The TCO for Full Disk Encryption

Studies in the US, UK, Germany & Japan

Sponsored by WinMagic

Independently conducted by Ponemon Institute LLC

Publication Date: July 2012

The TCO for Full Disk Encryption

Presented by Ponemon Institute, July 2012

Part 1. Introduction

We are pleased to present the findings of the *Total Cost of Ownership for Full Disk Encryption* (FDE), sponsored by WinMagic and independently conducted by Ponemon Institute, The purpose of this study is to learn important information about how organizations are deploying software and hardware full disk encryption solutions for desktop and laptop computers as well as the determination of total cost and benefits for organizations in different industries. Full disk encryption means that every bit of data that goes on a disk is encrypted.

Encryption is important to mitigating the damage caused by data breaches, complying with privacy and data protection regulations and preserving brand and reputation. However, there are many approaches and strategies for deploying encryption across the enterprise. In order to make rational decisions regarding the optimum use of encryption, it is important to comprehend the total cost of ownership (TCO). This particularly applies to solutions believed to be free but may have a significantly higher TCO than commercial products.

Ponemon Institute surveyed 1,335 individuals in IT and IT security in four separate country samples: the United States (US), United Kingdom (UK), Germany (DE) and Japan (JP) representing a variety of industry sectors. Respondents hold bona fide credentials in IT, IT security or data protection, and have nearly 10 years of relevant experience on average.

For purposes of this research, we defined self-encrypting drives (SEDs) as providing hardware-based data security, full disk encryption and enhanced secure erase capabilities. The OPAL storage specification provides a comprehensive architecture for putting storage devices such as SEDs under policy control as determined by a trusted platform host.

Following are the most salient findings from this research:

- Expected benefits of full disk encryption exceed cost in all four countries by a factor ranging from 4 to 20. In the context of this paper, the primary benefit of full disk encryption is a reduction in the probability of having a data breach as a result of a lost or stolen desktop or laptop computer.

- TCO varies inversely by organizational size: The highest TCO is for organizations with fewer than 50 employees ($403) and more than 25,000 employees ($315). The pure software cost (license and maintenance) only represents a small fraction of the total cost of FDE encryption solution.

- TCO varies by industry. Heavily regulated industries such as financial services and healthcare have the highest TCO ($388 and $366, respectively). Lowest TCO are in less regulated industries, such as entertainment & media and retail ($201 and $172, respectively)

- Our results suggest that respondents underestimate the TCO for full disk encryption. First, there is not a firm understanding of the amount of technician time required to complete a procedure. Second, the time incurred by users, including idle time because of the inability to access their computers, is not taken into account.

- The most expensive component of TCO concerns the value of user time incurred operating a desktop or laptop with encryption. In the U.S., the average extra time it takes each day to start-up, shutdown and hibernate their computers with FDE takes 42 seconds. This can amount to nearly three hours per employee in one year. Clearly, this can represent a significant burden when you sum the time-related cost for all employees with an assigned laptops or desktops.

- Germany has the highest rate of encryption of sensitive and confidential information. More than 50 percent of respondents report that their organizations encrypt trade secrets, financial confidential documents and employee records. Despite German organizations' efforts to encrypt sensitive information, in many cases more than half of this data is vulnerable to a data breach.

- Japanese organizations encrypt data-at-rest primarily to comply with self-regulatory programs such as PCI DSS, ISO, and other standards of compliance. U.S., UK and German organizations mainly encrypt to comply with state or federal/national data protection laws.

Part 2. Full Disk Encryption TCO Calculus

In this section, we analyze the individual components of TCO for full disk encryption. Our TCO analysis is conducted for four country samples on a per computer basis for one full year.[1] All costs are expressed in U.S. dollars for purposes of comparability across countries. Table 1 reports key assumptions that we use in our calculations:

Table 1 Assumptions used in TCO calculus	US	UK	DE	JP
Fully loaded hourly cost of technician time incurred while handling computing devices*	$36	$35	$41	$44
Fully loaded hourly cost of end-users	$56	$64	$72	$59
Approximate useful life of laptops or desktops assigned to end-users in years	3.0	3.1	3.0	2.9
Average number of 8-hour workdays per year#	247.5	235	225	245

*Estimated values derived from Ponemon Institute's 2011 Tracking Survey on Security Spending
#Estimated values from OECD labor statistics

Our analysis consists of eleven segments: (1) licensing cost; (2) maintenance cost; (3) SED incremental cost; (4) device pre-provisioning cost; (5) device staging cost; (6) value of tech time associated with password resets; (7) end-user downtime associated with password resets; (8) cost associated with re-imaging hard disks; (9) end-user downtime associated with initial disk encryption; (10) value of end-user time incurred operating a full disk encrypted computer; and (11) value of tech time incurred for various administrative tasks requiring access to encrypted drives.

Licensing cost

The average licensing costs per annum are computed in Table 2. The average licensing cost, which is derived from one survey question is divided by the useful life of the laptop or desktop computer in order to calculate cost per annum. As can be seen, this TCO component appears to be fairly consistent across country samples.

Table 2 Assumptions about licensing cost	US	UK	DE	JP
Average licensing cost for software and hardware encryption products combined	$15.7	$15.1	$16.3	$16.3
Approximate useful life of laptops or desktops assigned to end-users	3.0	3.1	3.0	2.9
Average licensing cost per annum	$5.3	$4.8	$5.5	$5.7

Annual maintenance cost

In this study, the average annual maintenance cost is expressed as a percentage of the total licensing cost. Using the above figure for licensing cost reported above, we calculate the maintenance cost for four country samples in Table 3. The percentage of annual maintenance cost is derived from one survey question. Once again, this cost appears to be stable across country samples.

Table 3 Assumptions about annual maintenance cost	US	UK	DE	JP
Annual maintenance as a percentage to licensing cost	17%	18%	18%	17%
Average licensing cost for software and hardware encryption combined	$15.7	$15.1	$16.3	$16.3
Annual maintenance cost	$2.7	$2.7	$2.9	$2.8

[1] In this analysis, we combine of software and hardware encryption costs rather then show these figures separately. For simplicity, we use a 50/50 split and not a weighted average.

