Ponemon INSTITUTE

Is Your Company Ready for a Big Data Breach?

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: March 2013

Is Your Company Ready for a Big Data Breach?

Ponemon Institute, March 2013

Part 1. Introduction

How prepared is your company for a material data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential business information? How would you grade the incident response plans in place that would reduce such negative consequences as the loss of reputation, customer loyalty and regulatory fines?

In a new study sponsored by Experian® Data Breach Resolution, Ponemon Institute surveyed a representative sample of privacy and compliance leaders in various-sized organizations in the United States on the following topics:

- Expectations that their organizations will experience a material data breach resulting in loss of customer trust, regulatory fines, loss of customer and negative public opinion.
- Data security practices in place to avoid a material data breach.
- The existence of a quality data breach preparedness plan.

In contrast to the numerous studies that survey IT and IT security practitioners about the readiness and responsiveness of their organizations to respond to a data breach, this research focuses on what executives and staff employees who work primarily in privacy and compliance think about this issue.

In order to qualify to participate in this research, all respondents report that their organizations had at least one data breach and 52 percent report they had two or more. The majority of the 471 respondents are employed in organizations with a headcount of more than 1,000.

Some of the most noteworthy findings are:

- The biggest concerns about the consequences of a big data breach are the loss of customers and business partners followed by negative opinion.

- The majority of organizations have a data breach preparedness plan that is funded through privacy or data security budgets. They also have a team dedicated to data breach response. Most often the team represents various functions within the organization.

- Based on the findings of this research, many organizations are losing opportunities to reduce the risk of negative opinion and loss of customer trust by not focusing on communications with victims. Only 21 percent of respondents have an internal communications team trained to assist in responding to victims.

- Only 30 percent of respondents say their organizations train customer service personnel on how to respond to questions about the data breach incident, only 11 percent of respondents say their organization verifies that contact with each victim has been completed and only 10 percent have a process for receiving feedback from victims about the quality and responsiveness of the notification.

- Only 23 percent of respondents say their organizations are able to determine the potential or actual harms to data breach victims. Further, only 26 percent of respondents have the ability to ensure that the data breach victims were those truly affected or harmed by the incident do that so there is no over-reporting or under-reporting the incident.

Part 2. Key Findings

The complete audited findings are presented in the appendix of this report. In this section, we organize the results of the study according to the following topics:

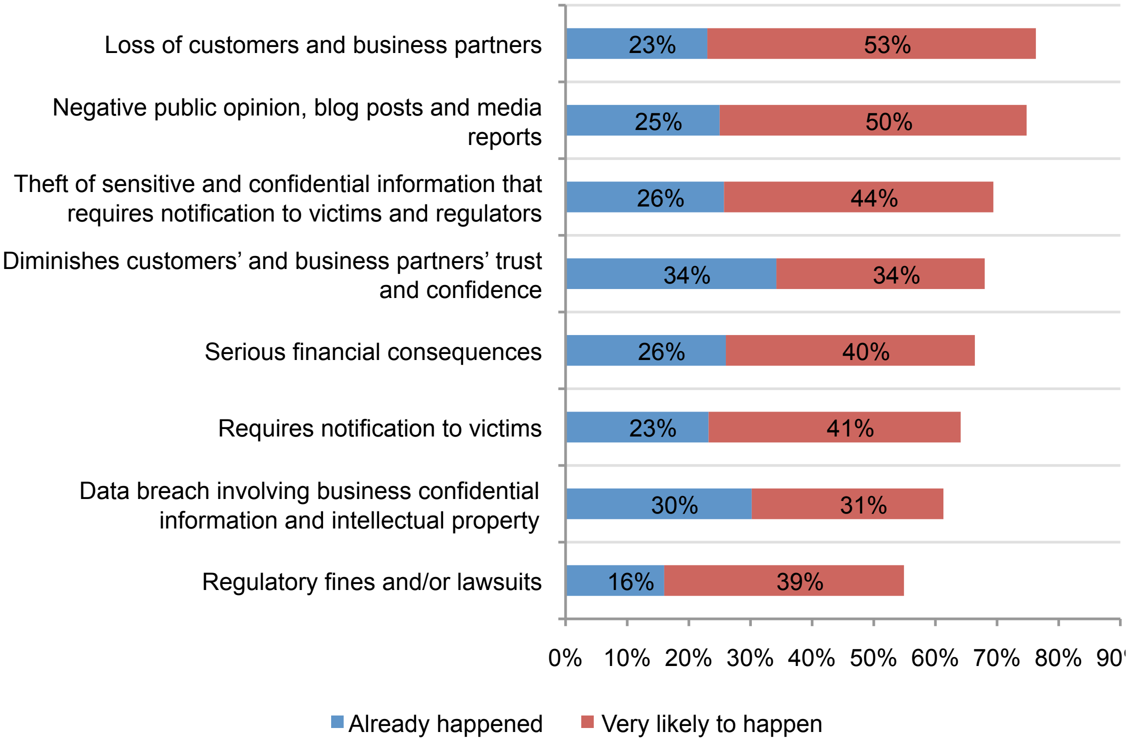
- Data breach experience of organizations
- Data security readiness of organizations
- Data breach preparedness of organizations
- Lessons learned: How to prepare for a material data breach

Data breach experience

Respondents rate the consequences of a data breach. Following a material data breach, respondents are most concerned about negative public opinion and lost customers and business partners. As shown in Figure 1**,** 76 percent of respondents say their organization already had or expect to have a material data breach that results in the loss of customers and business partners. Similarly, 75 percent say they have had or expect to have such an incident that results in negative public opinion. The majority of respondents also report they have had or expect to have the following incidents:

- Loss or theft of sensitive and confidential information that requires notification to victims and regulators
- A material data breach that diminishes customers' and business partners' trust and confidence
- A material data breach that has negative financial consequences
- Data breach involving business confidential information and intellectual property
- A material data breach that results in regulatory fines and/or lawsuits

Figure 1: Likelihood of data breach situation occurring
Already happened and very likely to happen responses



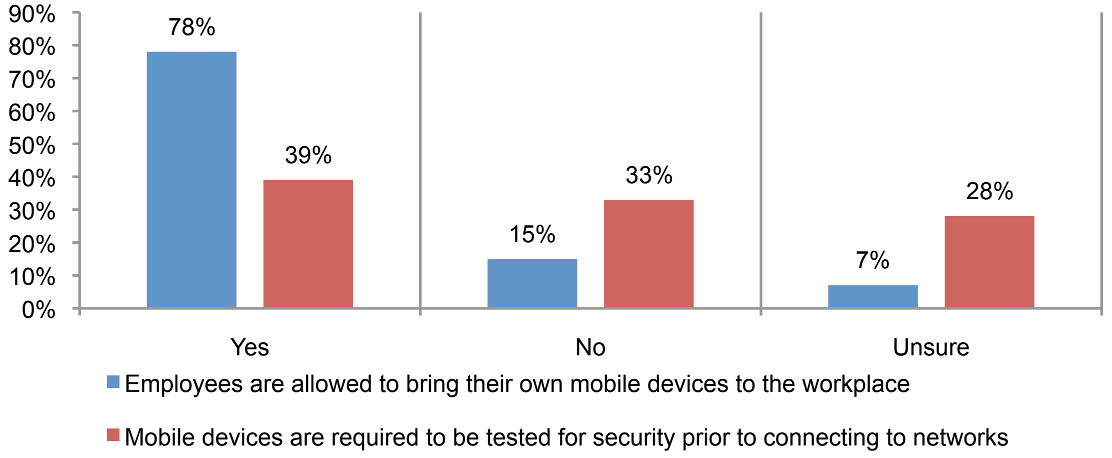
Data security readiness

This section measures respondents' understanding of the data security practices their organizations have in place to prevent and respond to a data breach.

The following practices within organizations in this study are creating the potential for a big data breach.

