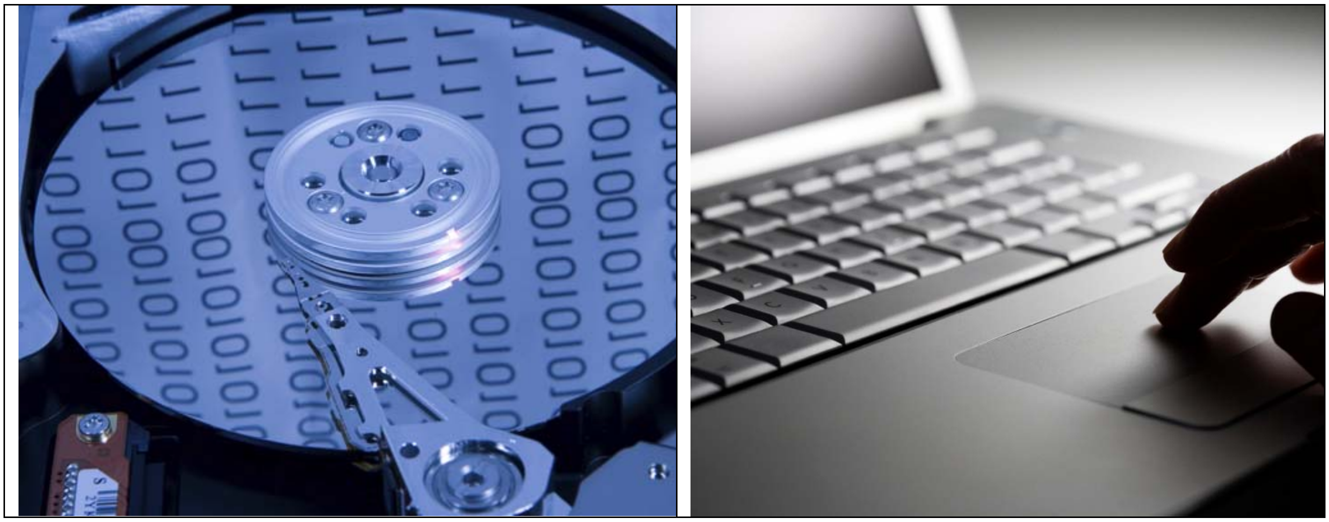


Security of Data Recovery Operations

Sponsored by DriveSavers

Independently conducted by Ponemon Institute LLC

Publication Date: December 7, 2009

Security of Data Recovery Operations

Prepared by Ponemon Institute, December 7, 2009

The following is based on an actual data breach incident.

Frank was employed as an IT helpdesk manager for a multinational financial services company. Late one afternoon he received a call from one of the company's senior level account executives. In a panic, the executive told Frank that his laptop was damaged and he needed to have access to its contents as quickly as possible. Frank did not ask and he was not told about the significant amount of personal data the laptop contained about the company's wealthiest customers.

After making a few calls, Frank selected a data recovery service provider that promised to be fast and cheap. Within 10 hours of taking possession of the damaged laptop, the vendor delivered what seemed to be a full saved copy of the contents on the hard drive. The executive was delighted with the fast turnaround and Frank thought everything was fine. In fact, he made a note to use them again.

A few weeks later the company began to see a pattern of identity theft among its wealthiest customers. A forensic examination allowed them to trace the information to the account executive with the damaged computer. Further investigation into the practices of the data recovery service provider revealed that the vendor employed individuals with criminal backgrounds, including identity theft crimes.

The moral of this story is that third-party data recovery service providers should be properly vetted before handing over a company's sensitive data contained on a drive. What our study reveals, however, is that many organizations are putting data at risk by not ensuring that proper security protocols are in place.

I. Executive Summary

The *Security of Data Recovery Operations* study was conducted by Ponemon Institute and sponsored by DriveSavers. This is the first national study on the security of data recovery operations for business and government organizations. Of specific focus are third-party data recovery services. We believe this is an important issue because of the confidential and sensitive data that may be at risk when in the possession of a third-party data recovery service provider.

We surveyed 636 IT security and IT support practitioners who are involved in their organization's data security or data recovery operations. According to the findings, 79 percent of these respondents report their organizations have used or will continue to use a third-party data recovery service provider to recover lost data. Recovery services are most often used when data files are damaged or lost and a back-up copy is not readily available.

The study reveals the uncertainty IT security and IT support practitioners have about their organizations' ability to safeguard sensitive and confidential information during the data recovery process. Specifically, there seems to be a lack of confidence that a data breach will not occur when using a third-party data recovery service.

The uncertainty about the ability to protect data when it is in the hands of third-parties can be attributed to the finding that only 20 percent of respondents believe data security is a major criterion when selecting a third-party data recovery service provider. However, 82 percent say it should be. This finding indicates there is awareness among IT practitioners that data is at risk when these third-party vendors are engaged.

A large percentage of respondents in this study report their organization has had at least one data breach (83 percent) in the past two years. (This is consistent with other Ponemon Institute studies about the prevalence of data breaches). Of the 83 percent who say their organization had a data breach, 19 percent say the breach occurred when a drive was in the possession of a third-party data recovery service provider. Forty-three percent of those respondents who say the breach occurred while at the vendor say it was due to a lack of data security protocols.

In addition, 81 percent of the respondents are not sure if a breach could have occurred when a drive was in the possession of a third-party data recovery service provider. This finding indicates respondents are not confident of their provider's security practices or that the third-party provider would inform them if a data breach involving their sensitive and confidential data occurred.

II. Key Findings

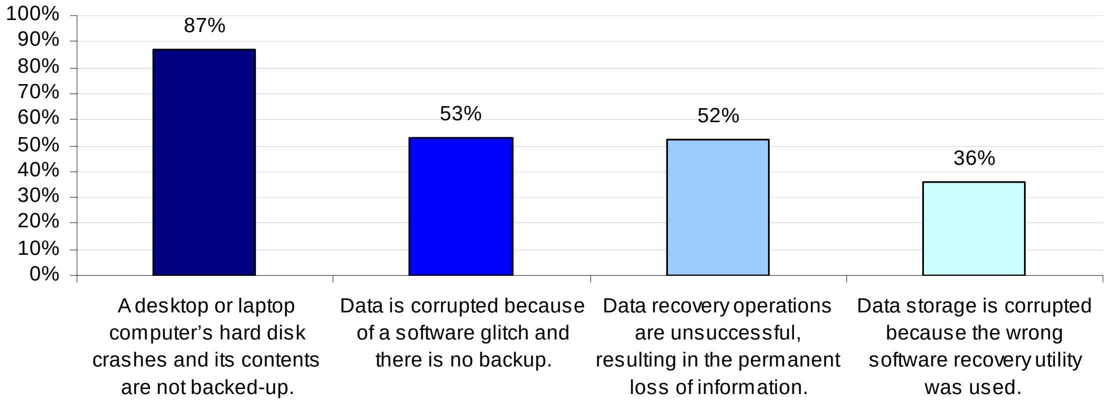
The following key findings are organized according to the following topics from the survey: use of third-party data recovery operations, selection of third-party data recovery operations, security risks of third-party data recovery operations and security practices of data recovery service providers.

Use of Data Recovery Service Providers

Findings indicate a majority of respondents' organizations use a third-party to recover lost or damaged data and this is expected to continue. Respondents also are aware that files containing their organization's most sensitive and confidential information are in the hands of a third-party data recovery service provider.

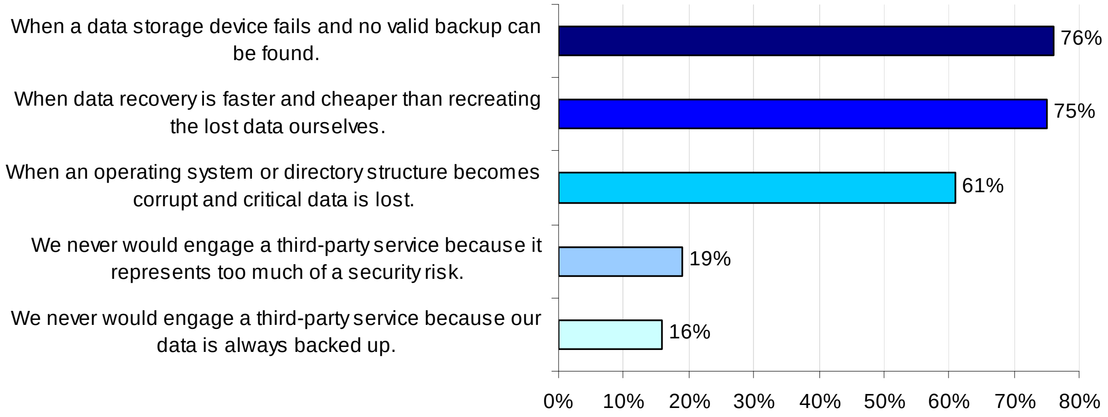
As shown in Bar Chart 1, a frequent occurrence in their organizations, according to 87 percent of respondents, is the crashing of hard disks on desktops or laptops and the content has not been backed up. Other data recovery problems faced by organizations include the corruption of data because of a software glitch and there is no backup (53 percent) and the failure of data recovery operations resulting in the permanent loss of data (52 percent).

