Ponemon INSTITUTE

Perceptions about Self-Encrypting Drives: A Study of IT Practitioners

Sponsored by Trusted Computing Group

Independently conducted by Ponemon Institute LLC

Publication Date: May 2011

Perceptions about Self-Encrypting Drives:
A Study of IT Practitioners

Ponemon Institute, May 2011

Part 1. Introduction

Organizations are using encryption to mitigate the damage caused by data breaches, comply with privacy and data protection regulations and preserve brand and reputation. However, there are many approaches and strategies for deploying encryption across the enterprise. The purpose of *Perceptions about Self-Encrypting Drives: A Study of IT Practitioners,* conducted by Ponemon Institute and sponsored by the Trusted Computing Group (TCG), is to understand organizations' use of hardware-based encryption technologies, including self-encrypting hard and solid state drives.

Self-encrypting drives (SEDs) are a recent addition to the technologies used to protect stored data on drives. TCG published final specifications for client drives, data center drives and interoperability of self-encrypting drives in January 2009 and are widely supported by PC, server drive and applications providers. In March 2009, hard drive vendors started shipping self-encrypting drives based on TCG's specifications.

The study surveyed 517 IT practitioners with an average of 10 years experience, most of whom report directly to the CIO or CISO in their organizations. To ensure a knowledgeable panel of respondents, only those who are familiar with SEDs were selected to complete the survey. All of the respondents work in organizations that use hardware-based and/or software-based encryption technologies.

More than one-third (37 percent) of respondents describe their information security and data protection as being at the late middle or mature stage. Those stages are achieved when the IT function begins to evaluate the effectiveness of key initiatives or they are focusing on program evaluation and refinement.

In the survey we included the following definition: *SEDs provide hardware-based data security and enhanced secure erase capability. SEDs continuously scramble data using a key as it is written to the drive and then descramble it with the key as it is retrieved, giving users a high level of data protection. It also speeds and simplifies the drive re-deployment process. By deleting the encryption key, the data is rendered unreadable, eliminating the need for time-consuming data-overwrite. The encryption logic is built into the drive electronics*.

Thirty-five percent of IT practitioners in our study report that they are very familiar with SEDs and 53 percent say they are somewhat familiar. Approximately 85 percent say their organizations mostly use software-based encryption. When we asked why they were not using hardware-based encryption, 36 percent say they do not understand the hardware-based encryption options available for their organizations. We believe this response can be due to the fact, as we noted above, that this option became available only recently.

An important finding of this study is that IT practitioners view hardware-based encryption favorably but are uncertain about the cost. However, 37 percent believe their organizations would pay a premium to gain the extra security SEDs promise.

The majority of respondents agree that in terms of protecting data-at-rest, hardware-based encryption (including SEDs) are more secure than software-based encryption. In fact, 70 percent say that SEDs would have had an enormous and positive impact on the protection of sensitive and confidential information in the event that a data breach should occur.

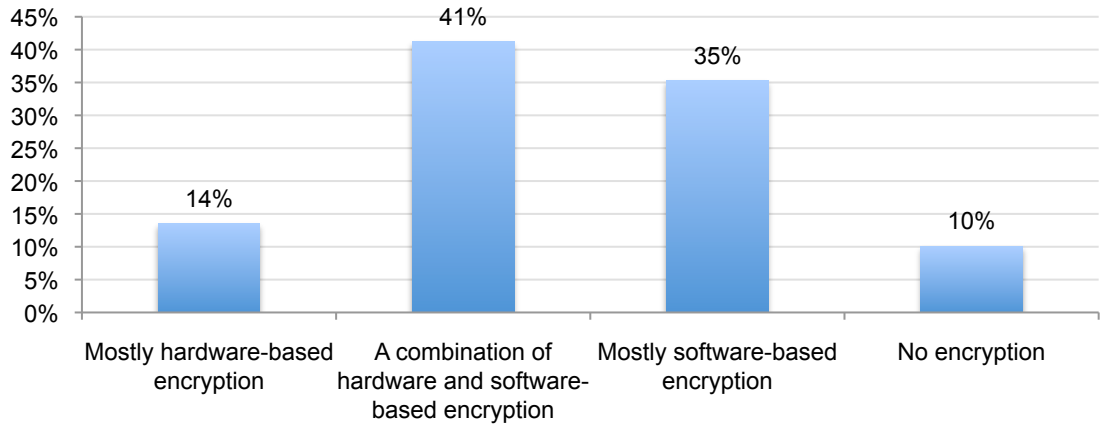
Based on Ponemon Institute's *2010 Annual Study: U.S. Cost of a Data Breach Study*[1], the average cost per lost or stolen record is $214. In this study, it was shown that organizations lost on average approximately 16,000 records from a data breach. This translates to a cost of about $3.4 million for each incident. We believe the results of this research should be very helpful in making the business case for investing in SEDs.

[1] See Ponemon Institute, 2010 Annual Study: US Cost of a Data Breach, sponsored by Symantec, February 2011

Part 2. Key Findings

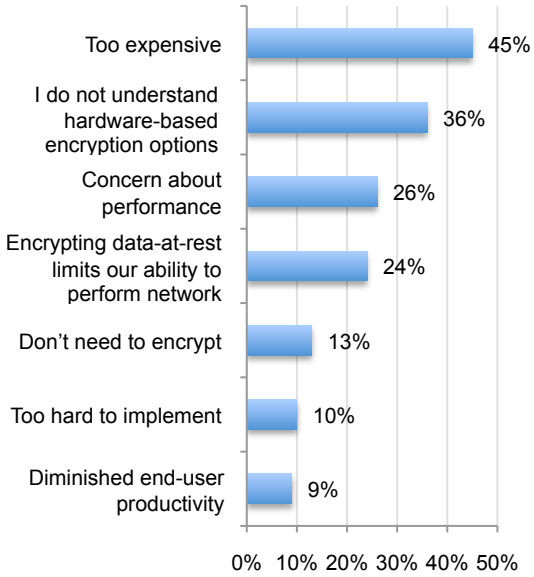
Why respondents are more likely to choose software-based vs. hardware-based encryption. As noted in Bar Chart 1, the majority of organizations use software-based encryption or a combination of hardware and software-based encryption. The most likely reasons for doing so are perceptions that it is less costly to implement and that they do not fully understand hardware-based encryption technology options available to their organization.

Bar Chart 1: Does your organization use hardware-based or software-based encryption for protecting stored data on drives?