BYOD is permitted without security testing. Seventy-eight percent say their organizations allow employees to bring their own mobile devices such as laptops, tablets and smart phones (BYOD) to the workplace (Figure 2). However, 61 percent say their organization does not require or they are unsure that mobile devices should be tested for security prior to connecting to networks or enterprise systems.

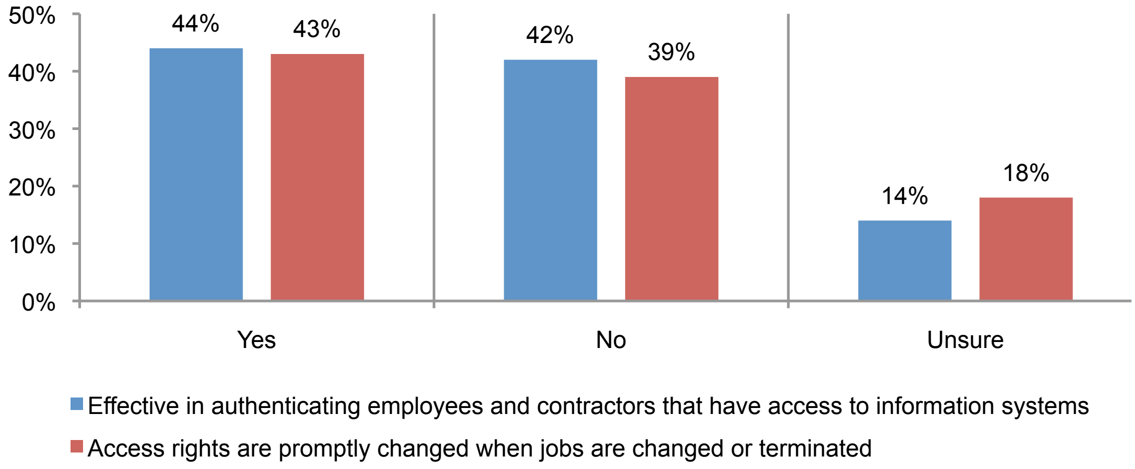
Figure 2: BYOD in the workplace



Lack of effective access and authentication practices could enable improper access to personal information. Less than half (44 percent) of respondents say that their organization is effective in authenticating and making sure that only the appropriate employees and contractors have access to its information systems, as revealed in Figure 3. Forty-two percent say no and 14 percent are unsure.

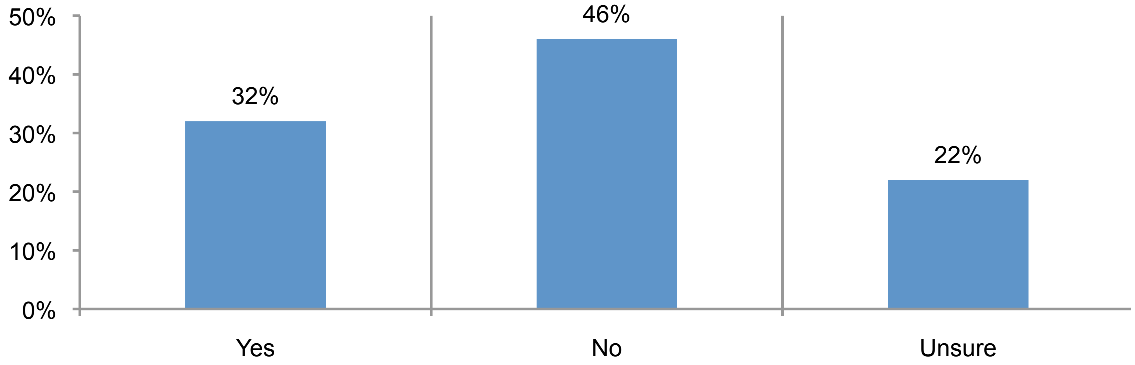
Further, only 43 percent say their organization promptly changes access rights of employees and contractors when they change jobs or are terminated. Thirty-nine percent say no and 18 percent are unsure.

Figure 3: Access and authentication practices



Encryption is not widely deployed. According to Figure 4, less than one-third of respondents say sensitive or confidential personal and business information stored on computers, servers and other storage devices generally encrypted. Forty-six percent say they do not encrypt and 22 percent are unsure.[1]

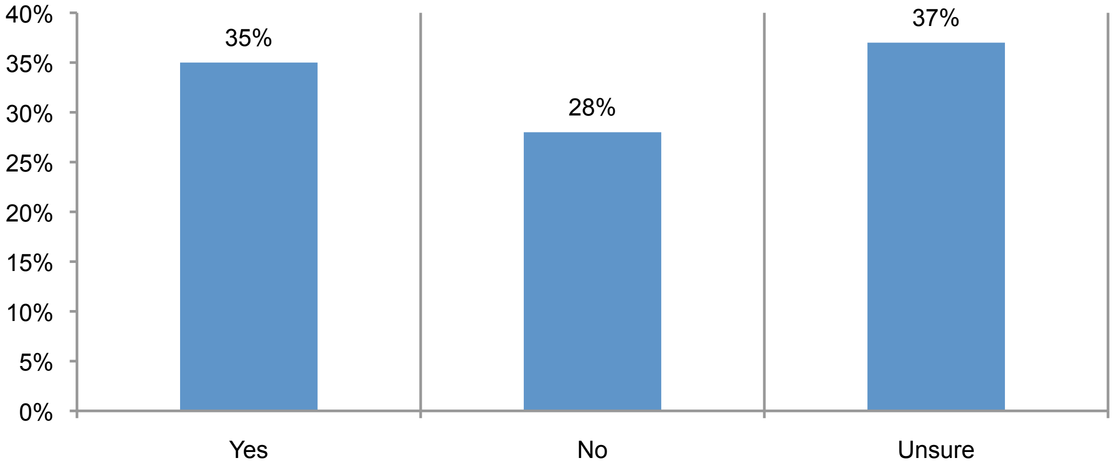
Figure 4: Encryption of sensitive information



[1] This result is consistent with another recent study showing the usage rate for 11 encryption technologies. See 2012 Encryption Trends Study, Ponemon Institute, February 2013.

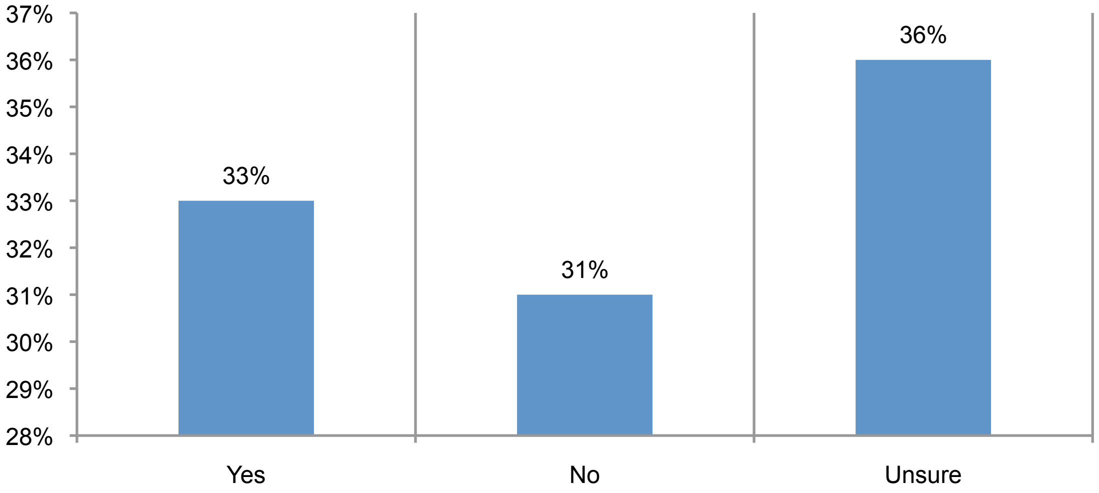
Applications and operating systems are not sufficiently tested. As shown in other Ponemon Institute research, insecure applications make organizations vulnerable to hundreds of threat vectors that can lead to cyber attacks. However, many organizations do not take steps to ensure applications' security. In fact, 37 percent of respondents are uncertain whether applications and operating systems are routinely tested or inspected for security and 28 percent say no tests or inspections take place, according to Figure 5. Only 35 percent say their organizations do conduct tests.