Bar Chart 1
How often do these scenarios happen in your organization?



Bar Chart 2 summarizes five primary reasons for engaging a third-party data recovery service provider.

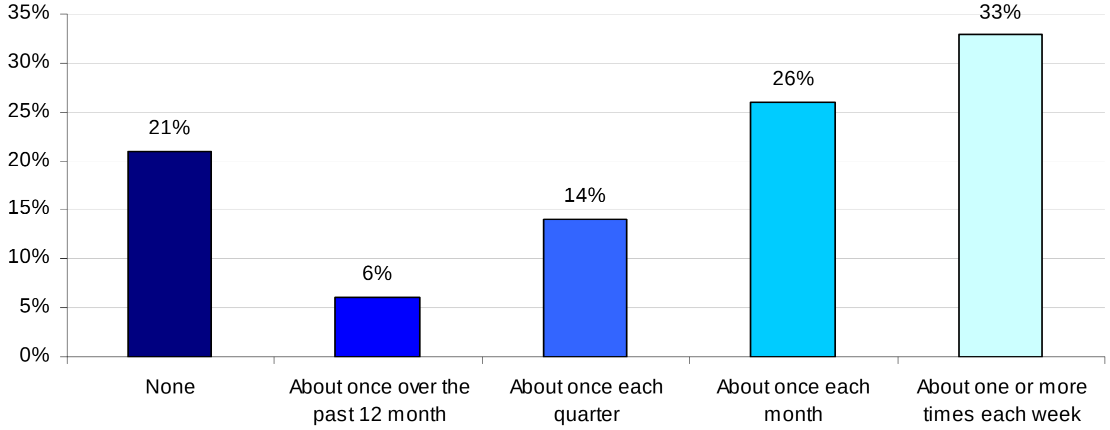
Bar Chart 2
When would your organization engage a data recovery service provider?



As noted above, the primary reasons to engage a data recovery service provider are the failure of a data storage device and no valid backup can be found (76 percent), when data recovery is faster and cheaper than recreating the lost data in-house (75 percent), and when an operating system or directory structure becomes corrupt and critical data is lost (61 percent). Only 19 percent say they would never engage a third-party service because it represents too much of a security risk.

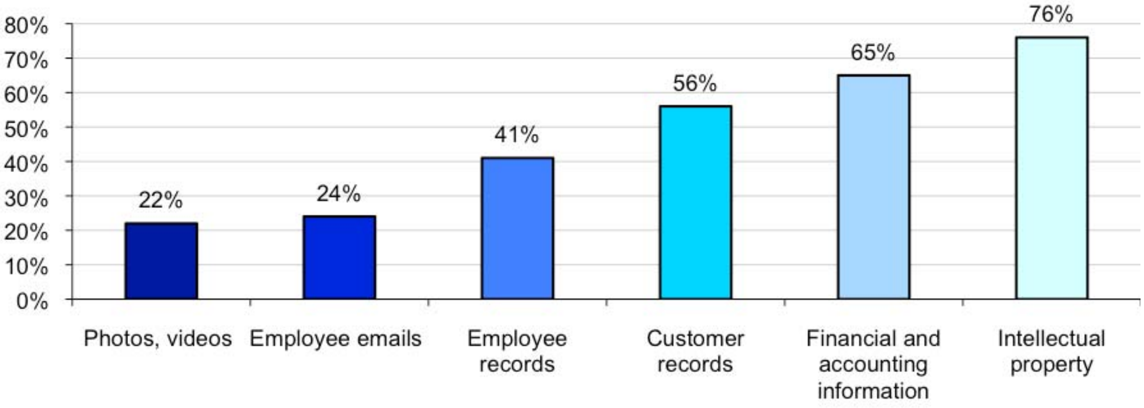
As shown in Bar Chart 3, 79 percent of respondents say their organizations have used and will continue to use a third-party to recover lost data. Thirty-three percent say they use a third-party one or more times each week, 26 percent say they use a third-party once each month, 14 percent say they use a third-party about once each quarter and 6 percent say it is about once over the past 12 months.

Bar Chart 3
How many times did your organization use a third-party data recovery service provider?



According to Bar Chart 4, organizations are most likely to use third-party services when recovery pertains to data files containing their most sensitive and confidential information. The top three data files sent to third-parties for recovery are an organization's intellectual property, financial and accounting information and customer records.

Bar Chart 4
What types of lost data warrant the use of a data recovery service provider?

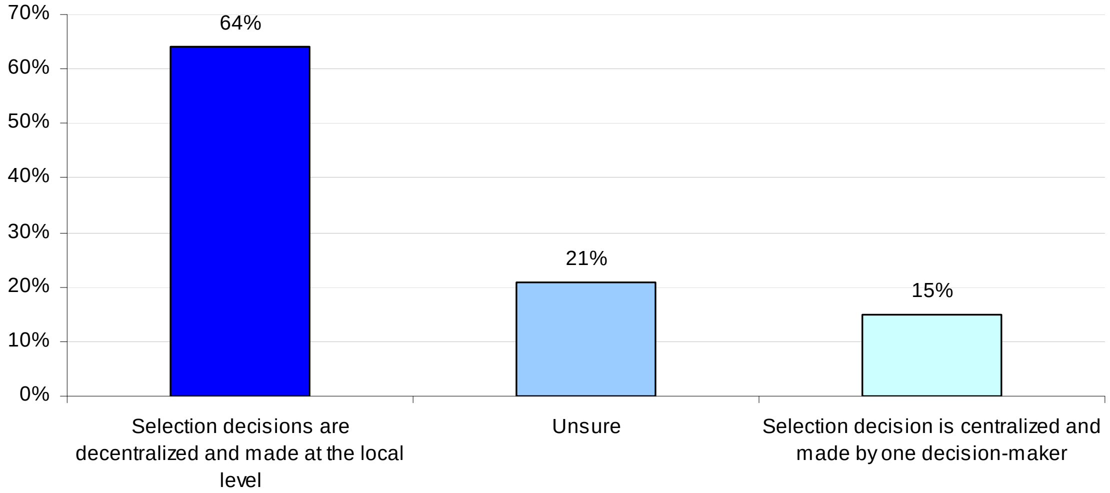


Selection of a Data Recovery Service Provider

As critical as security should be when engaging an outside data recovery service provider, the findings indicate it is not a priority in the vendor selection process. In fact, 69 percent do not have or are unsure they have a policy for ensuring the protection of data during the recovery process.

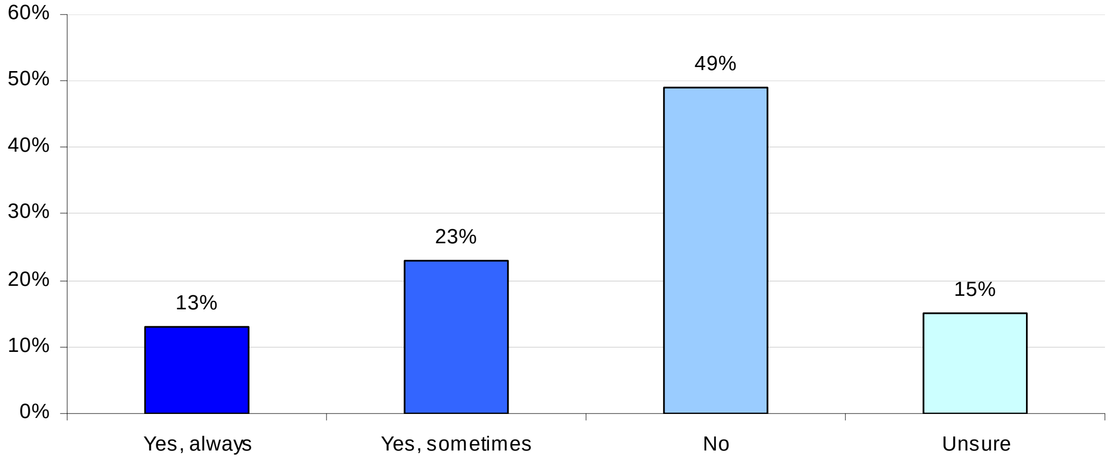
The process of selecting a third-party data recovery service is most often decentralized and made at the local level (64 percent of respondents), as shown in Bar Chart 5. However, 21 percent of respondents are unsure how the vendor is selected. Only 15 percent report selection is made by one decision-maker.