OPAL fees[2]

Table 4 computes the incremental licensing fee for OPAL-based hardware encrypted drives (a.k.a. self-encrypted drives abbreviated by SED). As can be seen, we assume an even split in terms of the use of hardware or software-based full disk encryption among participating companies. Our computation applies the estimated OPAL fee for hardware encrypted drives.

Table 4 Special fee for OPAL	US	UK	DE	JP
Fee paid for self-encrypted drives	$7.9	$6.8	$7.1	$7.7
Applied only to hardware encrypted drives*	50%	50%	50%	50%
SED incremental cost	$4.0	$3.4	$3.6	$3.9

*This analysis assumes a 50/50 split between software and hardware-based encrypted drives

Pre-provisioning cost

Table 5 computes the cost associated with pre-provisioning an encrypted and unencrypted laptop or desktop computer. Clearly, it takes more time to pre-provision a full disk encrypted computer and this time difference is multiplied by the value of tech time (in minutes) devoted to the pre-provisioning task. As can be seen, the US sample has the lowest pre-provisioning cost ($1.3) and the German sample has the highest cost ($6.4).

Table 5 Incremental cost associated with the pre-provisioning of a full disk encrypted computer	US	UK	DE	JP
Tech time to pre-provision FDE computer	21.6	19.8	18.9	18.5
Tech time to pre-provision unencrypted computer	19.5	13.0	9.5	13.7
Incremental time difference (minutes)	2.1	6.8	9.4	4.8
Tech time cost per hour	$36	$35	$41	$44
Tech time cost per minute	$0.6	$0.6	$0.7	$0.7
Value of tech time to pre-provision FDE computer	$1.3	$3.9	$6.4	$3.5

Staging cost

Table 6 computes the cost associated with the staging of an encrypted and unencrypted laptop or desktop computer. As shown, it takes more time to stage a full disk encrypted computer and this time difference is multiplied by the value of tech time (in minutes) devoted to the staging task. As can be seen, the US sample has the lowest staging cost ($12.0) and the UK sample has the highest cost ($18.5).

Table 6 Incremental cost associated with the staging of a full disk encrypted computer	US	UK	DE	JP
Tech time to stage FDE computer	47.1	54.2	48.4	49.6
Tech time to stage unencrypted computer	27.1	22.4	23.9	26.3
Incremental time difference (minutes)	20.0	31.8	24.5	23.3
Tech time cost per hour	$36	$35	$41	$44
Tech time cost per minute	$0.6	$0.6	$0.7	$0.7
Value of tech time to stage FDE computer	$12.0	$18.5	$16.7	$17.1

[2] Self-encrypting drives (SEDs) provide hardware-based data security, full disk encryption and enhanced secure erase capabilities. The OPAL storage specification provides a comprehensive architecture for putting storage devices such as SEDs under standard controls as determined by a trusted platform host.

Tech cost for password resets

Table 7 computes the value of tech time associated with resetting passwords for both encrypted and unencrypted laptop or desktop computers. Here again, it takes more tech time to perform a password reset for a full disk encrypted computer. This time difference is first multiplied by frequency of password resets performed, on average, each year (as determined from survey results). We then multiply the annualized incremental time by the value of tech time (in minutes). As can be seen, the UK sample reports the lowest cost of password reset ($35) and the Japanese sample has the highest cost ($44).

Table 7 Tech cost associated with password resets of a full disk encrypted computer	US	UK	DE	JP
Tech time to reset passwords for FDE computer	19.8	18.2	22.1	20.4
Tech time to reset passwords for unencrypted computer	17.5	16.1	20.1	18.0
Incremental time difference (minutes) for each reset	2.3	2.1	2.0	2.3
Frequency of password resets per annum	3.3	3.1	2.8	3.1
Time incurred per annum (minutes)	7.5	6.5	5.6	7.3
Tech time cost per hour	$36.0	$35.0	$41.0	$44.0
Tech time cost per minute	$0.6	$0.6	$0.7	$0.7
Value of tech time to reset passwords on FDE computer per annum	$4.5	$3.8	$3.8	$5.3

User idle cost for password resets

Table 8 computes the cost of end-user downtime waiting for the resetting of passwords for both encrypted and unencrypted laptop or desktop computers. As shown above, it takes more time, and therefore a longer wait, to perform a password reset for a full disk encrypted computer. This time difference is first multiplied by frequency of password resets performed, on average, each year (as determined from survey results). We then multiply the annualized incremental time by the value of end-user time (in minutes). As can be seen, the UK sample reports the lowest cost of password reset ($8.6) and the Japanese sample has the highest cost ($32.1).

Table 8 User downtime associated with password resets of a full disk encrypted computer	US	UK	DE	JP
User time waiting for a password reset on a FDE computer	31.4	32.6	23.7	35.7
User time waiting for a password reset on an unencrypted computer	24.2	29.9	20.6	25.3
Incremental time difference (minutes) for each reset	7.2	2.6	3.1	10.4
Frequency of password resets per annum	3.3	3.1	2.8	3.1
Time incurred per annum (minutes)	23.8	8.1	8.9	32.7
User time cost per hour	$56.0	$64.0	$72.0	$59.0
User time cost per minute	$0.9	$1.1	$1.2	$1.0
Value of user time waiting for password resets on a FDE computer per annum	$22.2	$8.6	$10.6	$32.1

Tech cost to encrypt after re-imaging

Table 9 computes the value of tech time encrypting a laptop or desktop computer after re-imaging a hard disk drive. Our survey results suggest that only a small percentage of computers are re-imaged each year. Hence, this percentage is multiplied by total tech time dedicated to the re-encryption task. We then multiply the annualized incremental time by the value of tech time (in minutes). As can be seen, these cost results are relatively consistent across country samples.