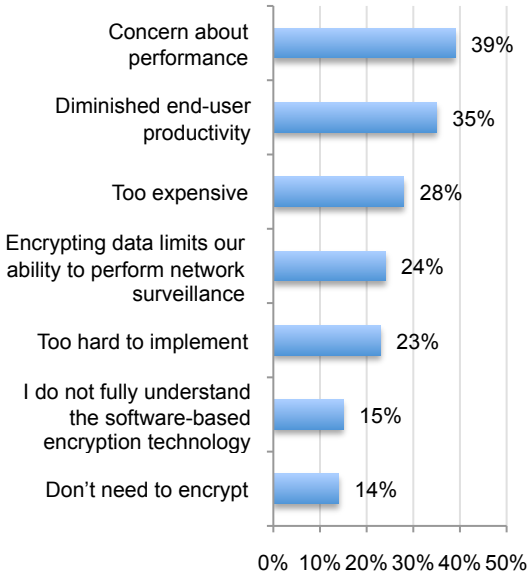


In contrast, those who seem to prefer hardware-based encryption believe it does not diminish end-user productivity and it is not too hard to implement. As a possible explanation as to why respondents hold these perceptions, SEDs have been available only for the past two years. Therefore, it seems as if IT practitioners need more awareness about the features and functionality of SEDs in order to make informed decisions.

Bar Chart 2: If your organization is not using hardware-based encryption, why not?

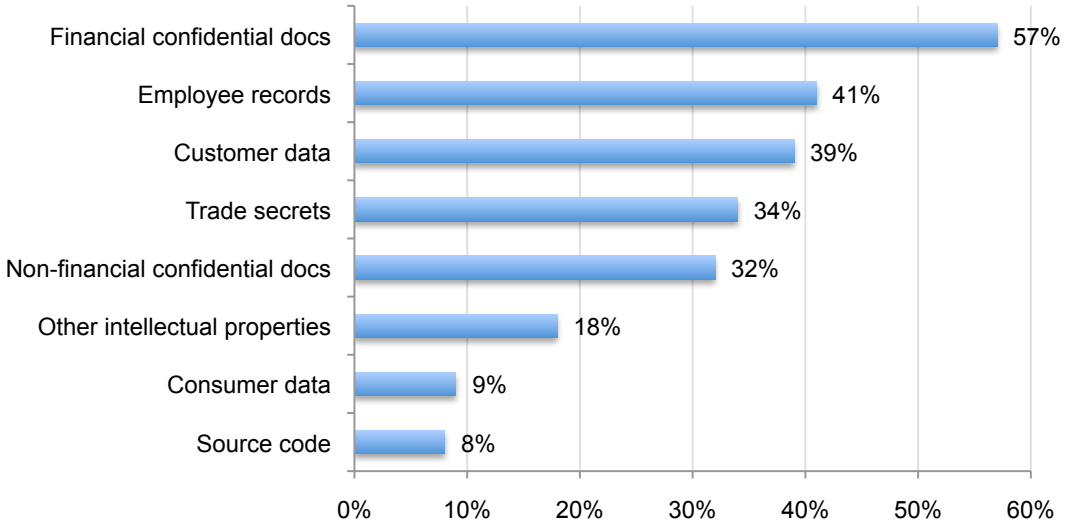


Bar Chart 3: If your organization is not using software-based encryption, why not?



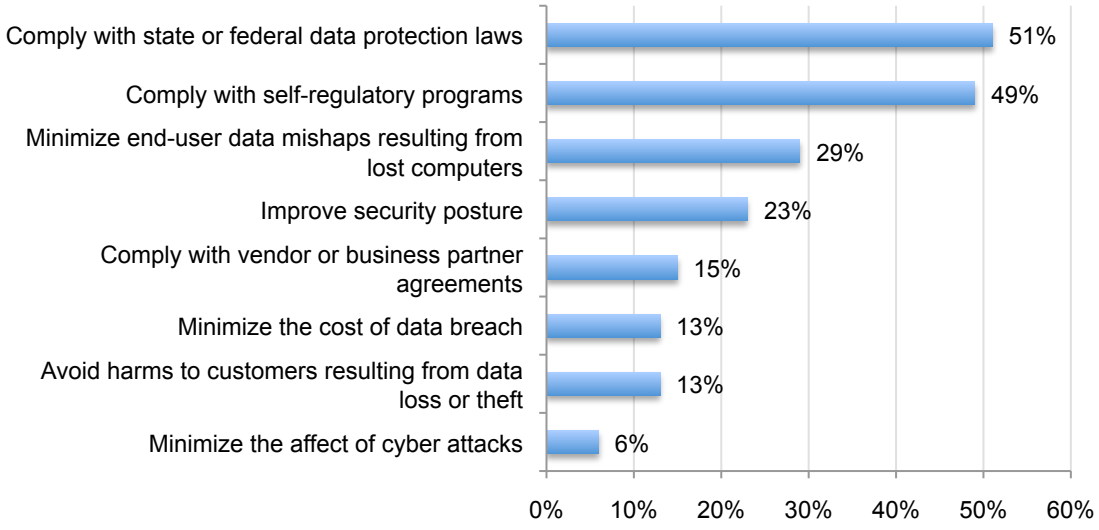
Compliance is the main driver for encrypting data-at-rest. Bar Chart 4 shows the top three types of data on drives (data-at-rest) that are normally encrypted, which include confidential financial documents, employee records and customer data. With the plethora of laws and regulations both at the state and federal level, this finding regarding compliance seems obvious.

Bar Chart 4: What types of stored data on drives (data-at-rest) are normally encrypted in your organization?



According to 51 percent IT practitioners, the main reason to encrypt data-at-rest is to comply with state or federal data protection laws followed by 49 percent who say their organization complies with self-regulatory programs such as PCI DSS, ISO, NIST and others. The state laws include the California Security Breach Notification Act, the recent Massachusetts and Nevada data privacy security and encryption laws as well as other state privacy laws. At the federal level, there are regulations such as the Health Insurance Portability and Accountability Act (HIPAA), including the Health Information Technology for Economic & Clinical Health Act (HITECH).

Bar Chart 5: Why does your organization encrypt data-at-rest?

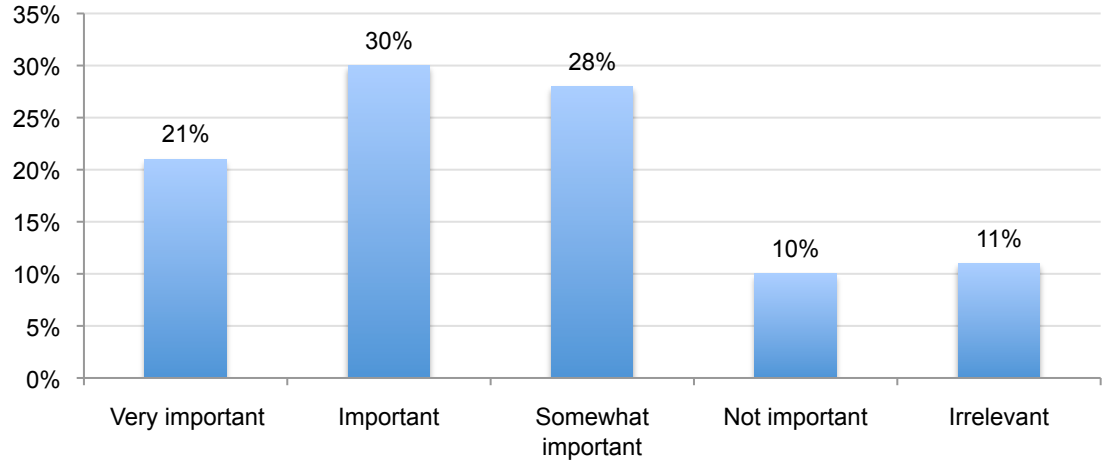


When asked why the encryption of data-at-rest is important, 29 percent say it is to minimize end-user mishaps resulting from lost computers followed by 23 percent who say encryption is necessary to improve the security posture of their organization.