Bar Chart 5
When data recovery services are required, how is the vendor selected?



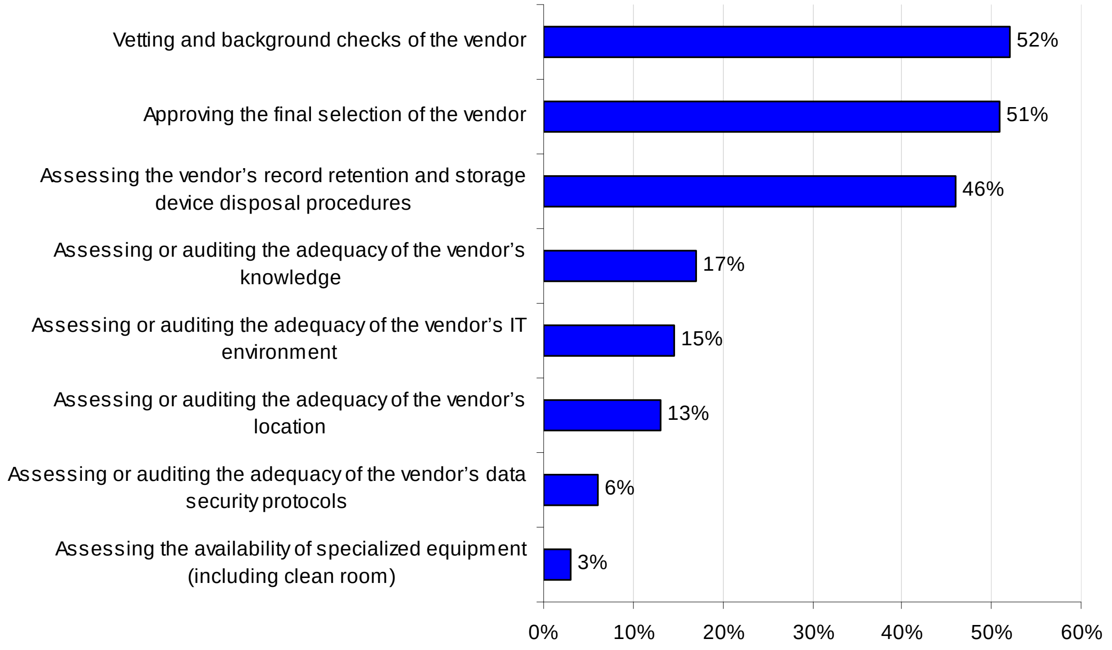
Bar Chart 6 shows almost half of respondents (49 percent) say IT security is not involved in selecting the third-party data recovery services and 15 percent are unsure.

Bar Chart 6
Is IT security involved in selecting the third party data recovery service provider?



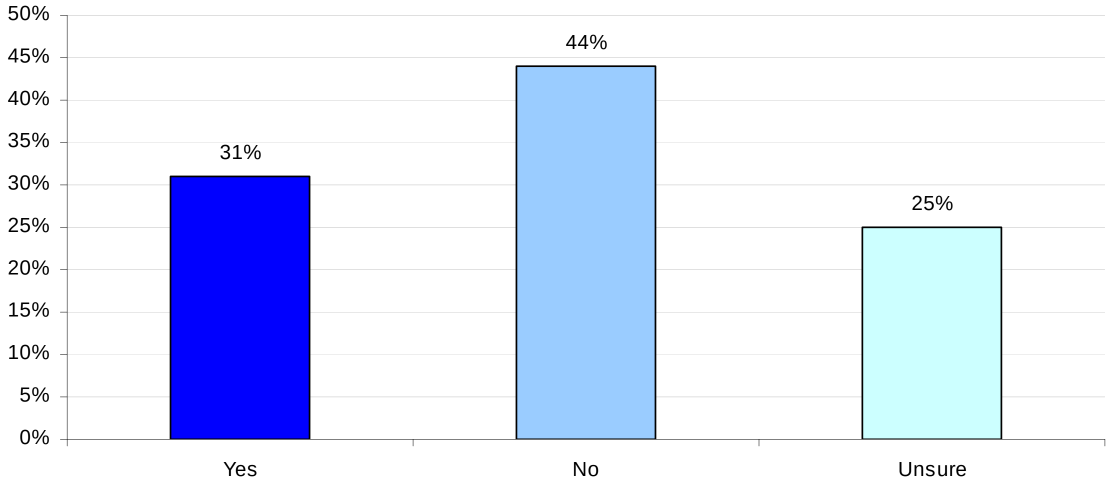
Those who say IT security practitioners are always involved (13 percent of respondents) or sometimes involved (23 percent of respondents) say they most often vet and conduct background checks, approve the final selection of the vendor and assess the vendor's record retention and storage device disposal procedures. See Bar Chart 7.

Bar Chart 7
How is IT security involved in the selection process of a data recovery service provider?



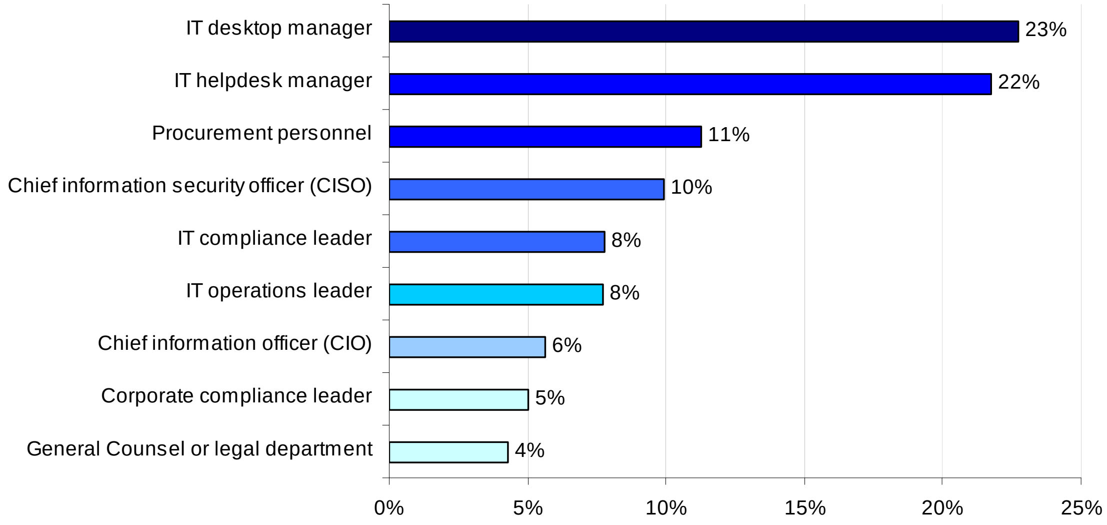
Only 31 percent say their organization has a policy for ensuring sensitive or confidential information is adequately protected during data recovery operations at a third-party vendor. In addition, as shown in Bar Chart 8, another 25 percent said they are unsure about whether such a policy exists within their organizations.

Bar Chart 8
Does your organization have a policy for ensuring sensitive or confidential information is adequately protected during data recovery operations at a third-party vendor?



Bar Chart 9 lists different functional areas that are responsible for ensuring data recovery providers are safe and secure. According to the findings, the person most responsible for vetting data recovery service providers is the IT desktop manager (23 percent) or the IT helpdesk manager (22 percent). Only 11 percent of procurement personnel are involved in the evaluation of vendors, and only 10 percent of chief information security officers (CISOs) and 6 percent of chief information officers (CIOs) are involved in the evaluation process.

