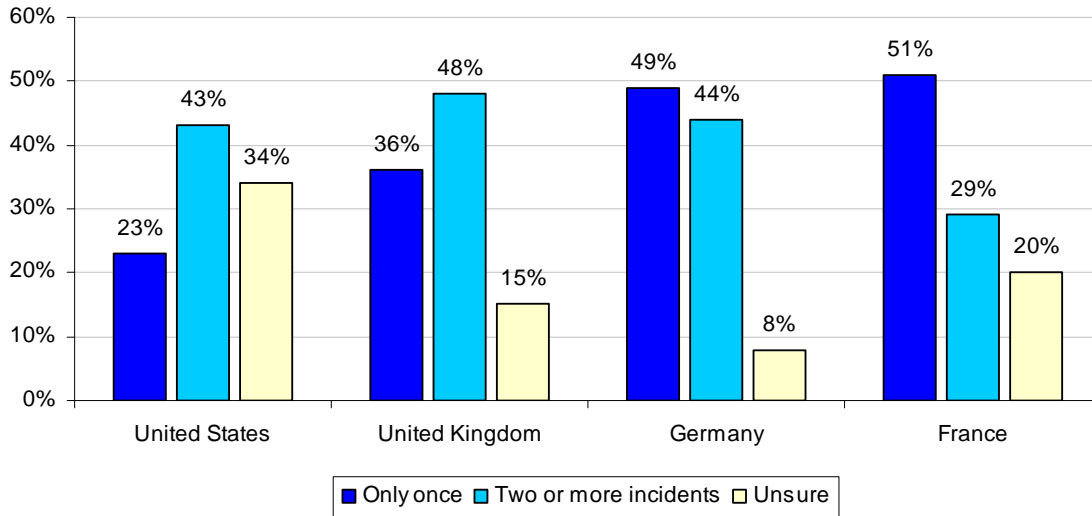
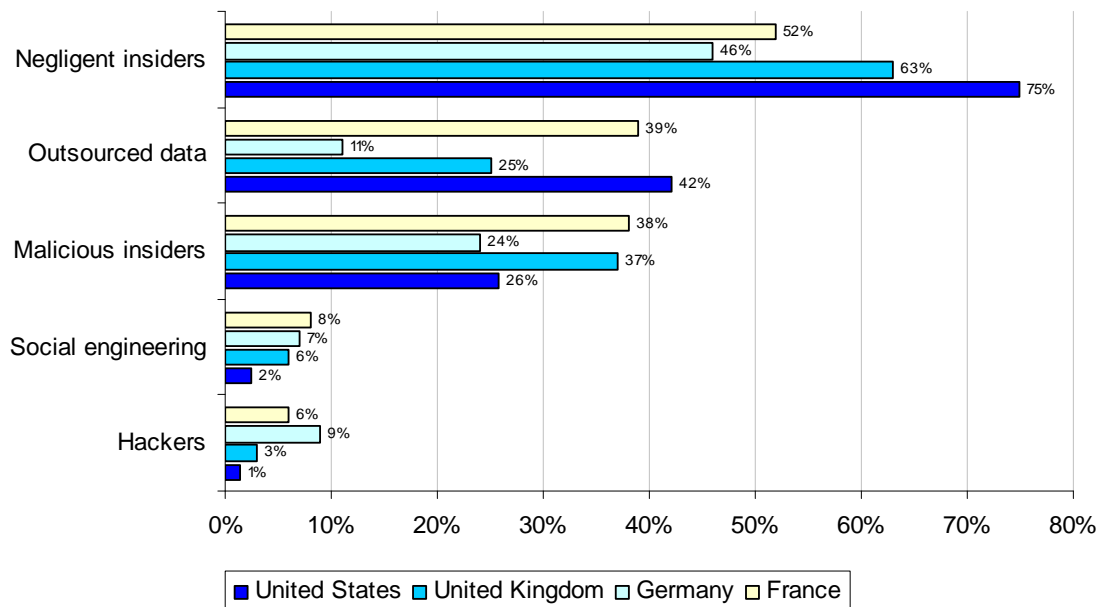