The need to encrypt is of lesser importance, according to respondents, if it is to avoid harms to customers resulting from data loss or theft (such as identity theft), to minimize the cost of a data breach and to minimize the affect of a cyber attack, (13 percent, 13 percent and 6 percent, respectively). These choices may be less important to IT practitioners because in their work they do not deal directly with consumer or financial issues.

Further, according to Bar Chart 6, about half (21+ 30 percent) believe compliance with high security standards such as Federal Information Processing Standards (FIPS) 197 (AES) or FIPS 140 is very important or important. Only 11 percent say such compliance is irrelevant. In the US, requirements for government security are regulated by FIPS publications, which are developed by the National Institute of Standards and Technology (NIST) for use government-wide. FIPs 140-2 is required for sale of products implementing cryptography to the federal government.

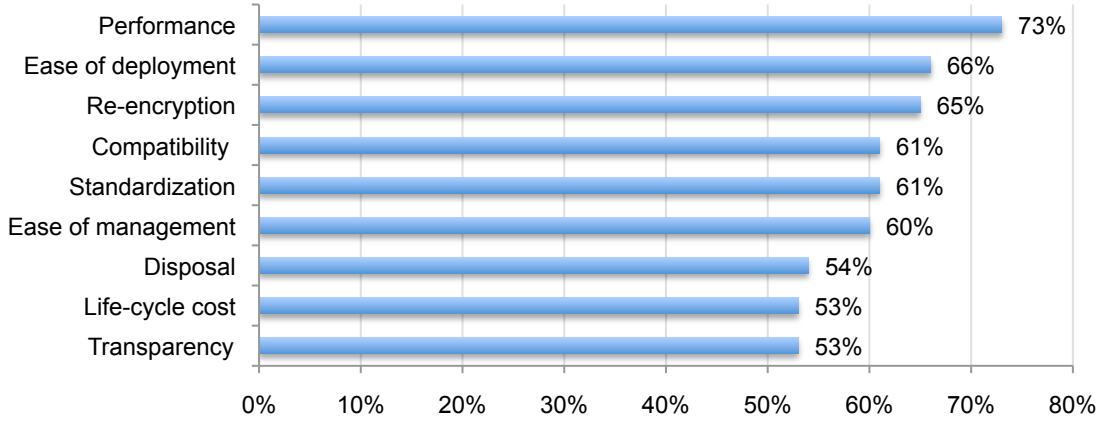
Bar Chart 6: How important is compliance with high security standards such as FIPS 197(AES) or FIPS 140 to your organization's decision to select a drive encryption solution?



Performance and ease of deployment are considered important features for encryption technologies. We asked the IT practitioners in our study to rate 9 drive encryption features based on how important they believe they are in meeting their data security goals (see Bar Chart 7). The nine features in order of importance according to the respondents are (very important and important responses combined):

- Performance: no degradation in SED performance (73 percent)
- Ease of deployment: the encryption key is generated in the factory (66 percent)
- Re-encryption: with self-encrypting drives, there is no need to ever re-encrypt the data (65 percent)
- Standardization: whole drive industry is building to the TCG/SED specifications (61 percent)
- Compatibility with encryption software and encryption key management platforms (61 percent)
- Ease of management: the encryption key need not be managed (60 percent)
- Disposal or re-purposing cost: erasure made easy (54 percent)
- Life-cycle costs: lower initial and on-going costs (53 percent)
- Transparency: once unlocked, it functions as a regular drive (53 percent)

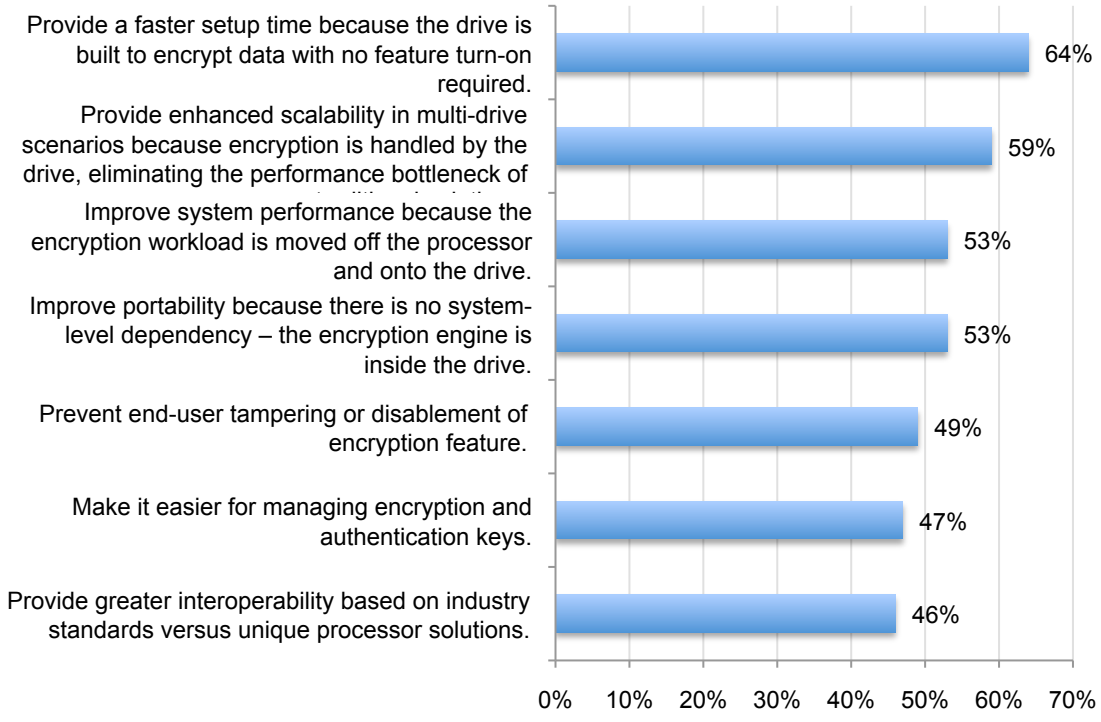
Bar Chart 7: The importance of each one of the following nine drive encryption features
Very important and important response combined



We asked this question to better understand if SEDs have the features most desirable to organizations. What we learned is that the perceptions of IT practitioners are supportive of investing in SEDs. According to the TCG, these drives are easily deployed in the enterprise. Because drives are based on TCG specifications they are easily managed and the cost of deployment is reduced.

Other benefits realized by encrypting the drive itself, reported by TCG, is the contents of the self-encrypting drives are always encrypted and the encryption keys are themselves encrypted and protected in hardware that cannot be observed by other parts of the system. Further, because encryption is handled in the drive, overall system performance is not affected and is not subject to attacks targeting other components of the system.