Table 9 Value of tech time to re-encrypt a computer after re-imaging a hard disk	US	UK	DE	JP
Percent of desktop or laptop computers re-imaged each year	15%	13%	11%	15%
Tech time to re-encrypt computer after re-imaging a hard disk	20.3	21.4	22.0	20.6
Total tech time to re-encrypt computer after re-imaging a hard disk per annum	2.94	2.86	2.49	3.01
Tech time cost per hour	$36.0	$35.0	$41.0	$44.0
Tech time cost per minute	$0.6	$0.6	$0.7	$0.7
Value of tech time to re-encrypt computer after re-imaging a hard disk per annum	$1.8	$1.7	$1.7	$2.2

User idle cost for initial encryption

Table 10 calculates the value of an end-user’s idle time waiting for the encrypted laptop or desktop computer. We estimate that this initial encryption task happens once during the useful life of the device. Hence, we divide the total estimated downtime by the useful life of the computer. This annualized idle time is then multiplied by the value of user time in minutes. The resulting values show the UK with the highest value of user downtime ($22.8) and Japan with the lowest value of user downtime ($18.7).

Table 10 User downtime associated with the initial encryption of the hard disk	US	UK	DE	JP
User downtime during the initial encryption of the hard disk	64.7	66.8	55.2	54.3
Approximate useful life of computers in years	3.0	3.1	3.0	2.9
User downtime per annum	21.9	21.3	18.7	19.0
User time cost per hour	$56.0	$64.0	$72.0	$59.0
User time cost per minute	$0.9	$1.1	$1.2	$1.0
Value of user downtime during the initial encryption task	$20.5	$22.8	$22.4	$18.7

User excess operating cost

Table 11 reports the annualized value associated with the end-user's excess time operating of a computer during the workday. Excess time includes idle minutes starting-up, hibernating and shutting down a laptop or desktop computer. We first determine the incremental time differences in the user's operation of encrypted and unencrypted devices. We then multiple this time difference by the average number of workdays per year (determined for international labor statistics for four countries). Finally, we multiply this annualized idle time by average user labor costs. This analysis shows wide variation among the four countries; namely, the US sample yields the lowest cost estimate ($160.6), while the UK reports a much higher idle cost ($263.9).

Table 11 User excess time operating a computer with and without encryption	US	UK	DE	JP
User excess time per day incurred operating computer without encryption	1.9	1.9	1.8	1.9
User excess time per day incurred operating computer with encryption	2.6	3.0	2.5	2.6
Incremental excess time difference (minutes)	0.7	1.1	0.7	0.7
Average number of workdays per year	247.5	235.0	225.0	245.0
User time cost per hour	$56.0	$64.0	$72.0	$59.0
User time cost per minute	$0.9	$1.1	$1.2	$1.0
Value of user excess time per day	$0.6	$1.1	$0.8	$0.7
Value of user excess time per annum	$160.6	$263.9	$188.2	$175.4

Tech cost for providing special administration to encrypted drives

Table 12 summarizes our final TCO cost component for full disk encryption. We first estimate the number of times each year that IT technicians are required to access locked computers containing an encrypted drive, but do not have the required token or other credentials. To analyze this cost, we calculate the total number of FDE computers issued and on-hand. We then divide the total number of events by the total number of FDE computers to determine the probability that any one computer will require special services during the year. We then multiply this probability by the calculated value of tech time in minutes to determine cost. As can be seen, this results in only a nominal value for all countries.

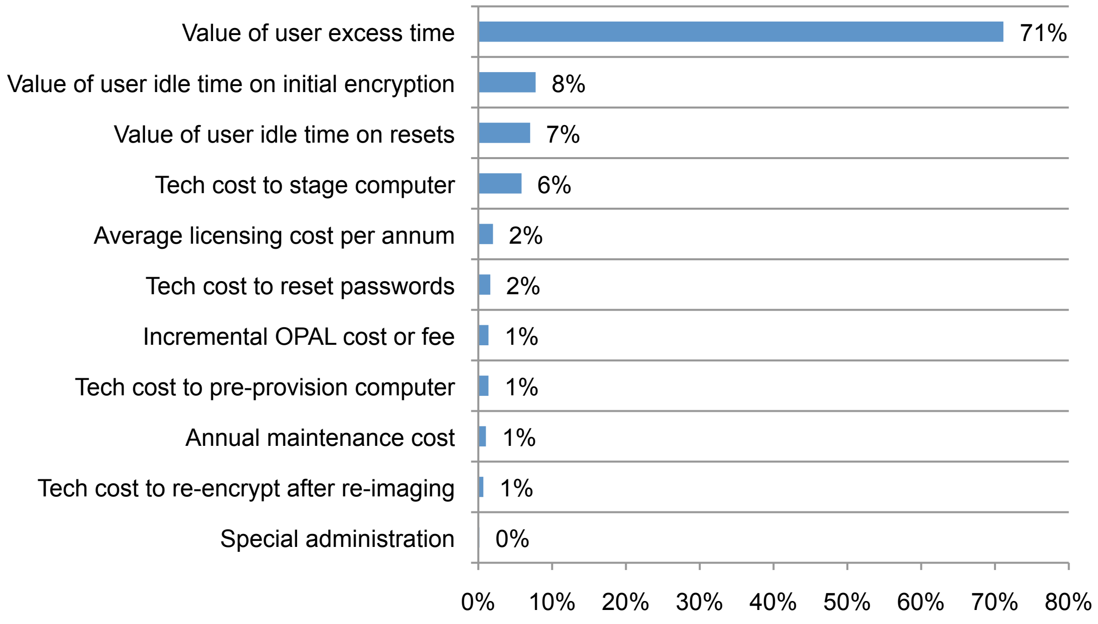
Table 12 Special administration is required to access encrypted drives	US	UK	DE	JP
Times per year special administration is required to access encrypted drives	104.8	98.1	122.7	93.6
Total number of computers issued and on-hand	7,788	5,678	7,421	6,693
Percentage of computers containing FDE	31%	26%	38%	29%
Total number of FDE computers issued and on-hand	2,382	1,473	2,838	1,948
Probability that a given encrypted drive will require special administration per annum	4.4%	6.7%	4.3%	4.8%
Tech time incurred in special administration of encrypted drives	12.9	12.4	15.4	9.5
Tech time cost per hour	$36.0	$35.0	$41.0	$44.0
Tech time cost per minute	$0.6	$0.6	$0.7	$0.7
Value of tech time incurred in special administration of encrypted drives per annum	$0.3	$0.5	$0.5	$0.3