Figure 5: Applications and operating systems are routinely tested or inspected for security



Monitoring information systems for unusual or anomalous traffic does not regularly occur. Only one-third of respondents say their organizations are taking such preventative measures as monitoring for potential risks to the network and enterprise system (Figure 6). Also, many respondents (36 percent) do not know if this practice is in place.

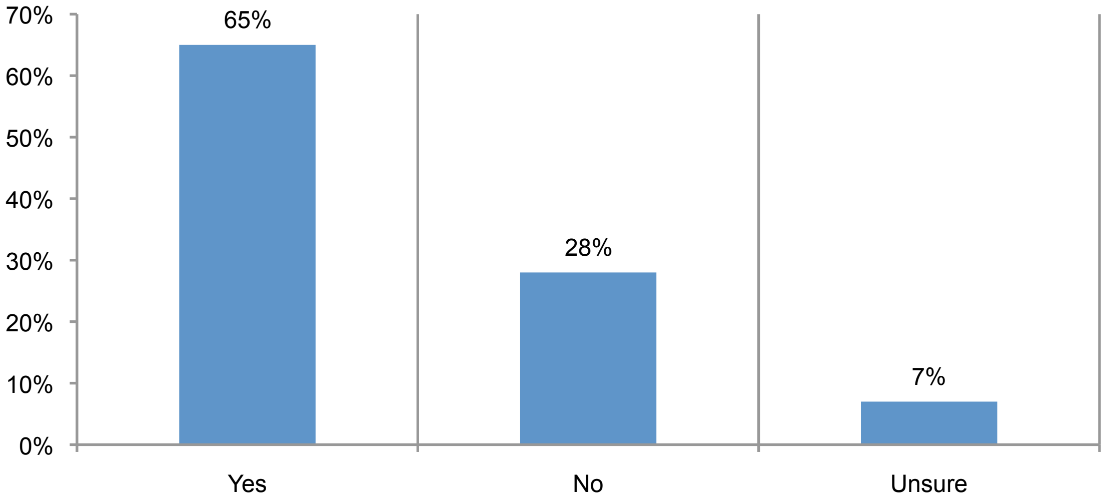
Figure 6: Information systems are regularly monitored for unusual or anomalous traffic



The following data security practices are helpful in reducing the risk of a data breach and increasing the organization's preparedness.

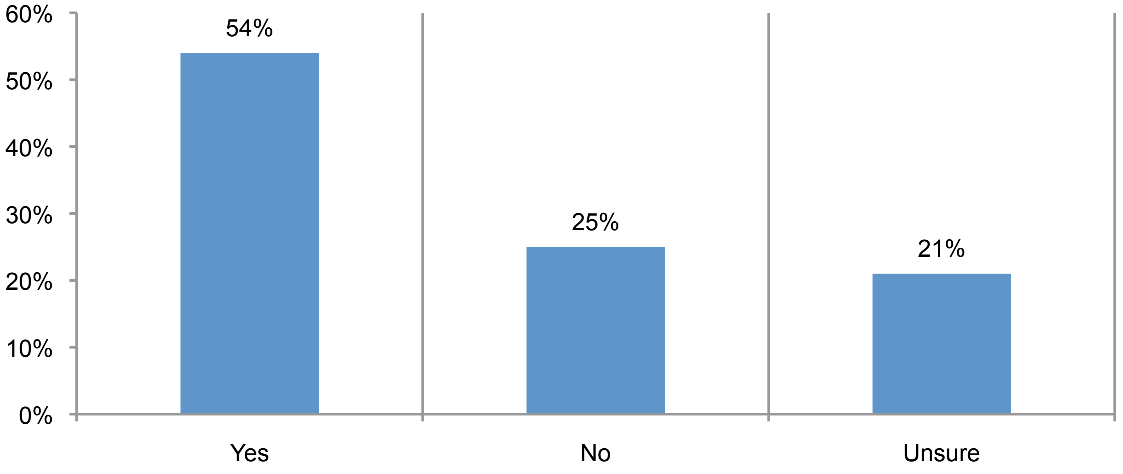
Third parties are required to use standard or model contract terms. According to Figure 7, 65 percent say their organization has contracts with third parties, vendors or business partners that require them to use standard or model contract terms (preferably with indemnification).

Figure 7: Organizations' use of standard or model contract terms



Third parties are vetted for their privacy and data protection practices. Fifty-four percent of respondents say their organizations conduct a privacy risk assessment and make sure appropriate privacy and data protection practices are in place before sharing sensitive and confidential information with third parties and business partners. However, several respondents (21 percent) are unsure if these procedures are in place, as revealed in Figure 8.

Figure 8: Vetting and privacy assessments of third parties and business partners



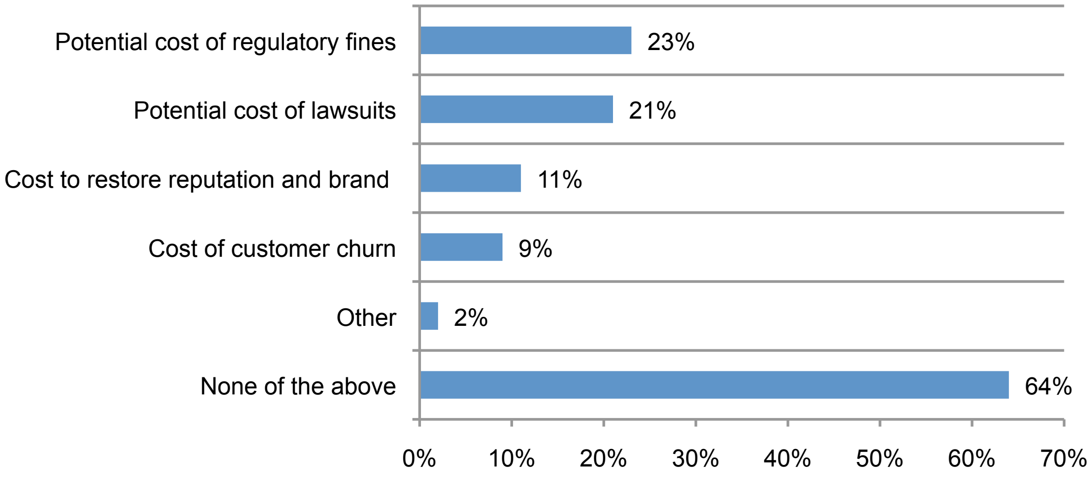
Data breach preparedness

According to the findings, 61 percent of respondents report their organizations have a data breach preparedness plan in place. Only those respondents in organizations that have such a plan participated in this part of the study.

The majority of these respondents say the following practices are included in their data breach preparedness plans.