Bar Chart 8: How do SEDs compare to software-encrypted drives?
Strongly agree and agree response combined.

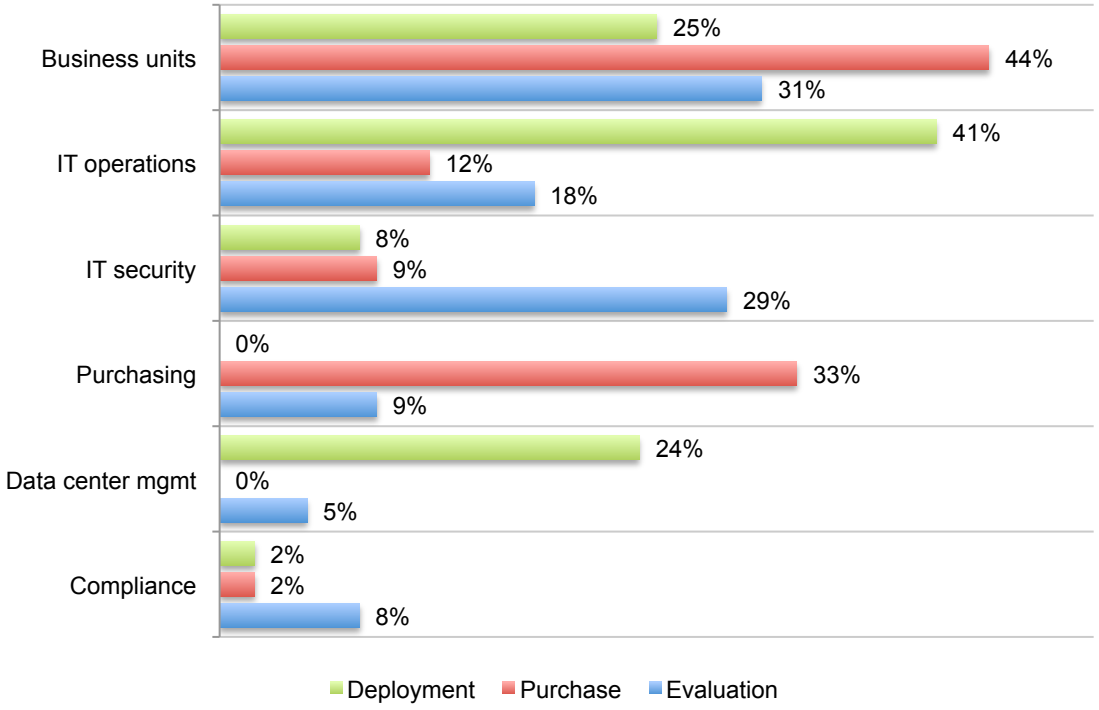


In comparison to software-based encrypted drives, 64 percent of respondents strongly agree (25 percent) and agree (39 percent) that SEDs provide a faster setup time because the drive is built to encrypt data with no feature turn-on required. Fifty-nine percent strongly agree (24 percent) and agree (35 percent) that SEDs provide enhanced scalability in multi-drive scenarios because encryption is handled by the drive, eliminating the performance bottleneck of traditional solutions (see Bar Chart 8).

However, there is a high degree of uncertainty among respondents as to whether SEDs make it easier for managing encryption and authentication keys (39 percent), if they prevent end-user tampering or disablement of encryption feature (36 percent) or if they provide greater interoperability based on industry standards versus unique processor solutions (36 percent). This uncertainty could be attributed to misperception about the capabilities of SEDs.

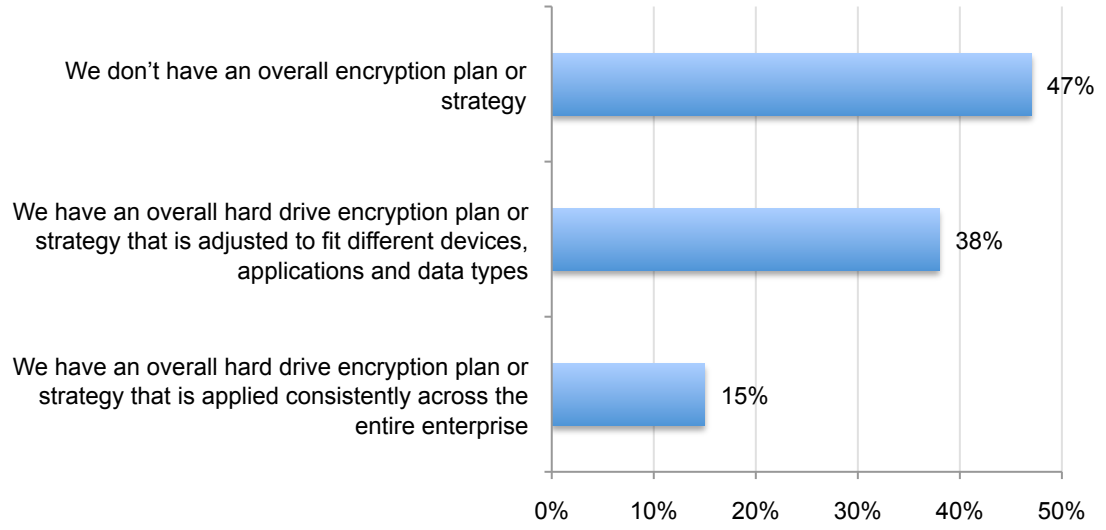
Encryption evaluation and purchasing decisions are often made at the business unit level but the IT operations function is most often responsible for deployment. Almost one-third (31 percent) say business units are most responsible for **evaluating** encryption solutions for drive storage devices followed by 29 percent who say it is IT security and 18 percent who say it is IT operations. Forty-four percent say business units are most responsible for **purchasing** encryption solutions for drive storage devices followed by 33 percent who say this decision is made by the purchasing function. Forty-one percent say that IT operations is most responsible for **deploying** encryption solutions for drive storage devices (see Bar Chart 9).

Bar Chart 9: What departments or operating units within your organization are most responsible for evaluating, purchasing and deploying encryption solutions for drive storage devices?



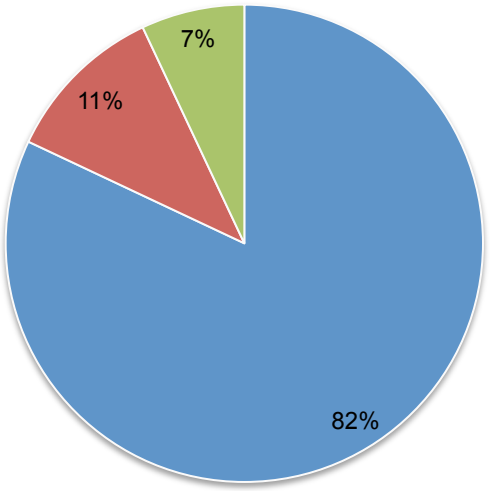
The fact that purchasing and deployment decisions are **not** made by the same function may make it difficult to achieve a consistent and overall encryption strategy for organizations. Bar Chart 10 shows 47 percent of respondents do not have a strategy. Thirty-eight percent say they have an overall hard drive encryption plan or strategy that is adjusted to fit different devices, applications and data types. Only 15 percent say they have an overall hard drive encryption plan or strategy that is applied consistently across the entire enterprise.