Table 13 summarizes the TCO for full disk encryption on a per computer basis. Representing more than two thirds of the total cost is the incremental value of an end-user's time handling an encrypted laptop or desktop versus an unencrypted machine. The second most significant cost, representing eight percent, concerns idle time among end-users waiting during the initial encryption of the hard disk drive. Another seven percent of cost concerns idle time waiting for the completion of password resets.

Table 13 Recap of TCO Components	US	UK	DE	JP
Licensing cost	5.34	4.82	5.53	5.70
Annual maintenance	2.70	2.71	2.89	2.83
SED Incremental cost	3.96	3.41	3.57	3.86
Tech cost to pre-provision computer	1.28	3.94	6.45	3.52
Tech cost to stage computer	11.99	18.54	16.75	17.11
Tech cost to reset passwords	4.50	3.78	3.83	5.34
Value of idle time for password resets	22.22	8.60	10.63	32.12
Tech cost to re-encrypt after re-imaging	1.77	1.67	1.70	2.21
Value of idle time on initial encryption	20.48	22.75	22.45	18.68
Value of excess time operating computer	160.62	263.95	188.25	175.44
Tech cost of special administration	0.34	0.48	0.45	0.34
Total	235.19	334.67	262.49	267.13

Figure 1 reports the percentage frequency of costs for all four-country samples combined in ascending order of magnitude or importance. Clearly, the unproductive or waiting time of end users appears to drive most of the cost in our TCO framework for full disk encryption. Hence, solutions that moderate the end user's idle or unproductive time operating a desktop or laptop computer would have a significant positive impact on TCO.

Figure 1. Percentage of TCO categories in descending order
Four country samples combined



Part 3. Expected Cost Benefit

Our next analysis attempts to measure the net benefits of full disk encryption. Clearly, one of the main value propositions for encryption is that it lessens the negative consequences of data loss or theft. We assume that the proper use and deployment of full disk encryption would mitigate the total economic impact of a data breach on the organization.

Drawing from our sample data in four countries, we determine the average number of laptop or desktop computers lost or stolen. As shown in Table 14, the percentage of lost of stolen laptops (ranging from 15.5 in Japan to 23.3 in the US) represents a very small percentage relative to the total number of computers assigned and issued to employees.

Also drawing from our four country samples, we determine the average number of records potentially at risk as a result of sensitive or confidential information residing on a laptop or desktop computer that is wrongfully accessed or stolen. The number of potential records at risk is highest in the US (11,518 records) and lowest in Germany (3,935 records).

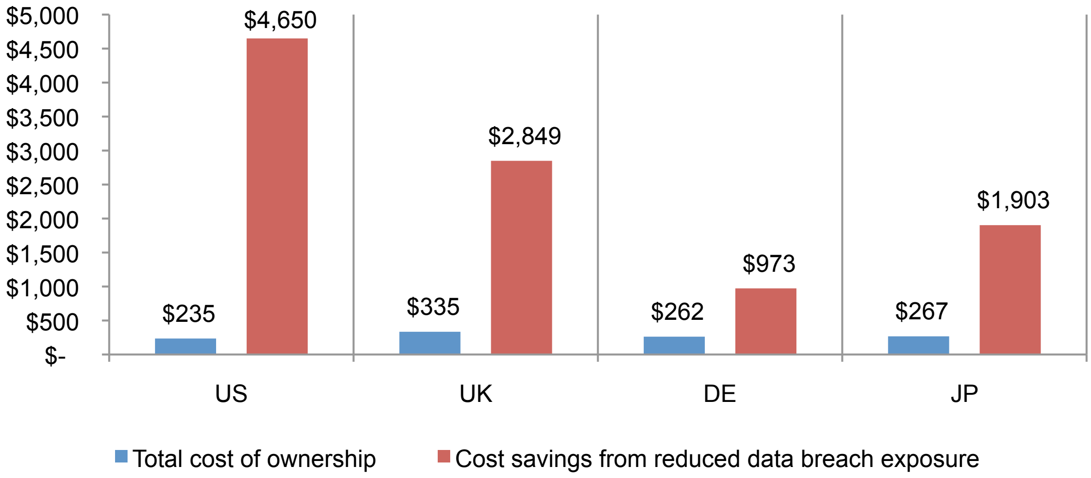
Using our Institute's research on the cost of data breach, we obtained the cost of data breach per compromised record for all four countries (converted into US dollars). Multiplying the per record cost by the average number of records exposed leads to our estimate of the total data breach exposure, which is reflected in millions of dollars in all countries. Multiplying the percentage of computers lost or stolen by the total data breach exposure results in the expected value of data breach exposure. This number varies considerably across country samples – from a low of $1,575 in Germany to a high of $6,698 in the US.

Our final computation uses the percentage of computers enabled by encryption. Again using extrapolations from our survey, we determine that percentage of unencrypted devices. We multiply this percentage by the total data breach exposure to obtain the adjusted data breach exposure. We declare that this number is our best, unbiased estimate of cost savings experienced by companies that participated in our survey resulting from their use of full disk encryption on laptops and desktop computers. Hence, the order cost savings by country is the US ($4,650), UK ($2,849), Japan ($1,903) and Germany ($973).