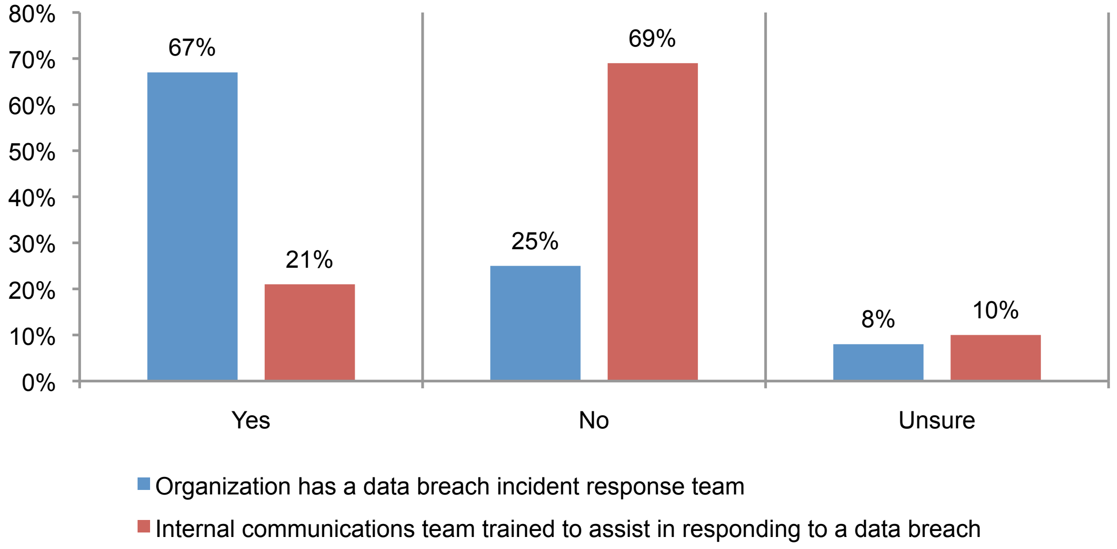
Privacy and data security budgets dedicate a portion to data breach preparedness. More than half (52 percent) fund their data breach preparedness plans. Based on the findings, it seems that most organizations are not justifying how data breach preparedness can have positive financial results. As shown in Figure 9, only 23 percent say they measure the potential cost of regulatory fines and 21 percent say they measure the potential cost of lawsuits. However, 64 percent do not use any of the measures listed.

Figure 9: Measures used to calculate the benefits of a data breach preparedness plan
More than one response permitted



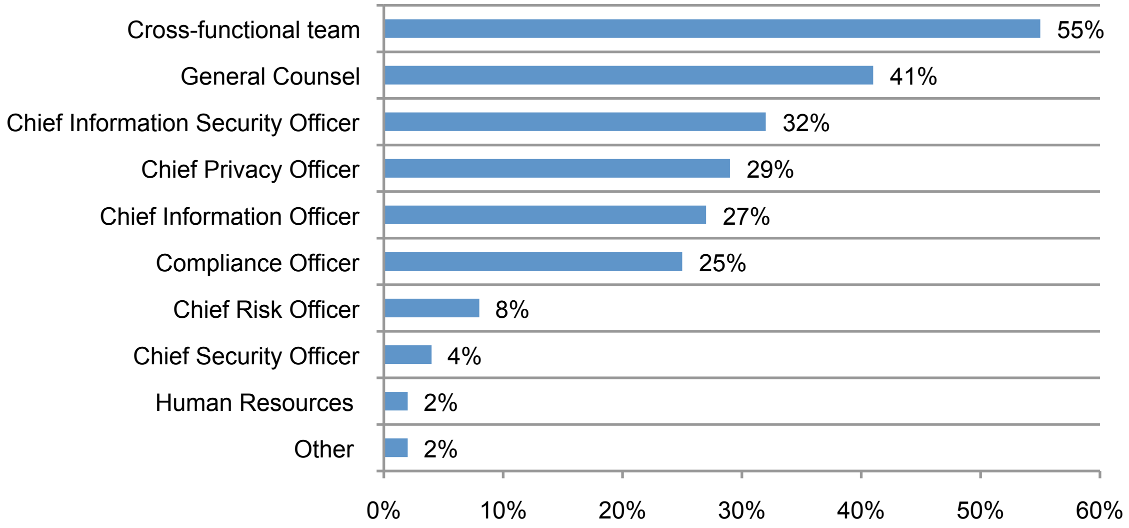
The majority of organizations have a team dedicated to responding to a data breach. According to 67 percent of respondents, their organization has a data breach incident response team as shown in Figure 10. However, only 21 percent have an internal communications team trained to assist in responding to a data breach including notifying victims, regulators and media.

Figure 10: Data breach response team and internal communications team



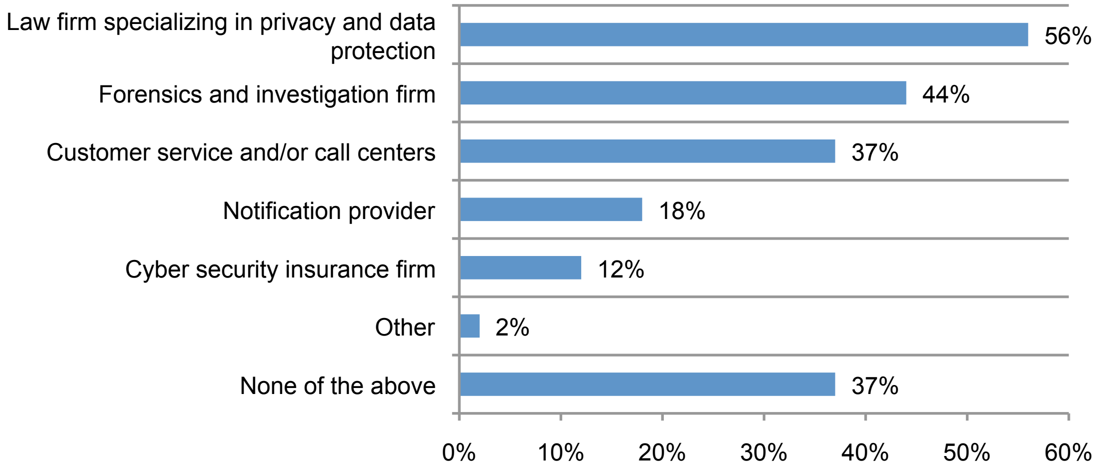
Only 29 percent of respondents say their organization has a department or function designated to manage data breach incidents. If they do, the functions most often designated to manage the incident are a cross-functional team involving multiple functions or departments (55 percent), the general counsel (41 percent of respondents) and the chief information security officer (32 percent), as shown in Figure 11.

Figure 11: Function responsible for managing the data breach incident



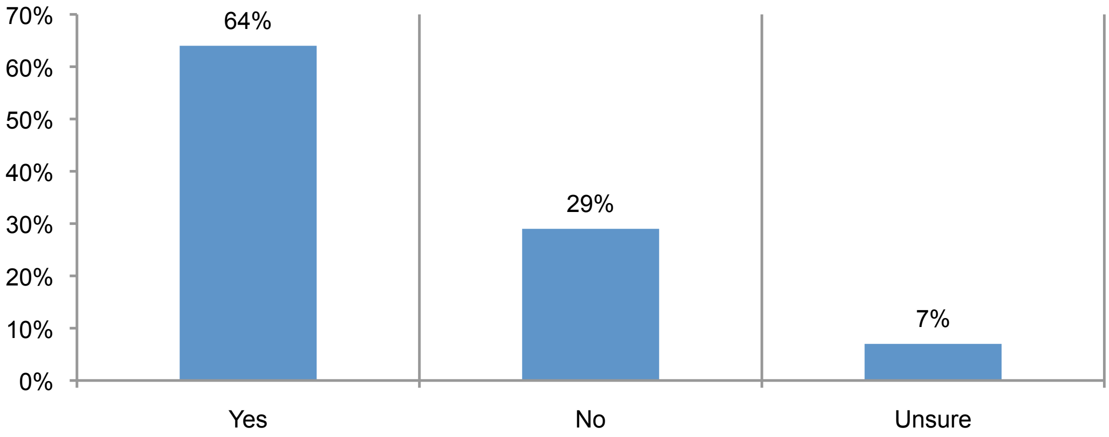
Organizations engage outside services to help them in the event of a material data breach. According to Figure 12, the top three services are a law firm specializing in privacy and data protection (56 percent), forensics and investigation firms (44 percent) and customer service and/or call centers.

Figure 12: Services engaged to help in the event of a material data breach
More than one response permitted



Most organizations understand state and federal disclosure requirements. Sixty-four percent of organizations have a process for determining and/or monitoring compliance to state and federal disclosure requirements as shown in Figure 13.