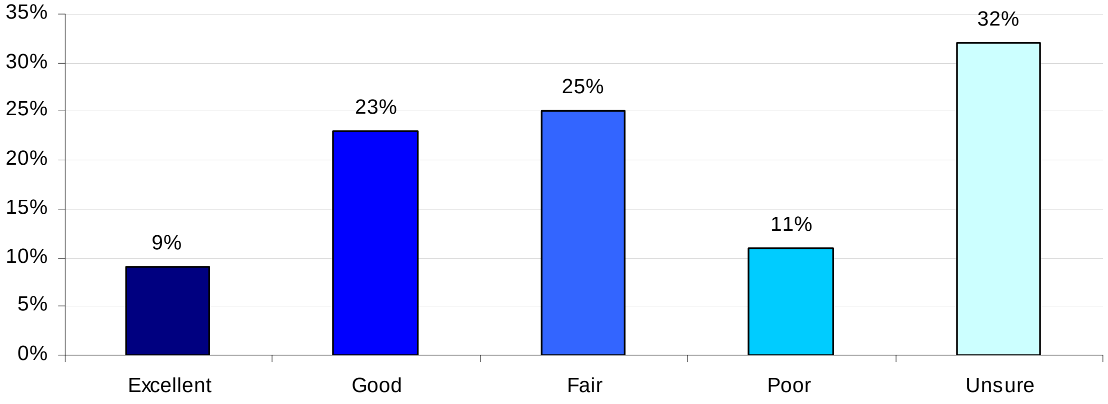
Bar Chart 9
Who in your organization is most responsible for vetting data recovery providers?



The above findings show that most often the evaluation and selection of third-party vendors is decentralized and IT security very often is not involved. The lack of clear responsibility and accountability for this process could suggest that there is little awareness of the importance of security in the data recovery process.

In support of this assertion, Bar Chart 10 summarizes how respondents rate their company's vetting process for selecting a secure third-party data recovery service provider. Specifically, 32 percent of respondents are unsure about their organization's third-party vetting process for selecting a secure third-party data recovery service provider. Only 9 percent rate the vetting process as excellent, 23 percent say it is good, 25 percent say it is fair and 11 percent believe their organization's vetting process is poor or non-existent.

Bar Chart 10
How would you rate your company's vetting process?

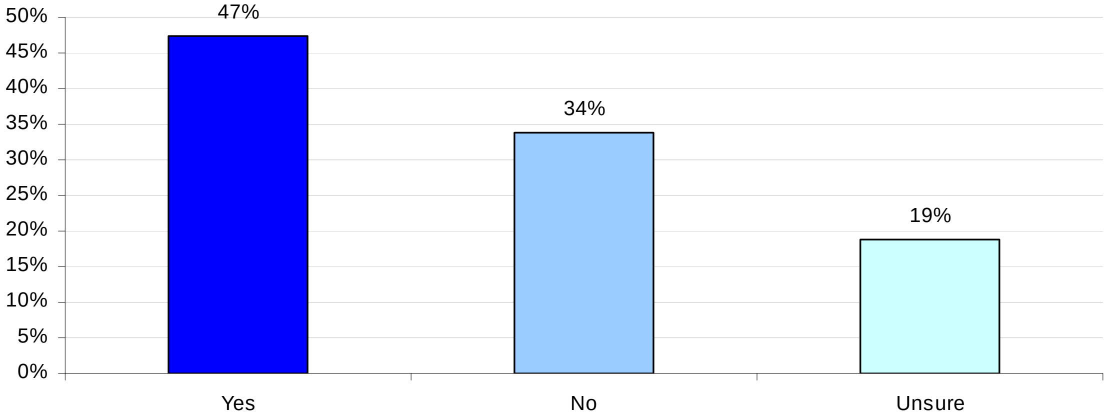


Risks to Confidential and Sensitive Data

The findings below reveal areas of risk to confidential and sensitive data in the data recovery process. For example, damaged or failed devices may not be disposed of properly. Other concerns include negligent or incompetent data recovery technicians and uncertainty if the third-party vendor properly vets its employees to ensure there are no criminals such as identity thieves.

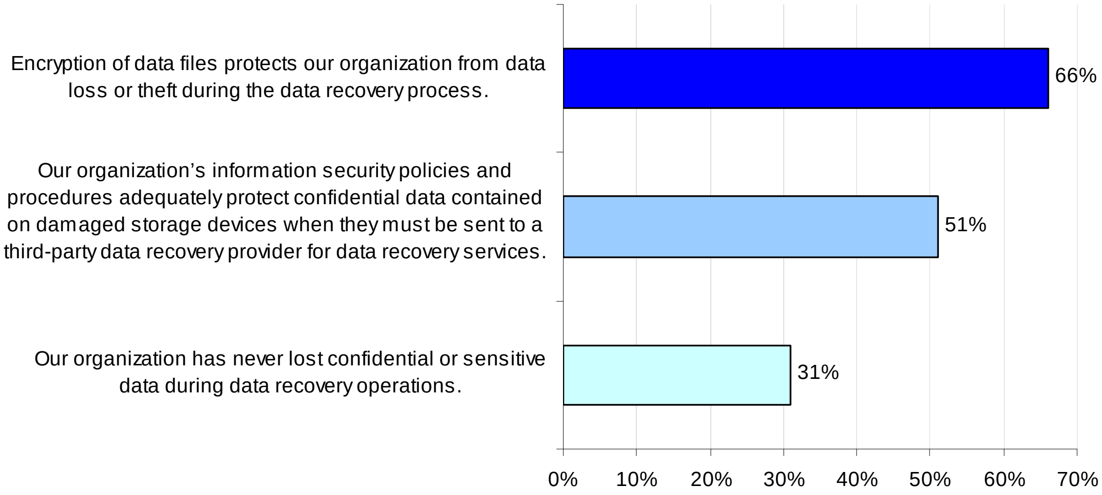
According to Bar Chart 11, 34 percent of respondents report their organization does not have a process for disposing of damaged or failed devices containing sensitive or confidential information after they are no longer needed and 19 percent are unsure.

Bar Chart 11
Does your organization have a process for disposing of damaged or failed devices?



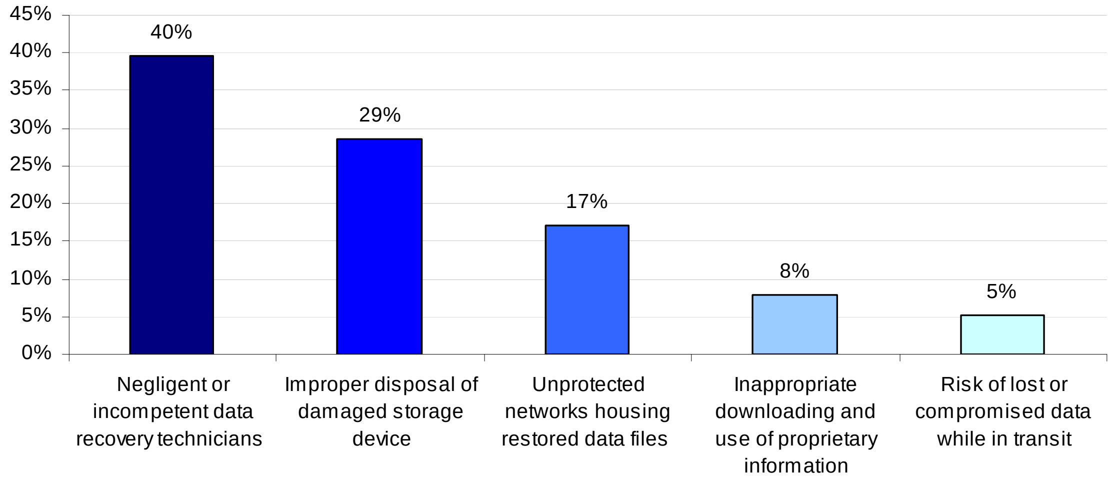
Fifty-one percent of respondents strongly agree or agree their organization's information security policies and procedures adequately protect confidential data contained on damaged storage devices when sent to a third-party for data recovery services. However, only 31 percent of respondents strongly agree or agree their organizations have never lost confidential or sensitive data during data recovery operations. Sixty-six percent strongly agree or agree that encryption protects the data from loss or theft during the recovery process.