Table 14 Data breach cost savings	**US**	**UK**	**DE**	**JP**
Number of computers lost or stolen per annum	23.3	19.7	15.6	15.5
Total number of computers	7,788	5,678	7,421	6,693
Percentage of computers lost or stolen per annum	0.30%	0.35%	0.21%	0.23%
Total number of records potentially at risk	11,518	8,931	3,935	8,758
Per capita cost of data breach (Ponemon Institute 2011 study)	$194	$124	$191	$132
Total data breach exposure	$2,234,492	$1,107,444	$751,585	$1,156,056
Expected value of data breach exposure	$6,698	$3,847	$1,575	$2,684
Percentage of **encrypted** lost or stolen computers	31%	26%	38%	29%
Percentage of **unencrypted** lost or stolen computers	69%	74%	62%	71%
Adjusted data breach exposure	$4,650	$2,849	$973	$1,903

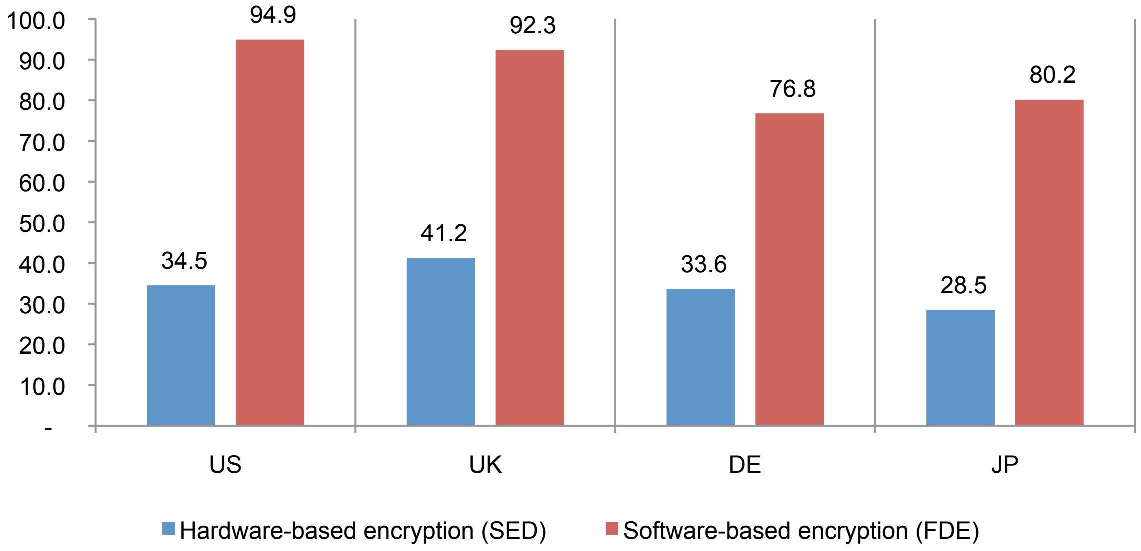
Figure 2 summarizes the cost and benefit analysis explained above. These data provide unambiguous evidence that full disk encryption yields a favorable net benefit. Despites favorable results in all four countries, we clearly see that organizations in the US experience the highest net value ($4,414), while German organizations experience a sizable but lower net value ($710).

Figure 2. Cost and benefit of full disk encryption on laptop and desktop computers



As noted in our TCO calculation, end-user idle time that results from the normal operation or handling of a full disk encrypted laptop or desktop represents the most costly components. Figure 3 provides additional insights, showing a user's downtime is substantially lower in the case of hardware-based encryption (SED) versus software-based encryption.

Figure 3. Idle time in minutes experienced by users during the initial encryption of a computer drive
Extrapolated value computed for each country sample



Part 4. Other TCO findings

Figure 4 reports the average TCO by the global headcount range of participating companies. The pattern of results suggests a U-shape relationship where the smallest and largest-sized companies have a higher average TCO than organizations in the middle ranges.

Figure 4. Average TCO by organizational headcount
Four country samples combined

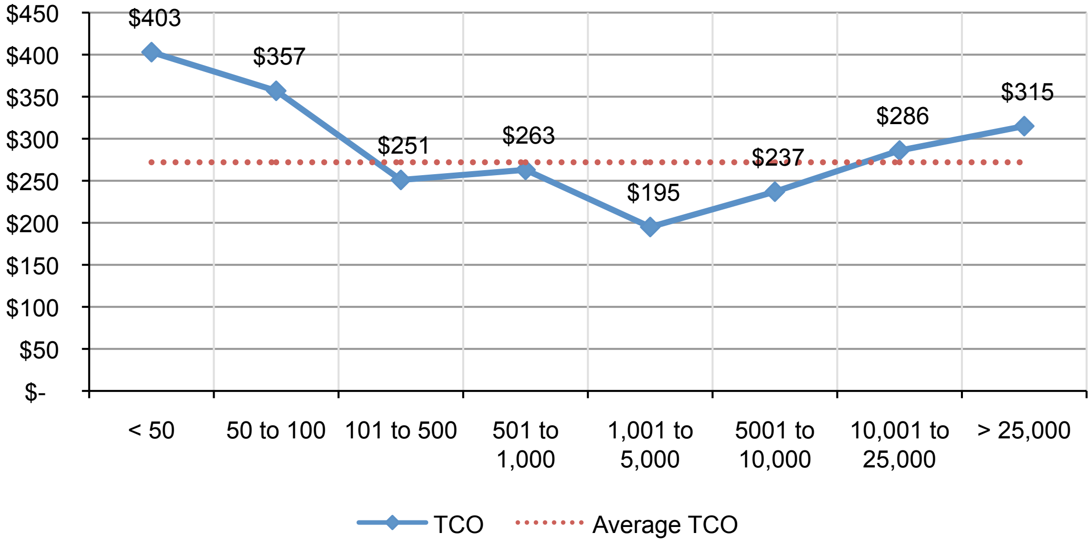
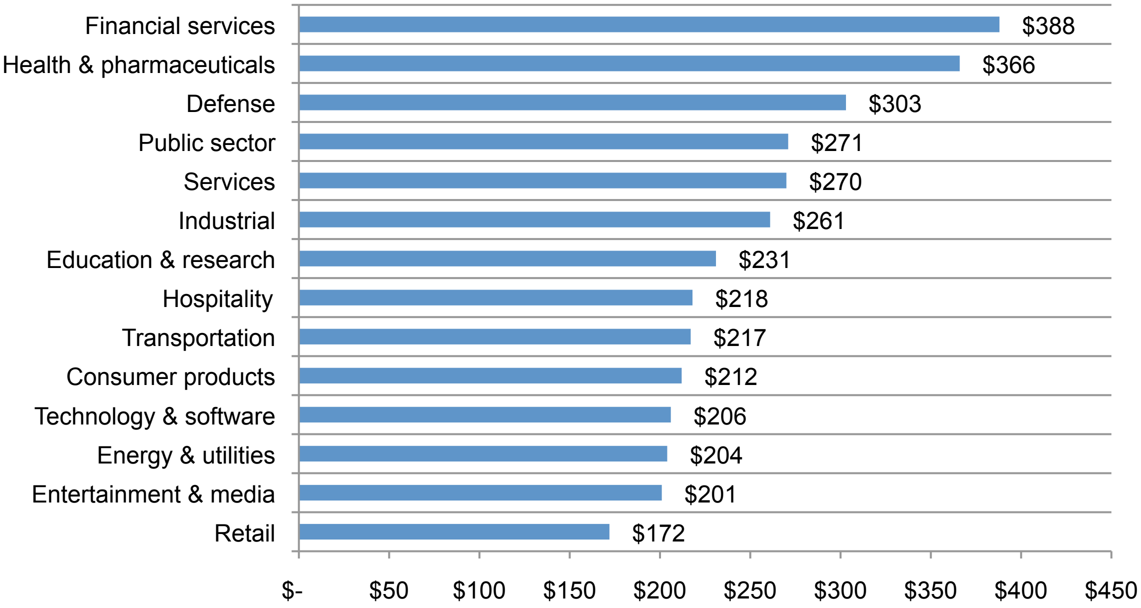