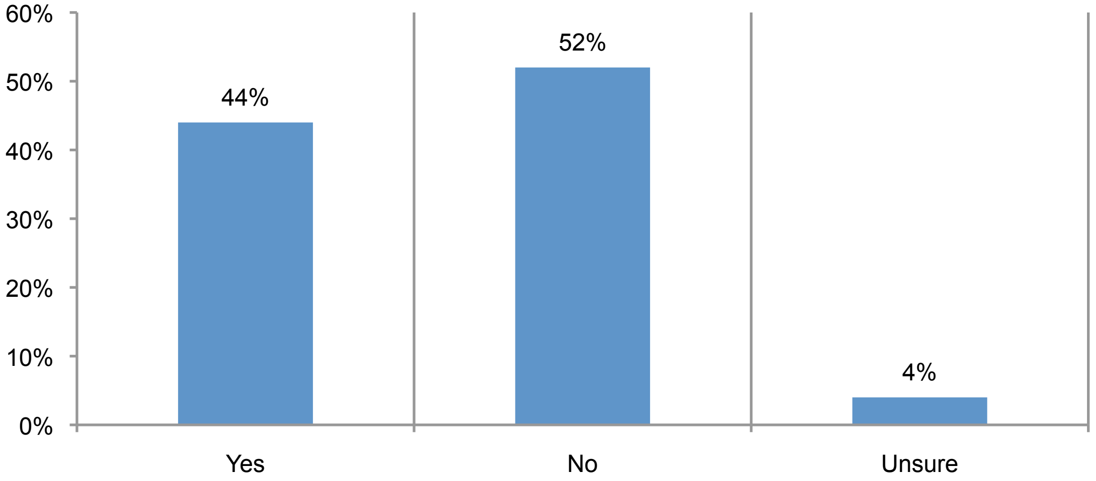
Figure 13: Compliance to state and federal disclosure requirements is monitored



The following practices are followed by less than a majority of respondents.

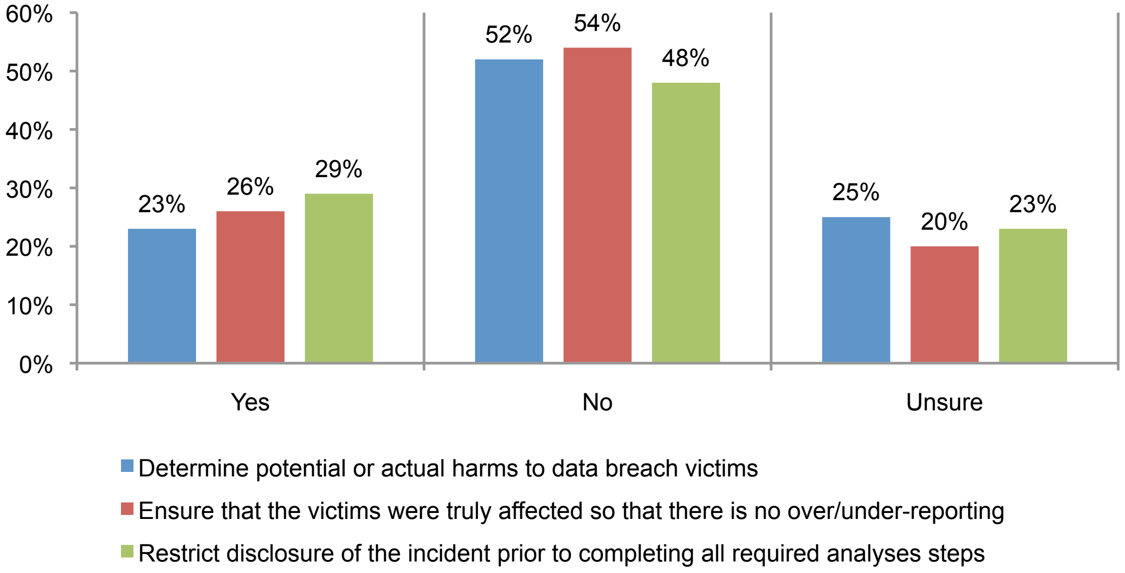
Many organizations do not have a privacy and/or data protection awareness program. As revealed in Figure 14, only 44 percent of respondents say their organizations have a privacy and or data protection awareness program for employees and other stakeholders who have access to sensitive or confidential personal information.

Figure 14: Privacy/data protection awareness program for employees & stakeholders



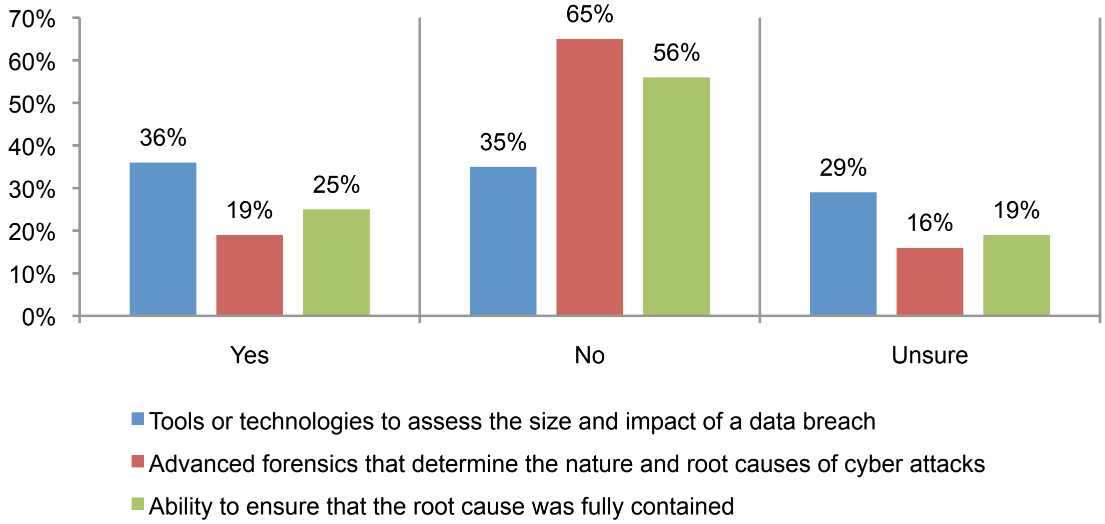
Many organizations do not have the ability to determine who was affected by the breach. Only 23 percent of respondents say their organizations are able to determine the potential or actual harms to data breach victims as shown in Figure 15. Further, only 26 percent of respondents have the ability to ensure that the data breach victims were those truly affected or harmed by the incident do that so there is no over-reporting or under-reporting the incident. Also lacking is the ability to restrict or limit disclosure of the incident prior to completing all required analyses and investigative steps.

Figure 15: Data breach analysis procedures



More technologies are needed to prepare for and reduce the consequences of a material breach. According to Figure 16, only 36 percent have the tools or technologies to assess the size and impact of a data breach, only 19 percent have advanced forensics to determine the nature and root causes of cyber attacks and only 25 percent have the ability to ensure the root cause of the data breach was fully contained.