Figure 13b
Frequency of data breach incidents by country



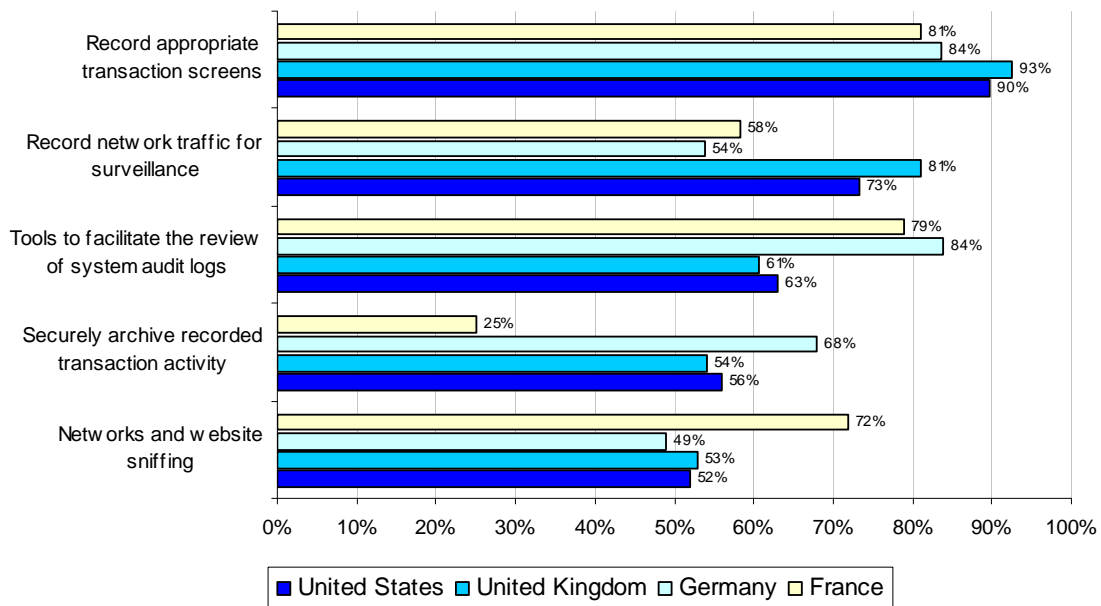
Bar Chart 14 provides an interesting breakdown of the most likely causes of a data breach. In all countries, negligent insiders are the number one cause of data breaches throughout the world. Of least concern are hackers and social engineers. Concern about insider negligence seems to be prompting many IT practitioners to become involved in training and education activities as shown in Bar Chart 2 in each country report.

Bar Chart 14
Most likely causes of a data breach by country



Bar Chart 15 presents the tools and techniques most favored to deter a data breach. It is consistent in all countries that recording appropriate transaction screens is the number one deterrent to a data breach. Also favored by France and Germany are tools to facilitate the review of system audit logs. The UK and US believe recording network traffic for surveillance is a possible deterrent to data breaches.

Bar Chart 15
Tools or technique that could serve as a deterrent to future data breach incidents



Recommendations

The findings of this study indicate that data breaches continue to be a major problem for organizations. According to the Privacy Rights Clearinghouse, since January 2005 to the present 225,786,657 records containing sensitive personal information have been lost or stolen. Unfortunately, as hard as it seems to prevent records from being lost or stolen they are often hard to detect.

The findings from this study indicate a serious governance issue—with no one function accountable or responsible for the management of a data breach detection, investigation and response program. In turn, without being able to understand the root cause of a data breach how can organizations prevent future incidents from occurring? Based on the results of the study, we recommend the following actions:

- Establish a data breach management governance framework. Accountability is required to detect data breaches and prevent future incidents.
- Establish criteria including scope, jurisdiction, type of data, source of breach (criminal vs. negligent insider) to determine which incidents require notification and how quickly notification should occur.
- Include plans to determine the scope of the breach. Limiting notification to the affected individuals not only saves on notification costs, but it also preserves your reputation.
- Plan and execute different scenarios to determine whether you have the appropriate forensic tools to quickly investigate a breach and determine its source. The results of your investigation should include an analysis of the security and archiving of forensic information

to ensure a proper chain of evidence is met. Repeating this analysis on a recurring basis should ensure that you have appropriate evidence if needed.

- Prevent future data breaches by understanding the root causes of current data breaches. Consider options that will help deter breaches. Bar chart 10 identifies what respondents felt would be most useful in investigating and deterring breaches. Ninety percent of respondents indicated that recording authorized user activity and their access to sensitive data would be an effective deterrent. Notifying users of this monitoring may be required but will also increase the deterrence factor.
- Review your data access security to include portable devices, i.e. thumb drives, CDs, etc. Off-network devices and networks are considered most at risk and are most vulnerable to what are considered the causes of breaches—negligent insiders and outsourced data.
- Implement tools and techniques to detect and deter a breach. IT practitioners report that information about the data breach victim are the facts most often missing when investigating a data breach, which makes it difficult to respond in a timely manner as required by data breach notification laws.