Bar Chart 10: The one statement that best describes respondent organizations' approach to drive encryption implementation across the enterprise.

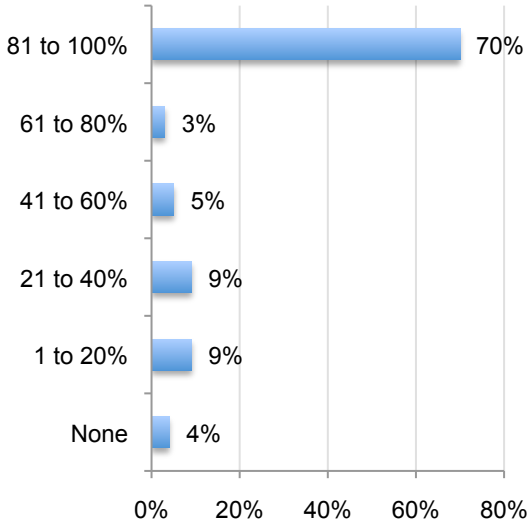


SEDs can protect lost or stolen records from abuse if a data breach occurs, according to respondents. Pie Chart 1 shows 82 percent of respondents report that their organization experienced one or more data breach incidents in the past 24 months. The majority of respondents (70 percent) say that SEDs would have had an enormous and positive impact on the protection of at least 80 percent of lost or stolen records.

Pie Chart 1: Did your organization experience one or more data breach incidents over the past 24 months?



Bar Chart 12: If yes, what percentage of these lost or stolen records would have been protected from abuse if they had been on self-encrypting drives?



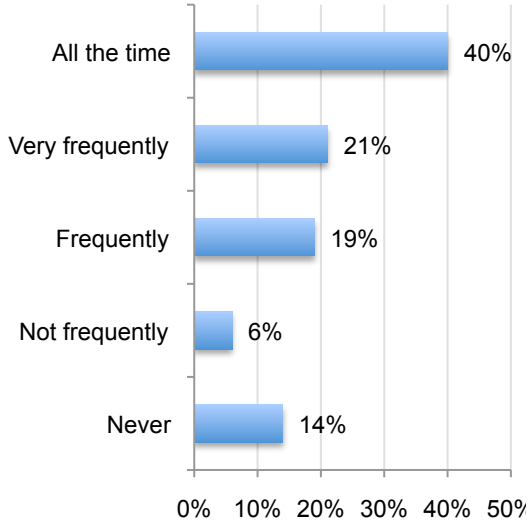
Another important reason for SEDs is inferred from *The Cost of a Lost Laptop*[2] study. This research revealed that the average cost of a lost laptop that is not encrypted is $56,165. However, when a lost laptop has encryption the average cost drops to $37,443.

[2] See Ponemon Institute, *The Cost of a Lost Laptop*, sponsored by Intel, April 2009

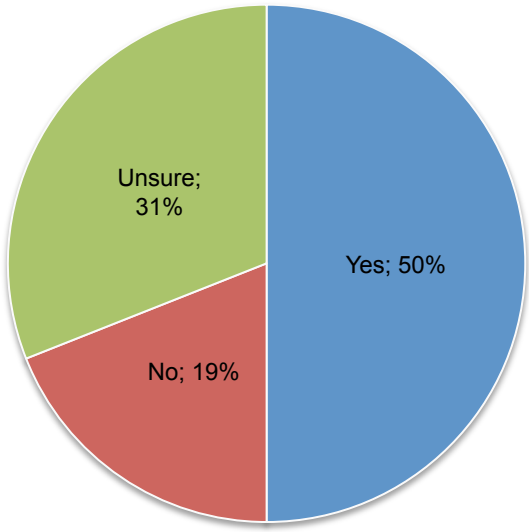
Based on Ponemon Institute's *2010 U.S. Cost of a Data Breach Study*, the average cost per lost or stolen record is $214. If organizations' lost on average approximately 16,000 records from a data breach this translates to a cost of about $3.4 million for each incident. We believe the results of this research should be very helpful in making the business case for investing in SEDs.

Employees violate security policies and put data at risk because they frequently disengage their laptops' security protections. Forty percent believe employees in their organizations routinely turn-off their laptops' security protection all the time (see Bar Chart 12). While not shown in the charts below, 68 percent say their organizations have policies that does not allow this practice. Such a high percentage of employees violating company policy suggest many organizations are not effective at enforcing or creating awareness about the need to protect sensitive and confidential information. Pie Chart 2 shows half (50 percent) of respondents believe SEDs would mitigate or significantly curtail employees from this dangerous practice.

Bar Chart 12: Employees (end-users) turn-off or disengage their laptop's security protection without obtaining advance permission to do so?



Pie Chart 2. Would the use of self-encrypting drives mitigate or significantly curtail employees from turning off or disengaging their laptop's security protections including encryption?

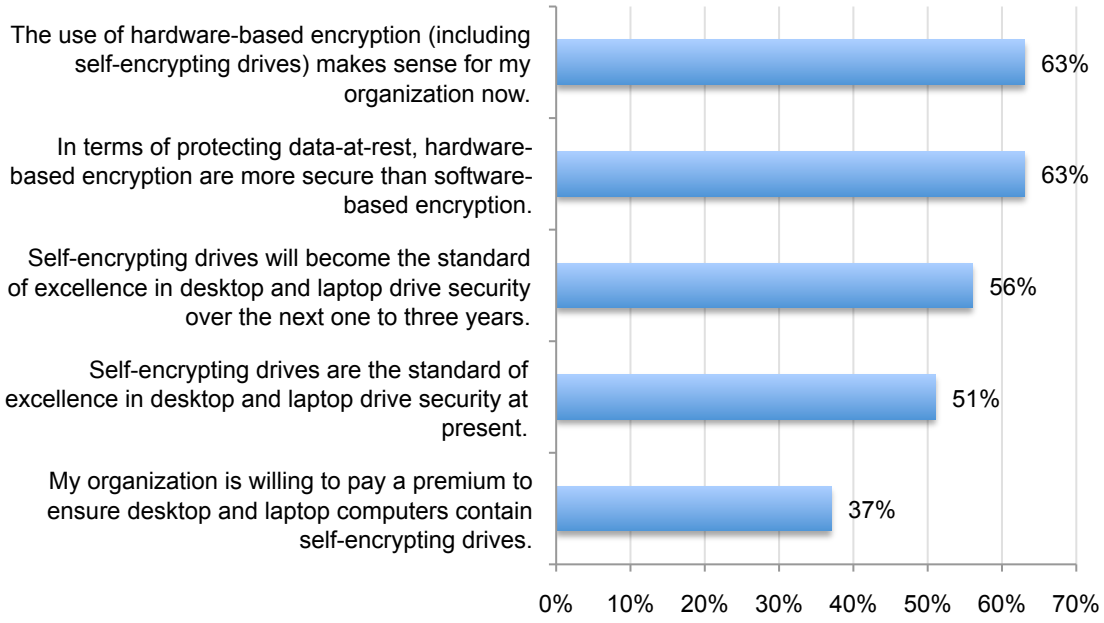


In the *2010 Airport Insecurity Study: The Case of Lost Laptops*[3], the research revealed that 65 percent of business travelers in our study admit to not taking steps to protect or secure sensitive information on their laptops. Despite this negligence, these travelers say the types of company information on their laptops includes business confidential information (52 percent), client, customer or consumer data (49 percent) and intellectual property such as software code (15 percent) and employee records (11 percent).