Figure 5 shows the average TCO by the participating organization's primary industry classification. As shown below, there appears to be marked differences in the TCO for full disk encryption based on industry, wherein heavily regulated entities such and financial services and healthcare experience the highest TCO. In contrast, companies in retail experience the lowest TCO.

Figure 5. Average TCO by industry sector
Four country samples combined



Part 5. Other survey findings

Figure 6 reports the usage rate of self-encrypting drive technologies relative to all computers containing a hard disk drive. As can be seen, the present usage rate is highest in the US (eight percent) and lowest in the UK (three percent). This figure also shows the project usage of SEDs over the next 12 months, which indicates an increase in all four countries.

Figure 6. Percentage of laptop and desktop enabled by self-encrypting drive (SED) technology
Extrapolated value computed for each country sample

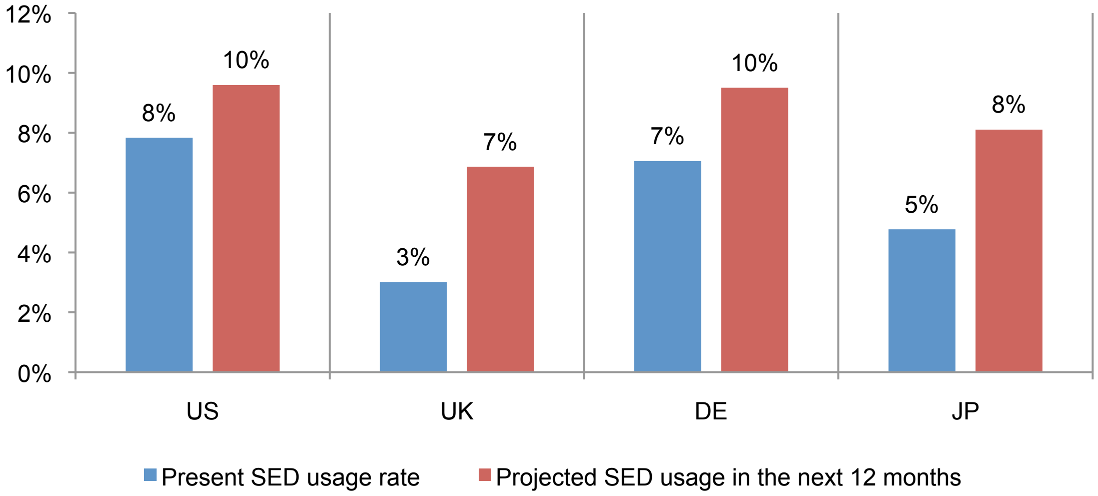


Figure 7 reports the average number of employee-assigned desktop or laptop computers lost or stolen over the past year. The US reports the highest average number at 23.3 computers and Japan reports the lowest average number at 15.5 computers.

Figure 7. Frequency of lost or stolen computers over the past 12-month period
Extrapolated value computed for each country sample

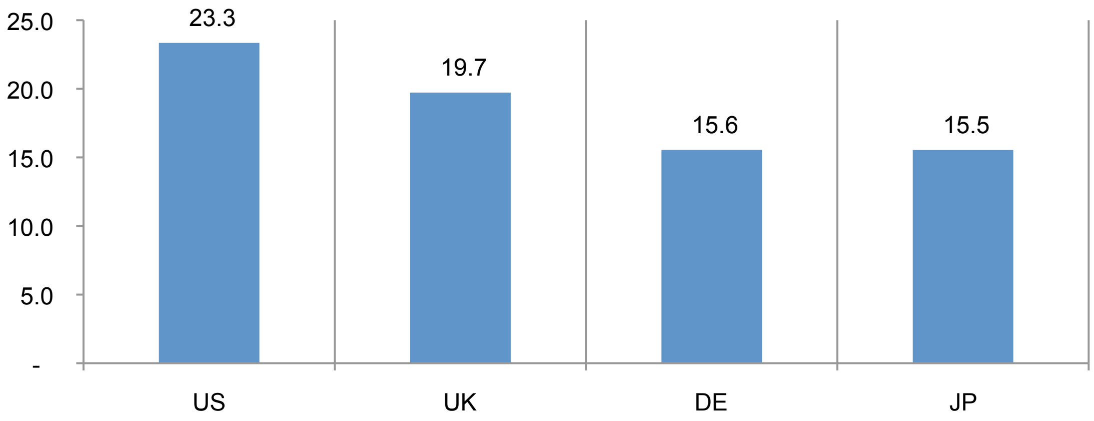


Figure 8 reports the extrapolated average number of sensitive or confidential records that are at risk as a result of the lost or stolen computers indicated in the above chart over the past year. The US reports 11,518 records, which represents the highest number of exposed records. German companies report a much lower number of 3,935 exposed records.