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 security 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 17,895 adult-aged individuals who reside within the United States was used to recruit participants to this web survey.¹ Our randomly selected sampling frame was selected from three national mailing lists of IT professionals.

In total, 1,163 respondents completed their survey results during within a eight-day research period. Of returned instruments, 51 survey forms were rejected because of reliability checks. A total of 1,112 surveys were used as our final sample. This sample represents a 6.2 percent net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is ≤ 3 percent.

¹ Respondents were given nominal compensation to complete all survey questions.

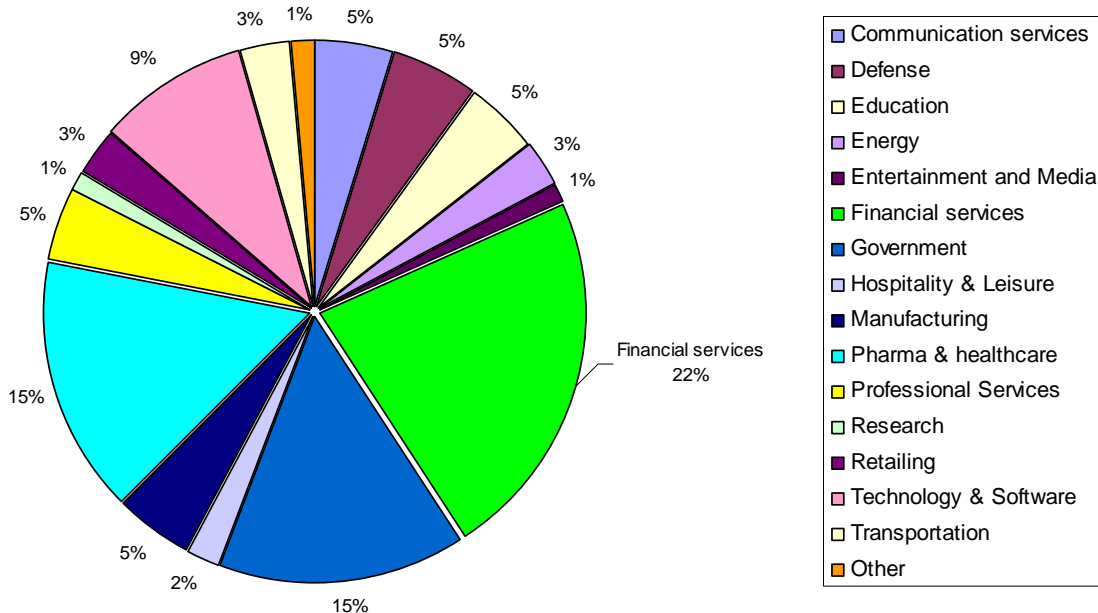
Over 92 percent of respondents completed all survey items within 10 minutes. Following are key demographics and organizational characteristics for U.S. respondents. Table 1a reports the most frequently cited job functions of respondents (top five). Table 1b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (42 percent) or staff/technician (33 percent) levels, respectively.

Table 1a: Job functions (based on top 5 titles only)	%
IT Operations	45%
Security	12%
Application development	12%
Compliance	9%
Procurement	9%
Database administration	8%

Table 1b: Organizational levels	%
Senior Executive	2%
Vice President	1%
Director	18%
Manager	42%
Staff/Technician	33%
Other	4%
Total	100%

On average, respondents have almost nine years of experience in the information management or security fields, and three years of experience in their current position. In total, 61 percent of respondents were males and 39 percent 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.

Pie Chart 1: Industry distribution of respondents



Pie Chart 1 reports the average distribution of respondents by their organization's primary industry classification. As shown, over 22 percent of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 15 percent work for federal or local government. Another 15 percent work in the health care and pharmaceutical sector.

Table 2a reports the organization’s economic structure, showing that the majority of respondents’ companies work for organizations that are publicly traded on a major exchange. Table 2b provides the approximate headcounts of these organizations. As can be seen, 39 percent of respondents are employed by larger-sized organizations (with more than 25,000 employees).

Table 2a. Economic structure	%
Yes, major stock exchange (NYSE or NASDAQ)	50%
Yes, minor stock exchange	6%
No	4 %
Total	100%

Table 2b. Corporate headcount	%
Less than 500 people	3%
500 to 1,000 people	1%
1,001 to 5,000 people	11%
5,001 to 25,000 people	44%
25,001 to 75,000 people	26%
More than 75,000 people	15%
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.