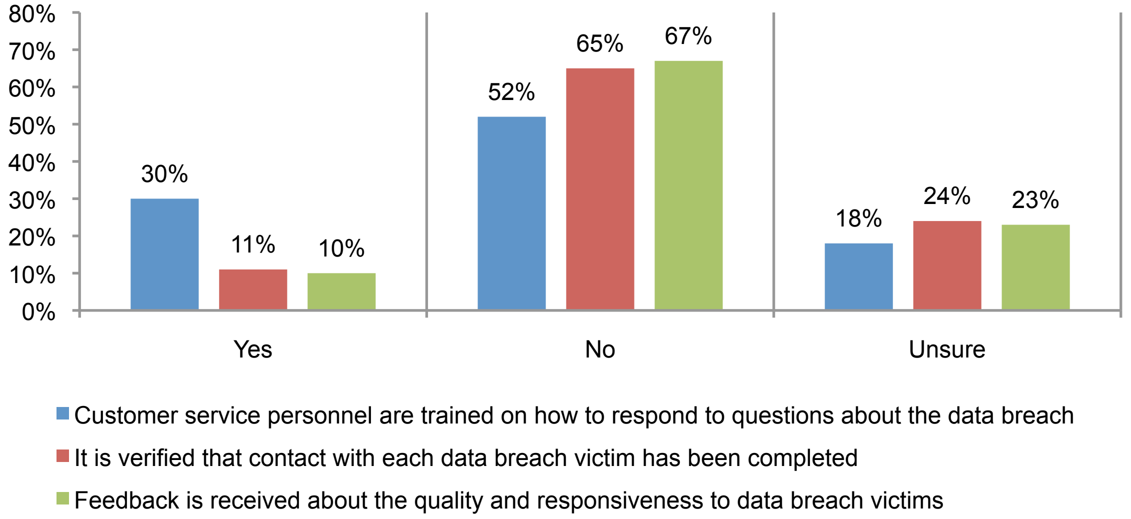
Figure 16: Data breach forensics



Quality of communication with victims needs to be improved. Based on the findings of this research, many organizations are losing opportunities to reduce the risk of negative opinion and loss of customer trust by not focusing on communications with victims. As we mentioned previously, only 21 percent of respondents have an internal communications team trained to assist in responding to victims.

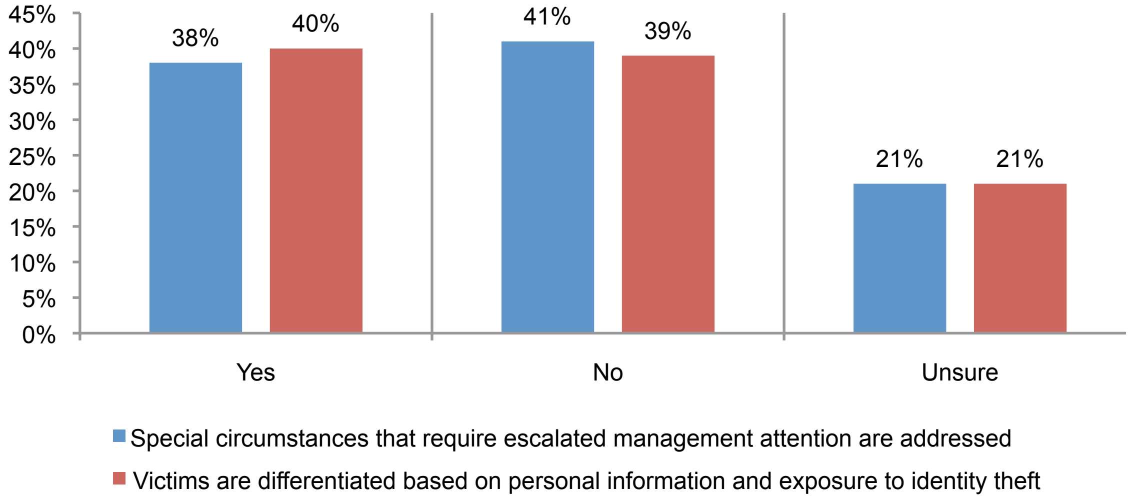
As shown in Figure 17, only 30 percent of respondents say their organizations train customer service personnel on how to respond to questions about the data breach incident, only 11 percent of respondents say their organization verifies that contact with each victim has been completed and only 10 percent have a process for receiving feed back from victims about the quality and responsiveness of the notification.

Figure 17: Communication procedures after the breach



Moreover, 62 percent of respondents say their organizations do not have a process for addressing special circumstances such as disgruntled victims, seniors and other special cases that require escalated management attention and 60 percent do not have a process for differentiating victims based on their personal information and accompanying exposure to identity theft or criminal activity as revealed in Figure 18.

Figure 18: Procedures for working with victims



Lessons learned: preparing for a big data breach

The goal of this study is to learn how prepared organizations are to respond to a material data breach and where there are opportunities for improvement. For the first time, our research on data breach preparedness focuses on the perceptions of mostly individuals in compliance and privacy functions. The questions in this survey are based upon Ponemon Institute's proprietary benchmarks.[2]

The participants in this study are knowledgeable about material data breaches. More than half (52 percent) of respondents say their organizations have had more than one data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past two years.

Based on the findings, organizations do not make the following practices part of their data breach preparedness plan:

- Require mobile devices to be tested for security prior to connecting to networks or enterprise systems.
- Improve access and authentication practices to make sure that only the appropriate employees and contractors have access to its information systems and promptly change access rights of employees and contractors when they change jobs or are terminated.
- Encrypt sensitive or confidential personal and business information stored on computers, servers and other storage devices.
- Routinely test and inspect the security of applications and operating systems security.
- Monitor information systems for unusual or anomalous traffic that pose risks to the network and enterprise system.
- Establish a privacy and/or data protection awareness program for employees and other stakeholders who have access to sensitive or confidential personal information.
- Establish processes that will make it possible to determine who was affected by the breach so that there is no over-reporting or under-reporting the incident. Also, create processes that will restrict or limit disclosure of the incident prior to completing all required analyses and investigative steps.
- Improve the quality of communication with victims**.** This should include having an internal communications team trained to assist in responding to victims**.**
- Train customer service personnel on how to respond to questions about the data breach incident, verify that contact with each victim has been completed and have a process for receiving feedback from victims about the quality and responsiveness of the notification.

These recommendations present a high-level overview of the processes that can be put in place to avoid a material data breach or reduce the negative consequences should one occur.

[2] Ponemon Institute has captured corporate benchmarks on corporate privacy and data protection practices over the past 10 years. Contact the Institute for more information.

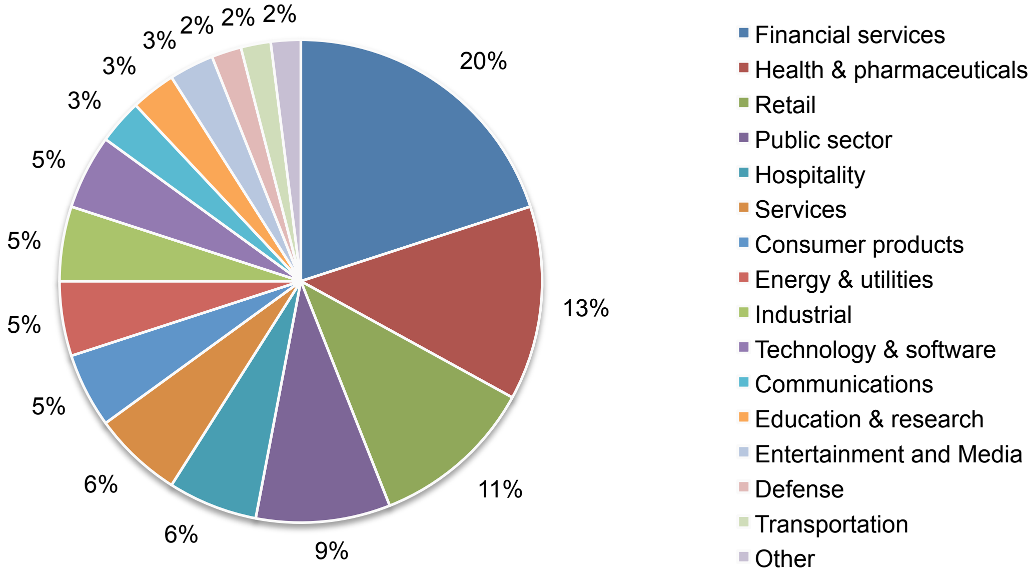
Part 3. Methods

A sampling frame composed of 11,056 individuals in compliance, privacy, IT and administration located in all regions of the United States were selected for participation for this survey. As noted above, the questions used in this survey are based upon Ponemon Institute's proprietary benchmarks on corporate privacy and data protection practices captured over several years. As shown in following table, 503 respondents completed the survey. Screening removed 32 surveys. The final sample was 471 surveys (or a 4.3 percent response rate).