Bar Chart 12
Three attributions about organizations' security posture
Strongly agree and agree response combined



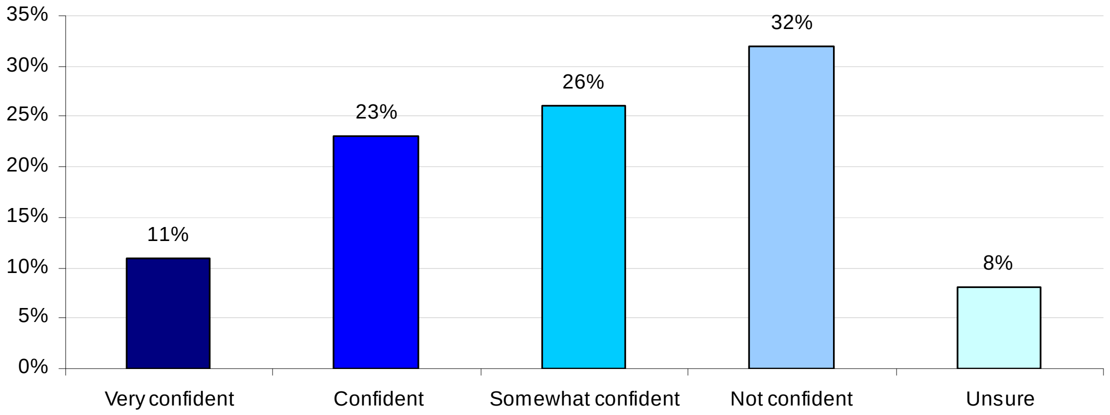
According to Bar Chart 13, the biggest threats to sensitive and confidential data on a failed storage device sent to a third-party data recovery service provider are negligent or incompetent data recovery technicians (40 percent of respondents) followed by improper disposal of a damaged storage device (29 percent).

Bar Chart 13
What do you see as the most significant threats to confidential data on that device?



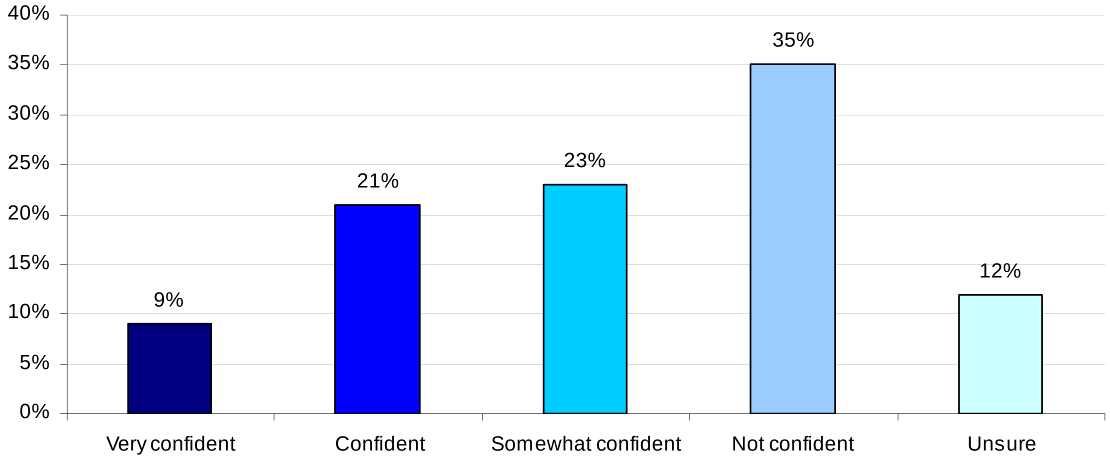
Bar Chart 14 shows 40 percent are not confident (32 percent) or unsure (8 percent) that their third-party data recovery service provider – without prior knowledge – could employ “would be” contractors who might engage in illegal activities such as identity theft.

Bar Chart 14
How confident are you that a recovery service provider does not employ criminals?



As discussed previously, a majority of respondents are unsure if a breach occurred as a result of a drive in the possession of a third-party data recovery service provider. Forty-seven percent of respondents say they are not confident or unsure that the third-party would advise them of a data breach resulting from error or mistakes. As noted in Bar Chart 15, only 9 percent are very confident they would be notified in the event of a data breach.

Bar Chart 15
How confident are you that a recovery service provider would inform you of a data breach?

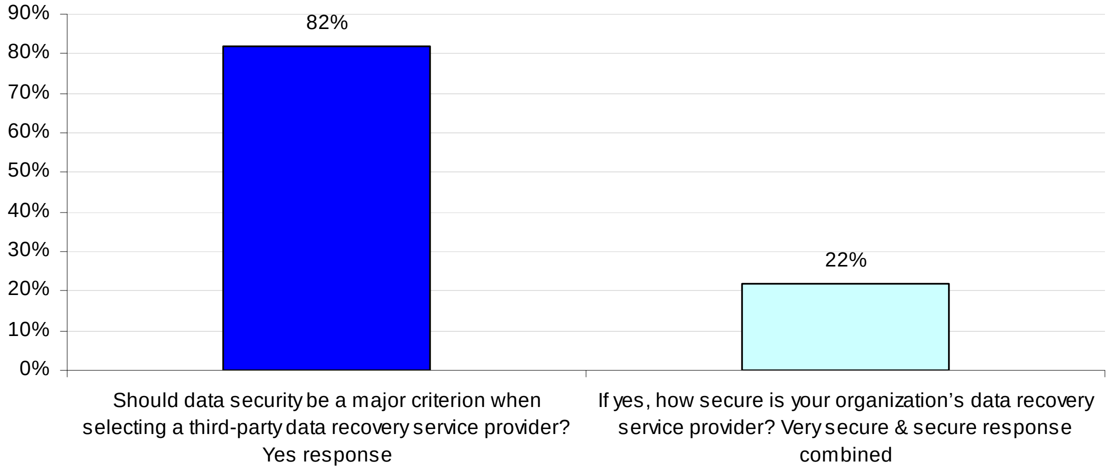


Security Practices of Data Recovery Service Providers

Our study indicates organizations are taking unnecessary risks because they are not doing a thorough examination of their data recovery service providers. The findings suggest there is awareness of the problem and immediate and simple steps can be taken to reduce these risks.

Bar Chart 16 summarizes the results of two questions. First, the chart shows 82 percent of respondents believe data security should be a major criterion when selecting a third-party data recovery service provider. However, only 22 percent of respondents say their organization's data recovery service provider is either very secure or secure.

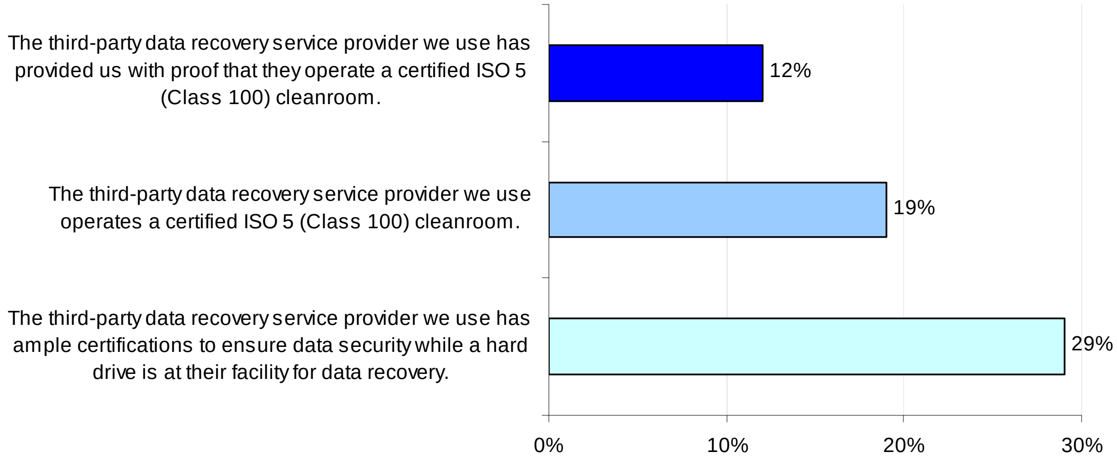
Bar Chart 16
Should data security be a major criterion in choosing a data recovery service provider?



As shown in Bar Chart 17, the majority of respondents either report their organization's third-party data recovery service provider does not have the following qualifications or they are unsure: certifications to ensure data security while a hard drive is at their facility and proof they operate a certified ISO 5 (Class 100) clean room.