IT practitioners view hardware-based encryption favorably. According to Bar Chart 13, a majority of respondents agree that in terms of protecting data-at-rest, hardware-based encryption (including self-encrypting drives) is more secure than software-based encryption. Fifty-six percent believe SEDs will become the standard of excellence in desktop and laptop drive security over the next one to three years and 63 percent agree that hardware-based encryption (including SEDs) make sense for their organization. Moreover, 37 percent say their organization would be willing to pay a premium to ensure desktop and laptop computers contain self-encrypting drives.

[3] See Ponemon Institute, 2010 Airport Insecurity: The Case of a Lost Laptop, sponsored by Dell, December 2010

Bar Chart 13: Perceptions about hardware-based encryption
Strongly agree and agree response combined



Part 3. Methods

A sampling frame of 15,749 of 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 several proprietary lists of experienced IT and IT security practitioners. In total, 719 respondents completed the survey. Of these returned instruments, 64 failed reliability checks. A total of 655 surveys were deemed usable. Applying four screening questions that assessed the respondents' experience and knowledge about hardware-based encryption resulted in a final sample of 517, or a 3.3 percent response rate.

Table 1: Sample response	Freq	Pct%
Total sampling frame	15,749	100.0%
Total survey returns	719	4.6%
Rejected surveys	64	0.4%
Sample before screening	655	4.2%
Final sample	517	3.3%

Pie Chart 3 reports the primary industry sector of respondents' organizations. The largest segments are financial services (19 percent), public sector (14 percent) and retailing (11 percent).

Pie Chart 3: Industry distribution of respondents' organizations

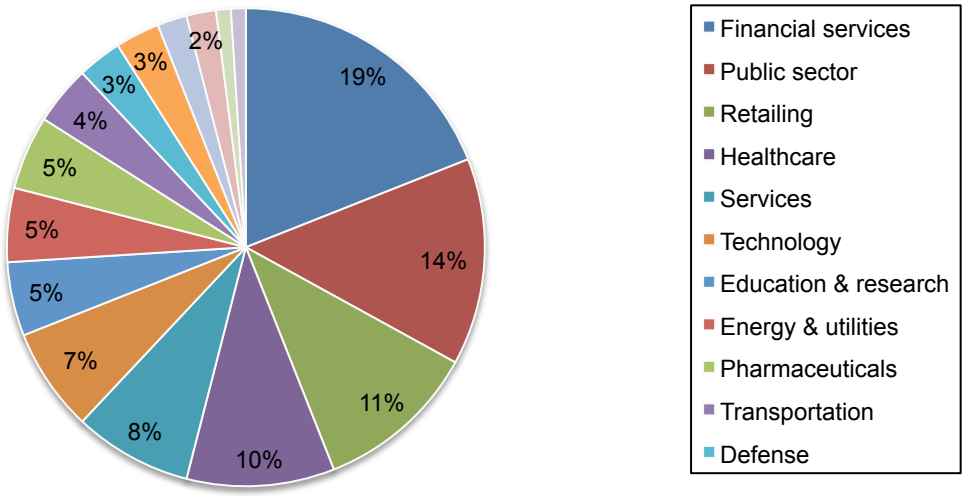


Table 4 reports the respondent organization's global headcount. As shown, half of respondents work within companies with more than 5,000 employees. Over 62 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 4. The worldwide headcount of respondents' organization	**Pct%**
Less than 500 people	9%
500 to 1,000 people	18%
1,001 to 5,000 people	23%
5,001 to 25,000 people	22%
25,001 to 75,000 people	20%
More than 75,000 people	8%
Total	100%

Table 5 reports the respondent's primary reporting channel. As can be seen, 56 percent of respondents are located in the organization's IT department (led by the company's CIO). Fifteen percent report to the company's head of information security (CISO).

Table 5: Respondents' primary reporting channel	Pct%
Chief Information Officer	56%
Head of information security (CISO)	15%
Compliance Officer	9%
Chief Risk Officer	6%
Head of security (CSO)	5%
Chief Financial Officer	2%
General Counsel	2%
Human Resources VP	2%
Other	2%
CEO/Executive Committee	1%
Total	100%

Table 6 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, Canada, EMEA, Latin America, and Asia-Pacific regions.

Table 6: Geographic footprint of respondents' organizations.	Pct%
United States	100%
Canada	63%
Europe	61%
Middle east & Africa	28%
Asia-Pacific	49%
Latin America (including Mexico)	50%

Table 7 reports the approximate position level or title of respondents. As shown, a majority of respondents state they are at or above the supervisory level (55 percent). The mean experience of respondents in this study is 9.55 years and the median is 10 years.

Table 7: Respondent's self-reported position level	Pct%
Senior Executive	1%
Vice President	2%
Director	15%
Manager	20%
Supervisor	17%
Technician	32%
Staff	5%
Contractor	6%
Other	2%
Total	100%

Part 4. Caveats & Conclusion

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 IT or IT 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.

Concluding Thoughts

IT practitioners participating in this study appear to have a high regard for SEDs and their ability to protect data stored on computers with no impact on performance. The barriers to adoption appear to be perceptions about cost and not understanding the hard drive options that are available to their organization. However as reported by the TCG, self-encrypting drives are easily deployed and managed at a reduced cost because of the TCG specifications used by hard drive vendors.

As understanding and awareness about the capabilities of hardware-based encryption versus software-based encryption grows, we predict that there will be greater adoption of SEDs. This is not just our opinion. Already, the majority of IT practitioners in this study predict that SEDs will become the standard of excellence in desktop and laptop drive security in the very near future.

Appendix: Detailed Survey Responses

Following are the survey results for a final sample of 517 IT and IT security practitioners. The survey and debriefing fieldwork concluded in April 2011.