Table 1: Survey response	Freq	Pct%
Sampling frame	11,056	100.0%
Total returns	503	4.5%
Total rejections	32	0.3%
Final sample	471	4.3%

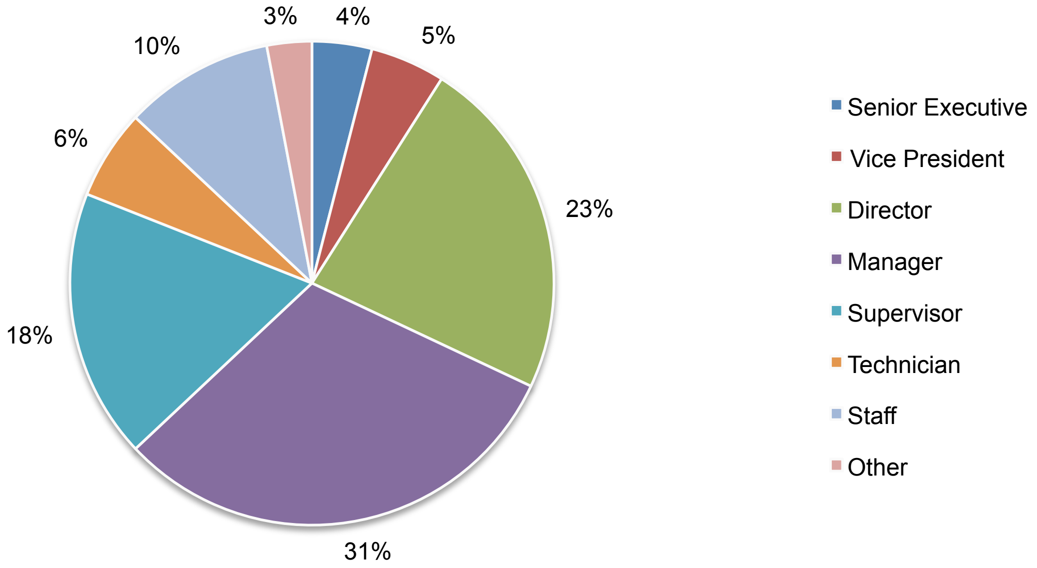
Pie Chart 1 reports the industry segments of respondents' organizations. This chart identifies financial services (20 percent) as the largest segment, followed by health and pharmaceuticals (13 percent) and retail (11 percent).

Pie Chart 1: Industry distribution of respondents' organizations



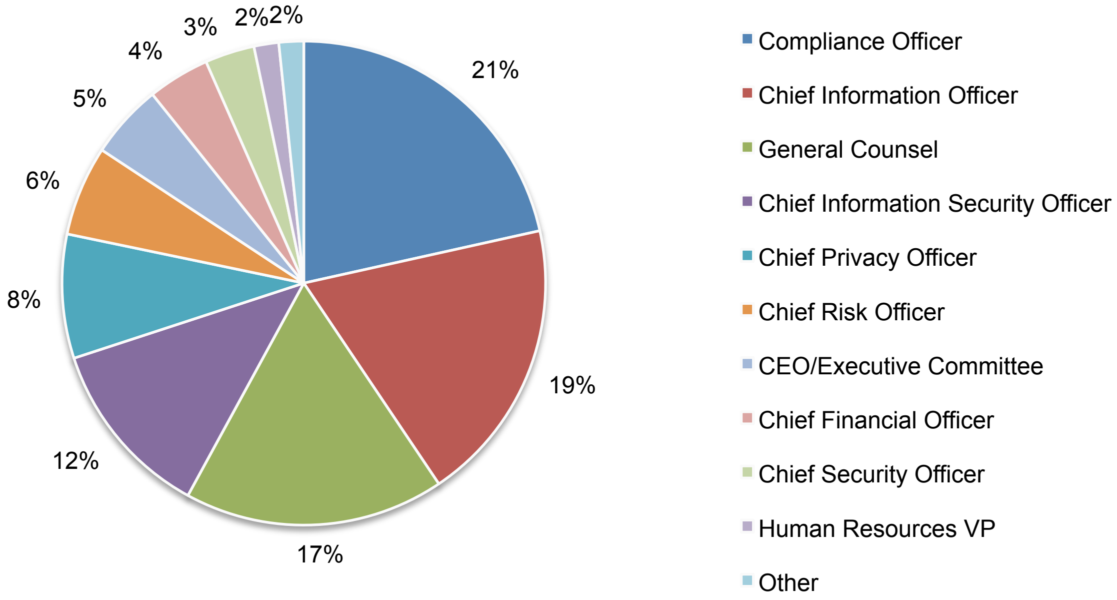
Pie Chart 2 reports the respondents' organizational level within participating organizations. Eighty-one percent of respondents are at or above the supervisor level.

Pie Chart 2: What organizational level best describes your current position?



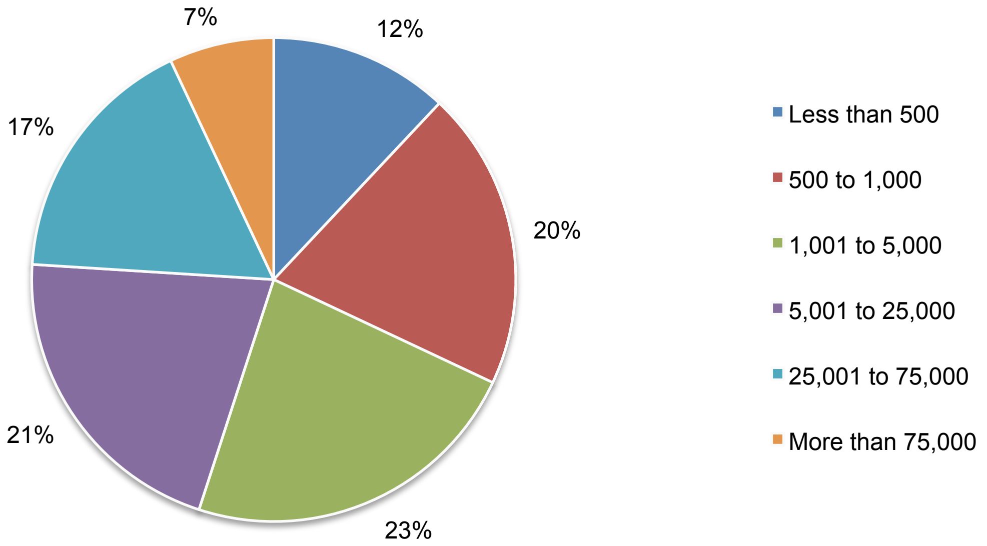
According to Pie Chart 3, 21 percent of respondents report directly to the Compliance Officer, 19 percent report to the Chief Information Officer and 17 percent report to the General Counsel.

Pie Chart 3: The primary person you report to within the organization



Almost half of the respondents (68 percent) are from organizations with a global headcount of over 1,000 employees, as shown in Pie Chart 4.

Pie Chart 4: Global headcount



Part 4. 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 is based on contact information and the degree to which the list is representative of individuals who are compliance or data protection practitioners in various organizations in the United States. 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 specified time period.

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 accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in January 2013.