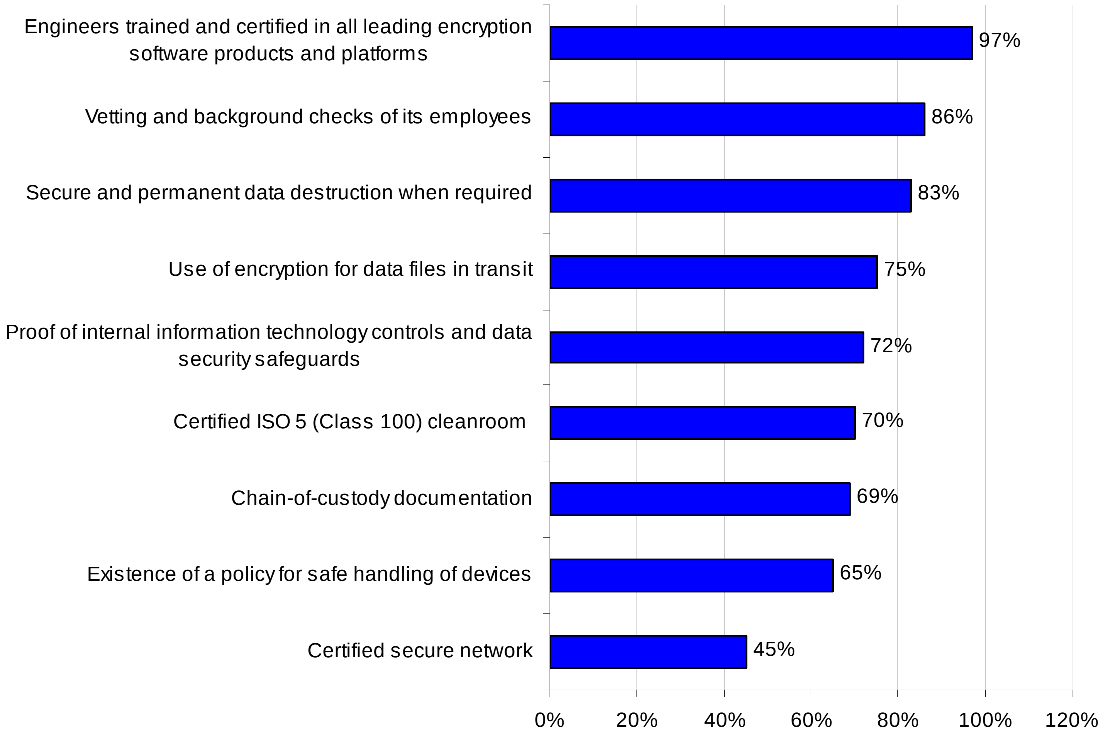
Bar Chart 17
Does the data recovery service provider have adequate qualifications or facilities?

Percentage Yes response



Eighty-one percent of IT practitioners in our study are unsure about any of the security protocols their organization requires the vendor to provide. However, respondents believe the following security protocols should be in place.

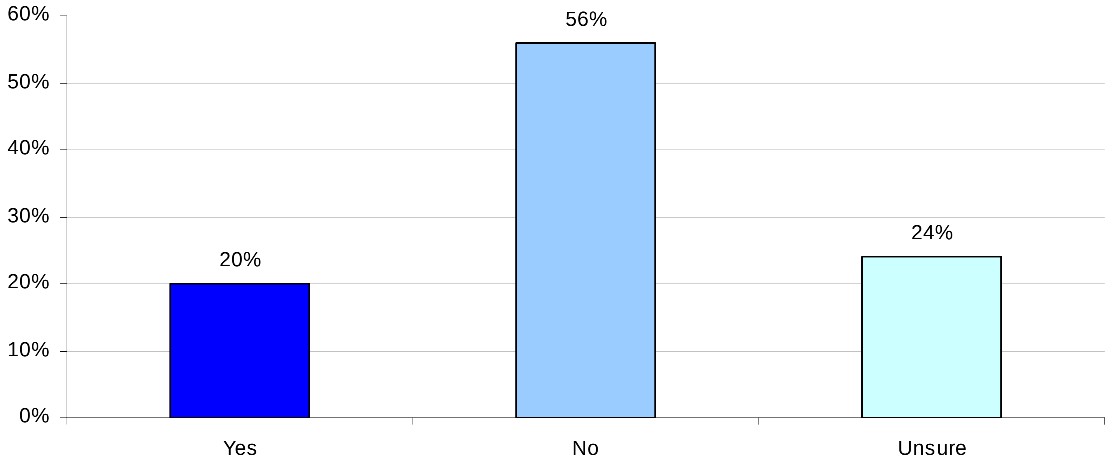
Bar Chart 18
What security protocols should be in place?



Bar Chart 18 shows that the top three security protocols that should be in-place are: assurances that engineers are trained and certified in all leading encryption software products and platforms (97 percent), vetting and background checks of its employees (86 percent), secure and permanent data destruction when required (83 percent).

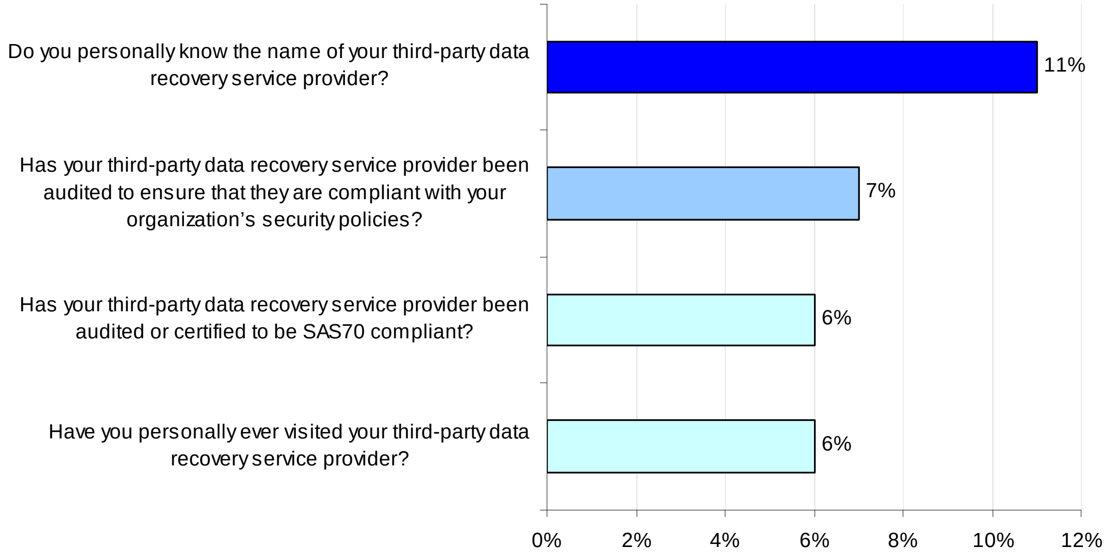
While 82 percent say data security should be a major criterion in the vetting and selection process for data recovery services (see Bar Chart 16), only 20 percent of respondents say data security is a major criterion in their organizations today. See Bar Chart 19.

Bar Chart 19
Is data security a major criterion when selecting a data recovery service provider?



As shown in Bar Chart 20, only 11 percent of respondents know the name of their data recovery service provider and only 6 percent have personally visited their third-party data recovery service. Only 7 percent say their data recovery service provider has been audited to ensure they are compliant with security policies, and only 6 percent say their vendor has been audited or certified to be SAS 70 compliant.

Bar Chart 20
Other questions and relevant criteria
Percentage Yes response



III. Methods

A random sampling frame of 11,805 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of experienced IT security and IT support practitioners.

Table 1: Response statistics	Freq.
Total sampling frame	11,805
Sent to subjects	10,032
Bounce backs	1670
Returns	813
Rejects	119
Net returns	694
Response rate	5.9%

As shown in Table 1, 813 respondents completed the survey. Of the returned instruments, 119 surveys failed reliability checks. A total of 694 surveys were used as our final sample, which represents a 5.9 percent net response rate. One screening question was used to ensure respondents had experience with data recovery services, resulting in a reduced sample size of 636 individuals.

Table 2 reports the respondent's organizational level within participating organizations. As can be seen, 59 percent of respondents are at or above the supervisory levels.

Table 2: Respondents' organizational level	Pct%
Director	18%
Manager	30%
Supervisor	11%
Associate/Staff	16%
Technician	25%
Total	100%

Table 3 shows that the most frequently cited reporting channels among respondents are the CIO (43 percent), CISO (21 percent) and CSO (12 percent).

Table 3: Respondents' primary reporting channel	Pct%
Chief Information Officer	43%
Chief Information Security Officer	21%
Chief Security Officer	12%
Chief Technology Officer	9%
Chief Risk Officer	5%
Chief Financial Officer	3%
Compliance Leader	3%
Chief Privacy Officer	3%
CEO/Executive Committee	1%
Total	100%

Table 4 reports the worldwide headcount of participating organizations. It reports that 49 percent of respondents are located in organizations with more than 5,000 employees.