Sample response	Freq	Pct%
Total sampling frame	15,749	100.0%
Total survey returns	719	4.6%
Rejected surveys	64	0.4%
Sample before screening	655	4.2%
Final sample	517	3.3%

Part 1: Screening questions

S1. How familiar are you with self-encrypting drives (SED)?	Freq	Pct%
Very familiar	230	35%
Somewhat familiar	345	53%
Not familiar (stop)	58	9%
No knowledge (stop)	22	3%
Total	655	100%

S2. Does your organization use hardware-based or software-based encryption for protecting stored data on drives? Please choose only one.	Freq	Pct%
Yes, mostly hardware-based encryption	78	14%
Yes, a combination of hardware and software-based encryption	237	41%
Yes, mostly software-based encryption	203	35%
No encryption (stop)	58	10%
Total	575	100%

Final sample	517

Part 2: Survey questions

Q1a. If your organization is not using hardware-based encryption, why not?	Pct%	n=203
Too hard to implement	10%	
Too expensive	45%	
Don't need to encrypt	13%	
Concern about performance	26%	
Diminished end-user productivity	9%	
Encrypting data-at-rest limits our ability to perform network surveillance	24%	
I do not fully understand the hardware-based encryption technology options available to my organization	36%	
Other (please specify)	1%	
Total	164%	

Q1b. If your organization is not using software-based encryption, why not?	Pct%	n=78
Too hard to implement	23%	
Too expensive	28%	
Don't need to encrypt	14%	
Concern about performance	39%	
Diminished end-user productivity	35%	
Encrypting data limits our ability to perform network surveillance	24%	
I do not fully understand the software-based encryption technology options available to my organization	15%	
Other (please specify)	0%	
Total	178%	

Q2. What types of stored data on drives (data-at-rest) are normally encrypted in your organization? Please check all that apply.	Pct%	n=517
Consumer data	9%	
Customer data	39%	
Employee records	41%	
Non-financial confidential documents	32%	
Financial confidential documents	57%	
Source code	8%	
Trade secrets	34%	
Other intellectual properties	18%	
Other (please specify)	5%	
Total	243%	

Q3. How important is compliance with high security standards such as FIPS 197(AES) or FIPS 140 to your organization's decision to select a drive encryption solution?	Pct%	n=517
Very important	21%	
Important	30%	
Somewhat important	28%	
Not important	10%	
Irrelevant	11%	
Total	100%	

Q4. Why does your organization encrypt data-at-rest? Please select your top two choices.	Pct%	n=517
Comply with state or federal data protection laws such as HIPAA	51%	
Comply with self-regulatory programs such as PCI DSS, ISO, NIST and others	49%	
Minimize end-user data mishaps resulting from lost computers	29%	
Comply with vendor or business partner agreements	15%	
Avoid harms to customers resulting from data loss or theft	13%	
Minimize the cost of data breach	13%	
Minimize the affect of cyber attacks	6%	
Improve security posture	23%	
Other (please specify)	1%	
Total	200%	

Q5. In evaluating encryption solutions for your organization, how important is each attribute listed below? Please rank the following six attributes from 6 = most important to 1 = least important to your organization.	Average Rank	Grand Average
Performance	5.08	3.68
Security	5.15	3.68
Scalability	3.33	3.68
Interoperability	3.65	3.68
Ease	2.28	3.68
Cost	2.59	3.68
Average	3.68	

Q6. Please rate the importance of each one of the following nine drive encryption features using the scale below the item.

Q6a. Ease of deployment: Encryption key is generated in the factory	Pct%	n=517
Very important	34%	
Important	32%	
Somewhat important	20%	
Not important	10%	
Irrelevant	4%	
Total	100%	

Q6b. Transparency: Once unlocked, it functions as a regular drive	Pct%	n=517
Very important	23%	
Important	30%	
Somewhat important	26%	
Not important	13%	
Irrelevant	8%	
Total	100%	

Q6c. Ease of management: The encryption key need not be managed	Pct%	n=517
Very important	31%	
Important	29%	
Somewhat important	24%	
Not important	11%	
Irrelevant	5%	
Total	100%	

Q6d. Life-cycle costs: Lower initial and on-going costs	Pct%	n=517
Very important	25%	
Important	28%	
Somewhat important	30%	
Not important	15%	
Irrelevant	2%	
Total	100%	

Q6f. Disposal or re-purposing cost: Erasure made easy	Pct%	n=517
Very important	23%	
Important	31%	
Somewhat important	28%	
Not important	13%	
Irrelevant	5%	
Total	100%	

Q6g. Re-encryption: With self-encrypting drives, there is no need to ever re-encrypt the data	Pct%	n=517
Very important	33%	
Important	32%	
Somewhat important	19%	
Not important	12%	
Irrelevant	4%	
Total	100%	

Q6h. Performance: No degradation in SED performance	Pct%	n=517
Very important	35%	
Important	38%	
Somewhat important	16%	
Not important	9%	
Irrelevant	2%	
Total	100%	

Q6i. Standardization: Whole drive industry is building to the TCG/SED specifications	Pct%	n=517
Very important	29%	
Important	32%	
Somewhat important	21%	
Not important	11%	
Irrelevant	7%	
Total	100%	

Q6j. Compatibility with encryption software and encryption key management platforms	Pct%	n=517
Very important	31%	
Important	30%	
Somewhat important	19%	
Not important	12%	
Irrelevant	8%	
Total	100%	

Q7. Please rate your level of agreement with each one of the following statements about self-encrypting drives using the scale below the item.		
In comparison to software-based encrypted drives, SEDs do the following:		
Q7a. Prevent end-user tampering or disablement of encryption feature.	Pct%	n=517
Strongly agree	23%	
Agree	26%	
Unsure	36%	
Disagree	13%	
Strongly disagree	2%	
Total	100%	

Q7b. Make it easier for managing encryption and authentication keys.	Pct%	n=517
Strongly agree	21%	
Agree	26%	
Unsure	39%	
Disagree	11%	
Strongly disagree	3%	
Total	100%	

Q7c. Provide a faster setup time because the drive is built to encrypt data with no feature turn-on required.	Pct%	n=517
Strongly agree	25%	
Agree	39%	
Unsure	23%	
Disagree	11%	
Strongly disagree	2%	
Total	100%	

Q7d. Provide enhanced scalability in multi-drive scenarios because encryption is handled by the drive, eliminating the performance bottleneck of traditional solutions.	Pct%	n=517
Strongly agree	24%	
Agree	35%	
Unsure	23%	
Disagree	15%	
Strongly disagree	3%	
Total	100%	

Q7e. Provide greater interoperability based on industry standards versus unique processor solutions.	Pct%	n=517
Strongly agree	21%	
Agree	25%	
Unsure	36%	
Disagree	15%	
Strongly disagree	3%	
Total	100%	

Q7f. Improve portability because there is no system-level dependency – the encryption engine is inside the drive.	Pct%	n=517
Strongly agree	25%	
Agree	28%	
Unsure	29%	
Disagree	15%	
Strongly disagree	3%	
Total	100%	

Q7g. Improve system performance because the encryption workload is moved off the processor and onto the drive.	Pct%	n=517
Strongly agree	23%	
Agree	30%	
Unsure	30%	
Disagree	12%	
Strongly disagree	5%	
Total	100%	

Q8a. Are you familiar with the Trusted Computing Group (TCG)?	Pct%	n=517
Very familiar	15%	
Somewhat familiar	43%	
Not familiar	24%	
No knowledge	18%	
Total	100%	

Q8b. [If familiar] which one of the following TCG standards is most applicable or relevant to your organization? Please check all that apply.	Pct%	n=300
Encryption standard for laptops	69%	
Encryption standard for enterprise storage	50%	
Encryption standard for interoperability of management software	37%	
None of the above	3%	
Total	159%	