Figure 8. Number of records contained on lost or stolen computers
Extrapolated value computed for each country sample

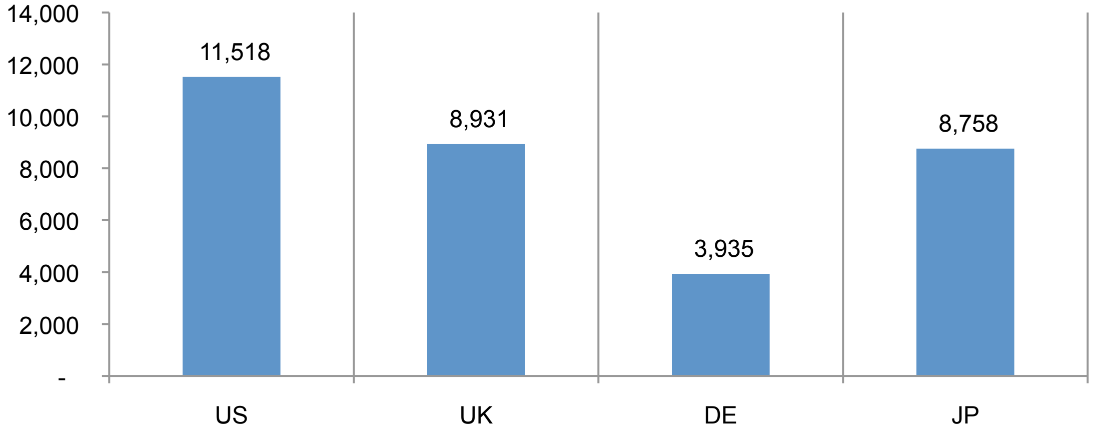


Figure 9 shows the percent deployment of whole or full disk encryption relative to all computers issued to employees. As can be seen, German companies have the highest disk encryption usage rate at 38 percent and UK companies have the lowest disk encryption usage rate at 26 percent.

Figure 9. Percentage of computers enabled with encryption
Extrapolated value computed for each country sample

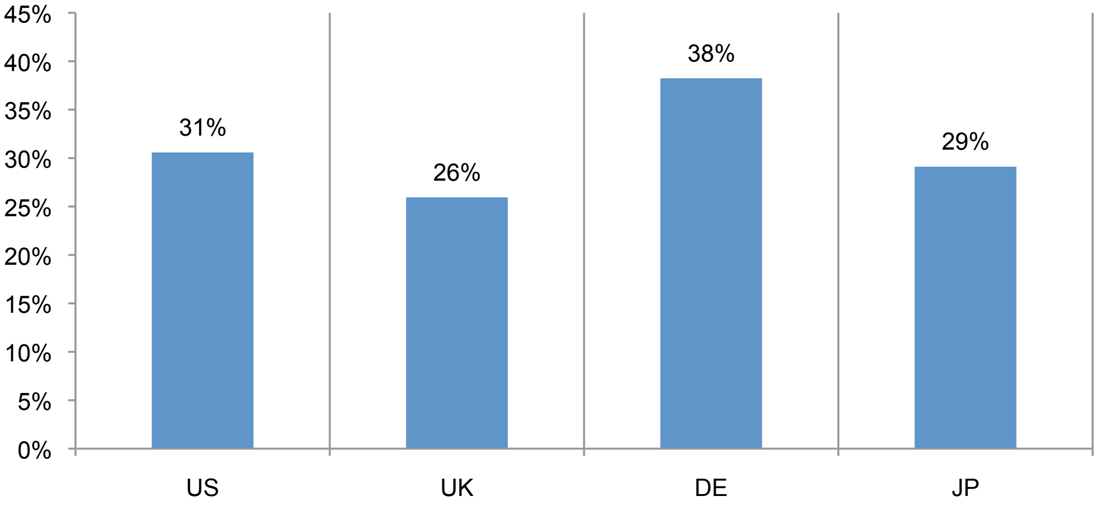


Figure 10 reports eight types of information that respondents believe are normally encrypted.[3] Trade secrets and financial information have the highest percentage rate of encryption (both at 41 percent). In contrast, source code and consumer data has the lowest encryption rates at five and 11 percent, respectively.