Appendix 1: Survey Questions in Percentage Frequency Format

Q1a. Has your organization experienced one or more data breaches involving the loss or theft of information about people or households (personal information)?	US%
Yes	79%
No (stop)	21%
Total	100%

Remaining sample	878
-------------------------	------------

Q1b. How were you involved? Please check all that apply.	US%
Defining response plan	3%
Establishing incident response team	10%
Training and educating staff and employees	16%
Detecting, verifying, investigating facts, and categorizing incidents	41%
Determining appropriate response (including internal escalation)	6%
Notifying parties /communicating with consumers, employees, shareholders and others	2%
Preparing reports to management	4%
Conducting root-cause analysis	11%
Remediation activities	18%
Interacting with regulatory/legal authorities/outside lawyers	2%
Other (please specify)	3%
None of the above (stop)	3%
Total	118%

Remaining sample	849
-------------------------	------------

Q2. How many data breach incidents involving the loss or theft of personal information occurred within your organization in the past 24 months?	US%
Only once	23%
About two to three incidents	15%
About four to five incidents	23%
More than five incidents	5%
Unsure	34%
Total	100%

Q3. How confident are you that all data breaches involving the loss or theft of personal information will be detected within your organization?	US%
Very confident	10%
Confident	16%
Somewhat confident	25%
Not confident	31%
Unsure	18%
Total	100%

Q4. In what IT environments did your organization's data breach incident occur? Please check all that apply.	US%
Mainframes	41%
Networks	50%
Backups	18%
Off-network devices	58%
Paper files	39%
Other	1%
Total	206%

Q5. What has been the most likely cause(s) of data breaches within your organization? Please check all that apply.	US%
External attack (hackers)	1%
Social engineering or pre-texting	2%
Negligent insiders	75%
Malicious insiders	26%
outsourced data	42%
Other	8%
Total	154%

Part II: Please respond based on the most recent data breach caused by an insider (including outsourcers) involving the loss or theft of personal information your organization experienced.

Q6a. Did this data breach incident require notification of individuals whose personal information was lost or stolen?	US%
Yes	53%
No	47%
Total	100%

Q6b. If yes , after discovering the incident, how much time did it take for your organization to respond to data breach victims who required notification?	US%
Immediately	5%
Within a few days	15%
Within a few weeks	39%
Within one month	23%
More than one month	17%
Total	100%

Q7. In your opinion, how important is it for your organization to respond quickly to data breach victims who require notification?	US%
Very important	11%
Important	26%
Somewhat important	40%
Not important	14%
Irrelevant	9%
Total	100%

Q8a. In your opinion, were you able to determine all relevant facts – that is, the “who, what, where, when and how” – in order to pinpoint the root cause of the incident as well as who needs to be notified?	US%
Yes	67%
No (Go to 8d)	33%
Total	100%

Q8b. If yes , how confident do you feel that you and your organization obtained <u>all the facts</u> associated with this data breach incident?	US%
Very confident	7%
Confident	34%
Somewhat confident	38%
Not confident	16%
Unsure	5%
Total	100%

Q8c. If yes , what facts did you gather to detect and appropriately respond to the data breach event?	US%
Nature of the incident (i.e., negligence or criminal intent)	27%
Source of the incident (i.e., privileged users, general employees, contractors and/or IT glitches that caused the event)	51%
Types of files or data-bearing electronic device lost or stolen	62%
Types of information (i.e., customer, employee, consumer)	61%
People whose information was lost or stolen (i.e., victim)	91%
Impact or harm resulting from the data breach	40%
The recipient(s) of the information	39%
Date and time of the actual incident	38%
Regulatory and legal requirements	14%
Other (please specify)	4%
Total	427%

Q8d. If no , what facts were missing to detect and appropriately respond to the data breach event?	US%
Nature of the incident (i.e., negligence or criminal intent)	53%
Source of the incident (i.e., privileged users, general employees, contractors and/or IT glitches that caused the event)	63%
Types of files or data-bearing electronic device lost or stolen	49%
Types of information (i.e., customer, employee, consumer)	43%
People whose information was lost or stolen (i.e., victim)	85%
Impact or harm resulting from the data breach	57%
The recipient(s) of the information	57%
Date and time of the actual incident	31%
Regulatory and legal requirements	31%
Other	4%
Total	474%