Survey response	Freq	Pct%
Sampling frame	11056	100.0%
Total returns	503	4.5%
Total rejections	32	0.3%
Final sample	471	4.3%

Part 1. Background

Q1a. Did your organization have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past 2 years?	Pct%
Yes	33%
No	45%
Unsure	22%
Total	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	Pct%
Only once	48%
2 to 3 times	27%
4 to 5 times	16%
More than 5 times	9%
Total	100%

Please rate the likelihood of each one of the following situations occurring. Please use the five-point scale provided below each item. Already happened and very likely.	Already happened	Very likely to happen
Q2. My organization experiences the theft of sensitive and confidential information that requires notification to victims and regulators.	26%	44%
Q3. My organization experiences a data breach involving business confidential information and intellectual property.	30%	31%
Q4. My organization has a material data breach that requires notification to victims.	23%	41%
Q5. My organization has a material data breach that diminishes customers' and business partners' trust and confidence.	34%	34%
Q6. My organization has a material data breach that has serious financial consequences.	26%	40%
Q7. My organization has a material data breach that results in the loss of customers and business partners.	23%	53%
Q8. My organization has a material data breach that results in regulatory fines and/or lawsuits.	16%	39%
Q9. My organization has a material data breach that results in negative public opinion, blog posts and media reports.	25%	50%

Part 2. Data Security Readiness

Q10. Is your organization effective in authenticating and making sure only the appropriate employees and contractors have access to its information systems?	Pct%
Yes	44%
No	42%
Unsure	14%
Total	100%

Q11. Does your organization promptly change access rights of employees and contractors when they change jobs or are terminated?	Pct%
Yes	43%
No	39%
Unsure	18%
Total	100%

Q12. Is sensitive or confidential personal and business information stored on computers, servers and other storage devices generally encrypted?	Pct%
Yes	32%
No	46%
Unsure	22%
Total	100%

Q13. Are applications and operating systems routinely tested or inspected for security?	Pct%
Yes	35%
No	28%
Unsure	37%
Total	100%

Q14. Has your organization performed vetting and privacy risk assessments of third parties, vendors or business partners who have access to sensitive or confidential personal information?	Pct%
Yes	54%
No	25%
Unsure	21%
Total	100%

Q15a. Does your organization allow employees to bring their own mobile devices such as laptops, tablets and smart phones (BYOD) to the workplace?	Pct%
Yes	78%
No	15%
Unsure	7%
Total	100%

Q15b. If yes, does your organization have policies that require these mobile devices to be tested for security prior to connecting to networks or enterprise systems?	Pct%
Yes	39%
No	33%
Unsure	28%
Total	100%

Q16. Has your organization performed privacy risk or impact assessment of new and significantly revised systems (including outsourced systems and the use of cloud computing resources)?	Pct%
Yes	26%
No	52%
Unsure	22%
Total	100%

Q17. Does your organization regularly monitor its information systems for unusual or anomalous traffic?	Pct%
Yes	33%
No	31%
Unsure	36%
Total	100%

Q18. Does your organization have contracts with third parties, vendors or business partners use standard or model contract terms (preferably with indemnification)?	Pct%
Yes	65%
No	28%
Unsure	7%
Total	100%

Part 3. Data Breach Preparedness

Q19a. Does your organization have a data breach preparedness plan in place?	Pct%
Yes	61%
No [stop and proceed to Q. 20]	30%
Unsure [stop and proceed to Q.20]	9%
Total	100%

Q19b. If yes, does your organization dedicate a portion of its privacy and/or data security budget for data breach preparedness?	Pct%
Yes	52%
No	42%
Unsure	6%
Total	100%

Q19c. If yes, does your organization use the following measures to calculate the financial benefits of a data breach preparedness plan?	Pct%
Cost of customer churn	9%
Cost to restore reputation and brand	11%
Potential cost of regulatory fines	23%
Potential cost of lawsuits	21%
Other	2%
None of the above	64%
Total	130%

Q20a. Does your organization have a data breach incident response team?	Pct%
Yes	67%
No	25%
Unsure	8%
Total	100%

Q20b. If yes, does it include an internal communications team trained to assist in responding to a data breach including notifying victims, regulators and media?	Pct%
Yes	21%
No	69%
Unsure	10%
Total	100%

Q21. Does your organization have a privacy/data protection awareness program for employees and other stakeholders who have access to sensitive or confidential personal information?	Pct%
Yes	44%
No	52%
Unsure	4%
Total	100%

Q22a. Does your organization have a department or function designated to manage data breach incidents?	Pct%
Yes	29%
No	65%
Unsure	6%
Total	100%

Q22b. If yes, who has been designated to manage the data breach incident? (Please select all that apply)	Pct%
General Counsel	41%
Chief Privacy Officer	29%
Chief Information Officer	27%
Chief Information Security Officer	32%
Compliance Officer	25%
Human Resources	2%
Chief Security Officer	4%
Chief Risk Officer	8%
Cross-functional team involving multiple functions/departments	55%
Other	2%
Total	225%

Q23. Does your organization have the ability to determine potential or actual harms to data breach victims?	Pct%
Yes	23%
No	52%
Unsure	25%
Total	100%

Q24. Does your organization have any of the following outside services available to help in the event of a material data breach? (Please select all that apply)	Pct%
Law firm specializing in privacy and data protection	56%
Forensics and investigation firm	44%
Cyber security insurance firm	12%
Customer service and/or call centers	37%
Notification provider	18%
Other	2%
None of the above	37%
Total	206%

Q25. Does your organization have the tools or technologies to assess the size and impact of a data breach?	Pct%
Yes	36%
No	35%
Unsure	29%
Total	100%

Q26. Does your organization have advanced forensics to determine the nature and root causes of cyber attacks?	Pct%
Yes	19%
No	65%
Unsure	16%
Total	100%

Q27. Does your organization have the ability to ensure that the data breach victims were those truly affected or harmed by the incident so that there is no over-reporting or under-reporting of the incident?	Pct%
Yes	26%
No,	54%
Unsure	20%
Total	100%

Q28. Does your organization have the ability to ensure the root cause of the data breach was fully contained?	Pct%
Yes	25%
No	56%
Unsure	19%
Total	100%

Q29. Does your organization have the ability to restrict or limit disclosure of the incident prior to completing all required analyses and investigative steps?	Pct%
Yes	29%
No	48%
Unsure	23%
Total	100%

Q30. Does your organization train customer service personnel on how to respond to questions about the data breach incident?	Pct%
Yes	30%
No	52%
Unsure	18%
Total	100%

Q31. Does your organization have a process for verifying that contact with each data breach victim has been completed?	Pct%
Yes	11%
No	65%
Unsure	24%
Total	100%

Q32. Does your organization have a process for receiving feedback about the quality and responsiveness of the organization to data breach victims such as a customer service questionnaire?	Pct%
Yes	10%
No	67%
Unsure	23%
Total	100%

Q33. Does your organization have a process for addressing special circumstances such as disgruntled victims, seniors and other special cases that require escalated management attention?	Pct%
Yes	38%
No	41%
Unsure	21%
Total	100%

Q34. Does your organization have a process for differentiating victims based on their personal information and accompanying exposure to identity theft or criminal activity?	Pct%
Yes	40%
No	39%
Unsure	21%
Total	100%

Q35. Does your organization have a process for determining/monitoring compliance to state and federal disclosure requirements?	Pct%
Yes	64%
No	29%
Unsure	7%
Total	100%

Q36. Does your organization have data breach or cyber insurance?	Pct%
Yes	10%
No	82%
Unsure	8%
Total	100%

Part 2. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	4%
Vice President	5%
Director	23%
Manager	31%
Supervisor	18%
Technician	6%
Staff	10%
Contractor	1%
Other	2%
Total	100%

D2. Check the **Primary Person** you report to within the organization.	Pct%
CEO/Executive Committee	5%
Chief Financial Officer	4%
General Counsel	17%
Chief Privacy Officer	8%
Chief Information Officer	19%
Compliance Officer	21%
Human Resources VP	2%
Chief Information Security Officer	12%
Chief Security Officer	3%
Chief Risk Officer	6%
Other	2%
Total	100%

D3. What industry best describes your organization’s industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense	2%
Education & research	3%
Energy & utilities	5%
Entertainment and Media	3%
Financial services	20%
Health & pharmaceuticals	13%
Hospitality	6%
Industrial	5%
Public sector	9%
Retail	11%
Services	6%
Technology & software	5%
Transportation	2%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	12%
500 to 1,000 people	20%
1,001 to 5,000 people	23%
5,001 to 25,000 people	21%
25,001 to 75,000 people	17%
More than 75,000 people	7%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

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.