Q9a. What departments or operating units within your organization are most responsible for **evaluating** encryption solutions for drive storage devices?	Pct%	n=517
IT operations	18%	
IT security	29%	
Business units	31%	
Purchasing	9%	
Compliance	8%	
Data center management	5%	
Total	100%	

Q9b. What departments or operating units within your organization are most responsible for **purchasing** encryption solutions for drive storage devices?	Pct%	n=517
IT operations	12%	
IT security	9%	
Business units	44%	
Purchasing	33%	
Compliance	2%	
Data center management	0%	
Total	100%	

Q9c. What departments or operating units within your organization are most responsible for **deploying** encryption solutions for drive storage devices?	Pct%	n=517
IT operations	41%	
IT security	8%	
Business units	25%	
Purchasing	0%	
Compliance	2%	
Data center management	24%	
Total	100%	

Q10. Please check the maturity stage of your company's information security and data protection program. Select the one that in your opinion best describes the present state of IT security activities.	Pct%	n=517
Pre stage – IT security program has not been established as a unit within the company.	5%	
Early stage – IT security program is just starting to become staffed and organized.	23%	
Middle stage – IT security program is in existence and is starting to launch key initiatives.	35%	
Late middle stage – IT security program is starting to evaluate the effectiveness of key initiatives.	14%	
Mature stage – IT security program is in maintenance mode focusing on program evaluation and refinement.	23%	

Q11. Please check one statement that best describes your organization's approach to drive encryption implementation across the enterprise.	Pct%	n=517
We have an overall hard drive encryption plan or strategy that is applied consistently across the entire enterprise	15%	
We have an overall hard drive encryption plan or strategy that is adjusted to fit different devices, applications and data types	38%	
We don't have an overall encryption plan or strategy	47%	
Total	100%	

Q12a. Did your organization experience one or more data breach incidents over the past 24 months?	Pct%	n=517
Yes	82%	
No	11%	
Unsure	7%	
Total	100%	

Q12b. If yes, how many records were lost or stolen as a result of the above data breach incidents over the past 24 months? An approximation is welcome.	Pct%	n=424
1 to 1,000	55%	
1,000 to 5,000	23%	
5,001 to 10,000	17%	
10,001 to 50,000	2%	
50,001 to 100,001	1%	
100,001 to 500,000	1%	
500,000 to 1,000,000	0%	
More than 1,000,000	1%	
Total	100%	
Extrapolated average number of compromised records	15,875	

Q12c. If yes, what percentage of these lost or stolen records would have been protected from abuse if they had been on self-encrypting drives? An approximation is welcome.	Pct%	n=424
None	4%	
1 to 20%	9%	
21 to 40%	9%	
41 to 60%	5%	
61 to 80%	3%	
81 to 100%	70%	
Total	100%	
Extrapolated average percentage of protected records	71%	

Q13. How frequently does the following situation occur within your organization?		
Employees (end-users) turn-off or disengage their laptop's security protection without obtaining advance permission to do so?	Pct%	n=517
All the time	40%	
Very frequently	21%	
Frequently	19%	
Not frequently	6%	
Never	14%	
Total	100%	

Q14. Does your organization's security policy allow employees (end-users) to turn-off or disengage their laptop's security protections including encryption without obtaining permission to do so?	Pct%	n=517
Yes	9%	
No	68%	
We don't have a security policy	4%	
Unsure	19%	
Total	100%	

Q15. In your opinion, would the use of self-encrypting drives mitigate or significantly curtail employees from turning off or disengaging their laptop's security protections including encryption?	Pct%	n=517
Yes	50%	
No	19%	
Unsure	31%	
Total	100%	

Part 3. Attributions

Q16. In terms of protecting data-at-rest, hardware-based encryption are more secure than software-based encryption.	Pct%	n=517
Strongly agree	0.34	
Agree	0.29	
Unsure	0.17	
Disagree	0.11	
Strongly disagree	0.09	
Total	1	

Q17. My organization is willing to pay a premium to ensure desktop and laptop computers contain self-encrypting drives.	Pct%	n=517
Strongly agree	15%	
Agree	22%	
Unsure	28%	
Disagree	21%	
Strongly disagree	14%	
Total	100%	

Q18. Self-encrypting drives are the standard of excellence in desktop and laptop drive security at present.	Pct%	n=517
Strongly agree	21%	
Agree	30%	
Unsure	20%	
Disagree	22%	
Strongly disagree	7%	
Total	100%	

Q19. Self-encrypting drives will become the standard of excellence in desktop and laptop drive security over the next one to three years.	Pct%	n=517
Strongly agree	35%	
Agree	21%	
Unsure	16%	
Disagree	21%	
Strongly disagree	7%	
Total	100%	

Q20. The use of hardware-based encryption (including self-encrypting drives) makes sense for my organization now.	Pct%	n=517
Strongly agree	33%	
Agree	30%	
Unsure	10%	
Disagree	16%	
Strongly disagree	11%	
Total	100%	

Part 4. Your role and organization

D1. What organizational level best describes your current position?	Pct%	n=517
Senior Executive	1%	
Vice President	2%	
Director	15%	
Manager	20%	
Supervisor	17%	
Technician	32%	
Staff	5%	
Contractor	6%	
Other	2%	
Total	100%	

D2. Is this a full time position?	Pct%	n=517
Yes	98%	
No	2%	
Total	100%	

D3. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%	n=517
CEO/Executive Committee	1%	
Chief Financial Officer	2%	
General Counsel	2%	
Chief Information Officer	56%	
Compliance Officer	9%	
Human Resources VP	2%	
Head of information security (CISO)	15%	
Head of security (CSO)	5%	
Chief Risk Officer	6%	
Other	2%	
Total	100%	

D4. Total years of relevant experience	Mean	Median
Total years of IT or security experience	9.55	10.00
Total years in current position	4.51	5.25

D5. Gender	Pct%	n=517
Female	28%	
Male	72%	
Total	100%	

D5. What industry best describes your company?	Pct%	n=517
Communications	2%	
Defense	3%	
Education & research	5%	
Energy & utilities	5%	
Financial services	19%	
Healthcare	10%	
Hospitality	2%	
Industrial	3%	
Manufacturing	1%	
Media	1%	
Pharmaceuticals	5%	
Public sector	14%	
Retailing	11%	
Services	8%	
Technology	7%	
Transportation	4%	
Total	100%	

D7. Where are your employees located? (Check all that apply):	Pct%	n=517
United States	100%	
Canada	63%	
Europe	61%	
Middle east	28%	
Asia-Pacific	49%	
Latin America (including Mexico)	50%	
Total	351%	

D8. What is the worldwide headcount of your organization?	Pct%	n=517
Less than 500 people	9%	
500 to 1,000 people	18%	
1,001 to 5,000 people	23%	
5,001 to 25,000 people	22%	
25,001 to 75,000 people	20%	
More than 75,000 people	8%	
Total	100%	

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.