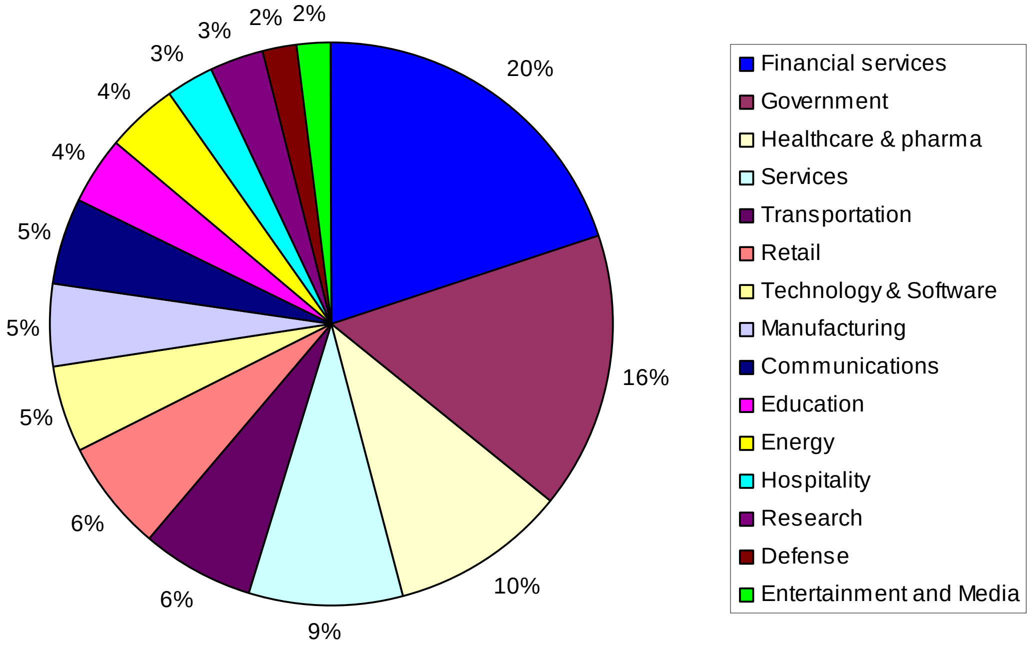
Table 4: Worldwide headcount of respondents' organizations	Pct%
Less than 500 people	10%
500 to 1,000 people	15%
1,001 to 5,000 people	26%
5,001 to 25,000 people	20%
25,001 to 75,000 people	18%
More than 75,000 people	11%
Total	100%

Table 5 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States.

Table 5: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	54%
Europe	51%
Asia-Pacific	26%
Latin America (including Mexico)	20%

Pie Chart 1 reports the industry distribution of respondents' organizations. As shown, financial services (including retail banking, insurance, brokerage and payments), government (federal, state and local), and healthcare and pharmaceuticals are the three largest industry segments.

Pie Chart 1
Industry distribution of respondents' organizations



On average, respondents had 9.15 years of overall experience in either the IT security and IT support practitioner fields. They also had, on average, 3.59 in their present position. Additional details about this sample are provided in Appendix I of this paper.

IV. 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 in IT security and IT support practitioners located in the United States, 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 sample is representative of individuals in the IT security and IT support practitioner fields. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents 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 certain respondents did not provide accurate responses.

V. Conclusion

Confidential and privacy-protected information is at risk because organizations do not have the proper security protocols in place when using third-party data recovery service providers. IT security and IT support respondents in our study admit they have not been involved in the selection of these vendors. Instead the selection process has been delegated, in many cases, to the IT desktop or IT helpdesk manager.

Organizations can take simple and immediate steps to ensure a data breach does not occur during the recovery process. Policies and procedures should be created and enforced when using third-parties. These policies and procedures should address the safe handling of drives and devices by data recovery service providers.

Before putting a device or drive at risk, we recommend organizations make sure their data recovery service provider has the following in place:

- Proof of internal information technology controls and data security safeguards such as compliance with SAS 70 Audit Reports
- Engineers trained and certified in all leading encryption software products and platforms
- Proof of chain-of-custody documentation and certified secure network
- Vetting and background checks of its employees
- Secure and permanent destruction when required
- Use of encryption for data files in transit
- Proof of Certified ISO 5 (Class 100) clean room

By following these recommended security protocols, organizations can quickly gain control over a practice that is putting sensitive and confidential data at risk.

Appendix 1: Detailed Survey Results

Audited findings presented by Dr. Larry Ponemon, October 22, 2009

The following table summarizes the sample response for the present study. The sample response rate is 5.9% (which is a very strong result relative to other studies using a similar panel).

Response statistics	Freq.
Total sampling frame	11,805
Sent to subjects	10,032
Bounce backs	1,670
Returns	813
Rejects	119
Net returns	694
Response rate	5.9%

One screening question was used to refine the sample. This resulted in the removal of 58 respondents, and a final sample size of 636 individuals.

S1. Are you involved in your organization's data security or data recovery operations?	Freq.
Yes (final sample)	636
No	58
Total	694

Q1. How often do these scenarios happen in your organization?

1=frequently, 2=not frequently, 3 = rarely, 4=never, 5=unsure	Frequently%
Q1a. A desktop or laptop computer's hard disk crashes and its contents are not backed-up.	87%
Q1b. Data is corrupted because of a software glitch and there is no backup.	53%
Q1c. Data recovery operations are unsuccessful, resulting in the permanent loss of information.	52%
Q1d. Data storage is corrupted because the wrong software recovery utility was used.	36%

Q2. How is data recovery accomplished within your organization?	Pct%
Mostly done In-house	44%
One primary third-party data recovery service provider	12%
Multiple third-party data recovery service providers	35%
Unsure	9%
Total	100%

Q3. In the past 12 months, how many times did your organization use a third-party data recovery service provider to recover lost data?	Pct%
None	21%
About once over the past 12 month	6%
About once each quarter	14%
About once each month	26%
About one or more times each week	33%
Total	100%

Q4. Typically, what kinds of data files warrant third-party data recovery services (if they are damaged or lost and a back up copy is not available)? Please select the top three choices based on your recent experiences.	Pct%
Customer records	56%
Employee records	41%
Employee e-mails	24%
Financial and accounting information	65%
Intellectual property (including source code)	76%
Photos, videos	22%
Other (please specify)	5%
Unsure	4%
Total	293%

Q5. When professional data recovery services are required, how is the third-party vendor selected?	Pct%
Selection decisions are decentralized and made at the local level	64%
Selection decision is centralized and made by one decision-maker	15%
Unsure	21%
Total	100%

Q6. When professional data recovery services are required, who is most responsible for selecting and working with the third-party data recovery service provider?	Pct%
Senior-level IT management	7%
Middle-level IT management	12%
IT security management	12%
IT desktop manager	30%
IT helpdesk manager	24%
Procurement personnel	5%
Other (please specify)	1%
Unsure	9%
Total	100%

Q7. Who in your organization is most responsible for vetting third-party data recovery providers?	Pct%
Chief information officer (CIO)	6%
Chief technology officer (CTO)	0%
Chief information security officer (CISO)	10%
Chief privacy officer (CPO)	0%
Corporate compliance leader	5%
General Counsel or legal department	4%
IT compliance leader	8%
IT operations leader	8%
IT desktop manager	23%
IT helpdesk manager	22%
Procurement personnel	11%
Other (please specify)	0%
Unsure	4%
Total	100%

Q8a. Is IT security involved in selecting the third-party data recovery service provider?	Pct%
Yes, always	13%
Yes, sometimes	23%
No	49%
Unsure	15%
Total	100%

Q8b. If yes, how is IT security involved in the selection process of a data recovery service provider? Check all that apply:	Pct%
Vetting and background checks of the vendor	52%
Assessing or auditing the adequacy of the vendor's knowledge	17%
Assessing or auditing the adequacy of the vendor's location	13%
Assessing or auditing the adequacy of the vendor's IT environment	15%
Assessing or auditing the adequacy of the vendor's data security protocols	6%
Assessing the availability of specialized equipment (including clean room)	3%
Assessing the vendor's record retention and storage device disposal procedures	46%
Approving the final selection of the vendor	51%
Other (please specify)	0%
Total	203%

Q9. Does your organization have a process for disposing of damaged or failed devices containing sensitive or confidential information after they are no longer needed?	Pct%
Yes	47%
No	34%
Unsure	19%
Total	100%