Q9. For each fact listed below, please check how important it is for understanding the cause of the breach? 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5
Nature of the incident (i.e., negligence or criminal intent)	26%	40%	23%	8%	4%
Source of the incident (i.e., employees, contractors and/or IT glitches that caused the event)	22%	35%	35%	4%	4%
Files or data-bearing electronic devices lost or stolen	18%	24%	34%	15%	9%
Information lost or stolen (i.e., customer, employee, consumer, business confidential, intellectual property)	32%	28%	23%	13%	4%
People whose personal information was lost or stolen (i.e., victims who may require notification)	29%	15%	22%	33%	1%
Impact or harm resulting from the data breach	16%	28%	46%	10%	0%
Recipients of the information	23%	23%	39%	14%	1%
Date and time of the actual incident	35%	34%	21%	5%	5%
Regulatory and legal requirements	18%	20%	29%	32%	1%

Q10. What tools or techniques did your organization use to obtain facts about the data breach incident? Please check all that applied to your investigation:	US%
Tools that reviewed system audit logs.	44%
Used content filtering to match key terms or phrases in documents	43%
Used sniffing to identify errors, irregularities or inconsistencies in networks and websites	25%
Evaluated end-user permissions such as opt-in or opt-out	53%
Recorded appropriate transaction screens for breach analysis and forensic evaluation	16 %
Determined compliance of identity and access management procedures	27%
Evaluated information for accuracy and quality	46%
Checked for alterations in backup and recovery procedures	9%
Reviewed software patch activity	69%
Recorded network traffic for surveillance and forensic evaluation	46%
None of the above tools were available	7%
Other	19%
Total	404%

Q11. What tools or techniques do you believe your organization should have to obtain facts about the data breach incident? Please check all that apply:	US%
Tools to facilitate the review of system audit logs	75%
Detection or prevention of intrusions to enterprise systems and networks	36%
Content filtering to match key terms or phrases in documents	26%
Sniffing to identify errors, irregularities or inconsistencies in networks and websites	21%
Evaluation of end-user permissions such as opt-in or opt-out	48%
Record appropriate transaction screens for breach analysis and forensic evaluation	88%
Determine compliance of identity and access management procedures	29%
Evaluate information accuracy and quality	19%
Check for alterations in backup and recovery procedures	28%
Review of software patch activity	11%
Record network traffic for surveillance and forensic evaluation	71%
Other	13%
Total	466%

Q12. What tools or techniques do you believe could serve as a deterrent to potential future data breach incidents? Please check all that apply:	US%
Tools to facilitate the review of system audit logs	63%
Detection or prevention of intrusions to enterprise systems and networks	33%
Content filtering to match key terms or phrases in documents	30%
Sniffing to identify errors, irregularities or inconsistencies in networks and websites	52%
Evaluation of end-user permissions such as opt-in or opt-out	39%
Record appropriate transaction screens for breach analysis and forensic evaluation	90%
Determine compliance of identity and access management procedures	20%
Evaluate information accuracy and quality	17%
Check for alterations in backup and recovery procedures	21%
Review software patch activity	5%
Record network traffic for surveillance and forensic evaluation	73%
Announce and record transaction activity	40%
Securely archive recorded transaction activity	56%
Other	0%
Total	540%

For each question listed below, please check 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5
Q13. Are automated tools important to your overall audit and compliance mission?	36%	32%	22%	11%	0%
Q14. How important are tools that help you and your organization perform forensic activities when determining the cause and effect of a data breach?	32%	29%	20%	3%	17%
Q15. How important are tools that help you and your organization deter employee or contractor negligent or malicious behaviors that may cause future data breaches?	55%	25%	7%	12%	1%

Q16. Please check all the regulations listed below that are most influential to your organization's IT security policies and programs:	US%
Breach notification statutes	52%
Sarbanes-Oxley	32%
Payment Card Industry (PCI) requirements	47%
Gramm-Leach-Bliley Act	19%
National privacy & data protection laws	NA
FTC Safeguards Rule	1%
European Union Privacy Directive	13%
Health Insurance Portability & Accountability Act	28%
Financial Service Authority (FSA)	NA
Other	2%
Total	196%

Q17. Who is responsible within your organization for detecting or responding to a data breach incident? Please check all that apply:	US%
Chief information officer	17%
Chief information security officer	9%
Data base administrator	5%
Compliance officer	18%
Internal audit director	5%
IT operations	15%
Privacy officer	8%
No one party is accountable	43%
Unsure	28%
Other	0%
Total	429%