Q10. **Attributions:** Please rate each one of the following statements using the opinion scale from "strongly agree" to "strongly disagree" below each item.	SA & A combined
Q10a. Our organization can handle data recovery without the assistance of outside specialists or experts.	53%
Q10b. Our organization has never lost confidential or sensitive data during data recovery operations.	31%
Q10c. Our disaster recovery plan adequately addresses our organization's data recovery operations.	63%
Q10d. Our organization's information security policies and procedures adequately protect confidential data contained on damaged storage devices when they must be sent to a third-party data recovery provider for data recovery services.	51%
Q10e. Encryption of data files protects our organization from data loss or theft during the data recovery process.	66%
Q10f. All third-party data recovery service providers offer the same capabilities and security protocols.	54%
Q10g. Our organization's information security department oversees the security of data recovery operations.	47%

Q11. **Attributions:** Please rate each one of the following statements using the frequency scale from “very frequently” to “unsure” below each item.	Unsure%
Q11a. Lack of security at a third-party data recovery service provider has resulted in the loss or theft of our sensitive/confidential business information.	43%
Q11b. Our third-party data recovery service provider improperly disposed of a data storage device that still contained sensitive or confidential information.	45%

Q12. In your organization, data recovery is best associated with what IT or business operation:	Pct%
Data backup	34%
Disaster recovery	29%
Data recovery is its own process	17%
Other (please specify)	20%
Total	100%

Q13. When would your organization engage a third-party data recovery service provider? Check all that apply:	Pct%
When a data storage device fails and no valid backup can be found.	76%
When an operating system or directory structure becomes corrupt and critical data is lost.	61%
When data recovery is faster and cheaper than recreating the lost data ourselves.	75%
We never would engage a third-party service because our data is always backed up.	16%
We never would engage a third-party service because it represents too much of a security risk.	19%
Total	247%

Q14. When using a third-party data recovery service provider, how confident are you that all your data will be recovered?	Pct%
Very confident	19%
Confident	28%
Somewhat confident	29%
Not confident	20%
Unsure	4%
Total	100%

Q15. Does your organization have a policy for ensuring sensitive or confidential information is adequately protected during data recovery operations at a third-party vendor?	Pct%
Yes	31%
No	44%
Unsure	25%
Total	100%

Q16. With respect to the protection of sensitive or confidential data during data recovery, how would you rate your company's vetting process for selecting a secure third-party data recovery service provider?	Pct%
Excellent	9%
Good	23%
Fair	25%
Poor	11%
Unsure	32%
Total	100%

Q17. The third-party data recovery service provider we use has ample certifications to ensure data security while a hard drive is at their facility for data recovery.	Pct%
Yes	29%
No	21%
Unsure	50%
Total	100%

Q18. The third-party data recovery service provider we use operates a certified ISO 5 (Class 100) cleanroom.	Pct%
Yes	19%
No	18%
Unsure	63%
Total	100%

Q19. The third-party data recovery service provider we use has provided us with proof that they operate a certified ISO 5 (Class 100) cleanroom.	Pct%
Yes	12%
No	31%
Unsure	57%
Total	100%

Q20a. Has your organization experienced a data breach involving the loss or theft of personal information sometime over the past two years?	Pct%
Yes, only one incident	29%
Yes, two to five incidents	35%
Yes, more than five incidents	19%
No	17%
Total	100%

Q20b. If yes, how many incidents of data breach occurred when a drive was in the possession of a third-party data recovery service provider?	Pct%
One incident	6%
Two to five incidents	8%
More than five incidents	5%
Unsure	81%
Total	100%

Q20c. Was this data breach incident due to the data recovery service provider's lack of security protocols?	Pct%
Yes	43%
No	29%
Unsure	28%
Total	100%

Q21. When a failed storage device must be sent to a third-party data recovery service provider, what do you see as the **most significant** threats to the sensitive or confidential data on that device? Please select no more than two threats.	Pct%
Negligent or incompetent data recovery technicians	40%
Inappropriate downloading and use of proprietary information	8%
Unprotected networks housing restored data files	17%
Risk of lost or compromised data while in transit	5%
Improper disposal of damaged storage device	29%
Other (please specify)	2%
Total	100%

Q22a. When using a third-party data recovery service provider, how confident are you that they would advise you of a data breach resulting from their error or mistakes?	Pct%
Very confident	9%
Confident	21%
Somewhat confident	23%
Not confident	35%
Unsure	12%
Total	100%

Q22b. When using a third-party data recovery service provider, how confident are you that they do not employ criminals such as identity thieves?	Pct%
Very confident	11%
Confident	23%
Somewhat confident	26%
Not confident	32%
Unsure	8%
Total	100%

Q23a. In general, what security protocols **do you require** your third-party data recovery service provider follow when they are in possession of your damaged data storage device? Please check all that apply.	Pct%
Vetting and background checks of its employees	18%
Existence of a policy for safe handling of devices	16%
Use of encryption for data files in transit	19%
Certified ISO 5 (Class 100) cleanroom	13%
Chain-of-custody documentation	15%
Certified secure network	8%
Proof of internal information technology controls and data security safeguards	5%
Engineers trained and certified in all leading encryption software products and platforms	18%
Secure and permanent data destruction when required	6%
Other (please specify)	0%
Unsure about any of the above procedures being required	81%
Total	199%

Q23b. In general, what security protocols **should you require** your third-party data recovery service provider follow when they are in possession of your damaged data storage device? Please check all that apply.	Pct%
Vetting and background checks of its employees	86%
Existence of a policy for safe handling of devices	65%
Use of encryption for data files in transit	75%
Certified ISO 5 (Class 100) cleanroom	70%
Proof of chain-of-custody documentation	69%
Certified secure network	45%
Proof of internal information technology controls and data security safeguards	72%
Engineers trained and certified in all leading encryption software products and platforms	97%
Secure and permanent data destruction when required	83%
Other (please specify)	3%
Total	665%

Q24a. Is data security a major criteria when selecting a third-party data recovery service provider?	Pct%
Yes	20%
No	56%
Unsure	24%
Total	100%

Q24b. **Should** data security be a major criteria when selecting a third-party data recovery service provider?	Pct%
Yes	82%
No	7%
Unsure	11%
Total	100%

Q24c. If yes (Q24a), how secure is your organization's data recovery service provider?	Pct%
Very secure	10%
Secure	12%
Adequate	24%
Not secure	28%
Unsure	26%
Total	100%

Q25a. Do you personally know the name of your third-party data recovery service provider?	Pct%
Yes	11%
No	89%
Total	100%

Q25b. Have you personally ever visited your third-party data recovery service provider?	Pct%
Yes	6%
No	94%
Total	100%

Q25c. Has your third-party data recovery service provider been audited to ensure that they are compliant with your organization's security policies?	Pct%
Yes	7%
No	45%
Unsure	48%
Total	100%

Q25d. Has your third-party data recovery service provider been audited or certified to be SAS70 compliant?	Pct%
Yes	6%
No	49%
Unsure	45%
Total	100%

Demographics & organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	0%
Director	18%
Manager	30%
Supervisor	11%
Associate/Staff	16%
Technician	25%
Other (please specify)	0%
Total	100%

D2. Check the **Primary Person** you or your IT organization reports into within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer	3%
General Counsel	0%
Chief Information Officer	43%
Chief Technology Officer	9%
Compliance Leader	3%
Human Resources VP	0%
Chief Security Officer	12%
Chief Information Security Officer	21%
Chief Privacy Officer	3%
Chief Risk Officer	5%
Other (please specify)	0%
Total	100%

D3a. Experience in IT or IT security	9.15
D3b. Years in present position	3.59

D4. What industry best describes your organization’s industry focus?	Pct%
Airlines	2%
Automotive	2%
Brokerage & Investments	3%
Communications	3%
Chemicals	0%
Credit Cards	3%
Defense	2%
Education	4%
Energy	4%
Entertainment and Media	2%
Federal Government	10%
Food Service	1%
Healthcare	7%
Hospitality	3%

Manufacturing	5%
Insurance	3%
Internet & ISPs	2%
State or Local Government	6%
Pharmaceuticals	3%
Professional Services	4%
Research	3%
Retailing	5%
Retail Banking	11%
Services	5%
Technology & Software	5%
Transportation	2%
Total	100%

D5. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	54%
Europe	51%
Asia-Pacific	26%
Latin America (including Mexico)	20%

D6. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	10%
500 to 1,000 people	15%
1,001 to 5,000 people	26%
5,001 to 25,000 people	20%
25,001 to 75,000 people	18%
More than 75,000 people	11%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.