Figure 10. Types of information normally encrypted
Four country samples combined

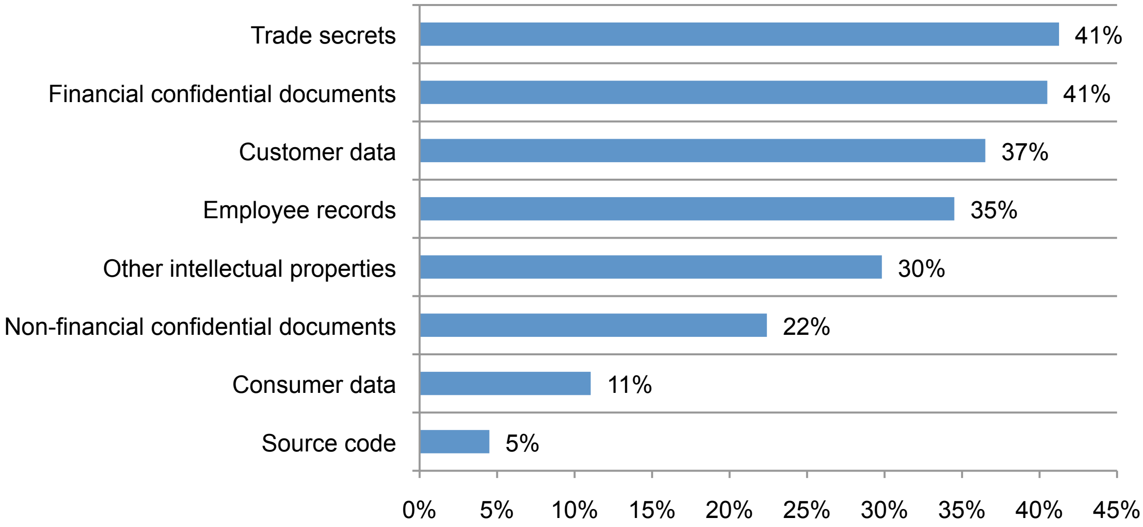
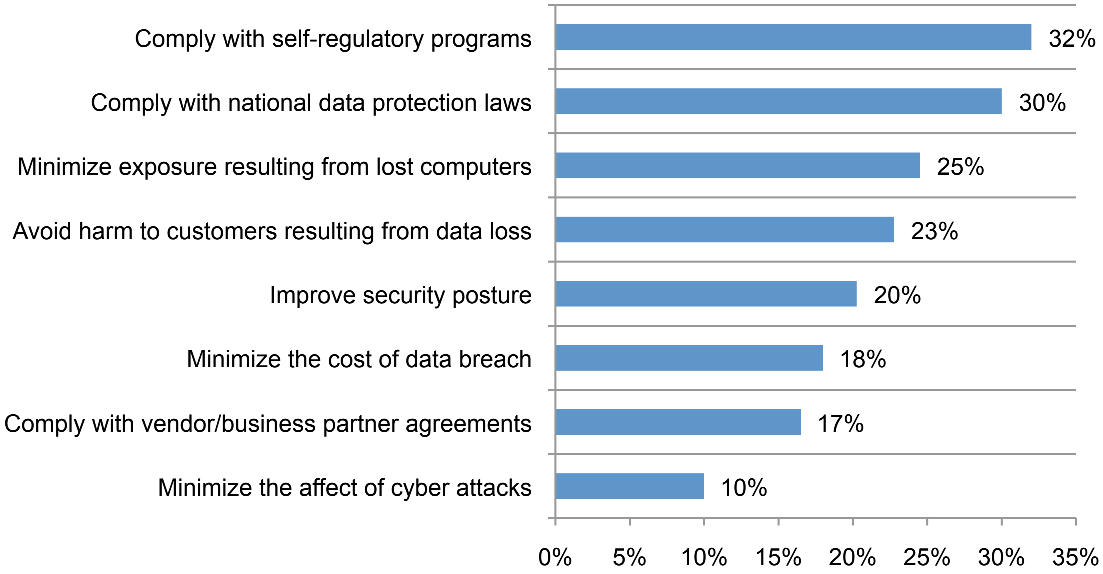


Figure 11 provides a list of reasons why organizations choose to encrypt laptop and desktop computers. According to this chart, compliance with self-regulations and national laws are the two main reasons. The least important reasons are minimizing cyber attacks on devices and complying with vendor or business partner agreements.

Figure 11. Reasons for encrypting data on laptop and desktop computers
Four country samples combined (top two choices)



[3] In the context of this study, customer data is specific data the organization has collected about its customers such as their account information and purchases. Consumer data is information the organization has for marketing or other communications.

Figure 12 reports the average rank for six attributes considered important in the context of evaluating a full disk encryption solution.[4] As can be seen, the top attribute is strong security followed by performance/speed. The least important attributes are interoperability and total cost of ownership.

Figure 12. Attributes considered most important in evaluating a full disk encryption solution
Four country samples combined (ranking from 6 = highest to 1 = lowest)

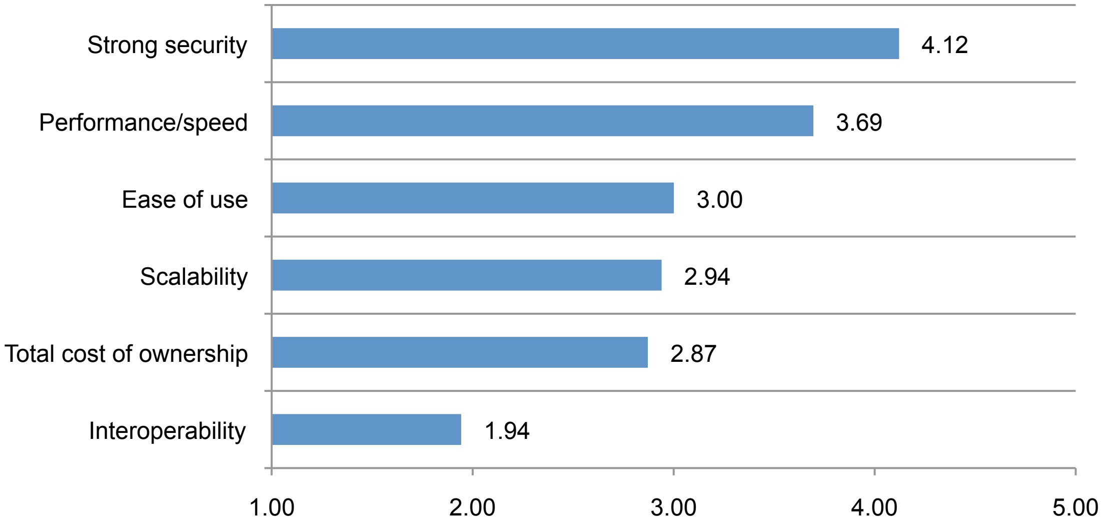
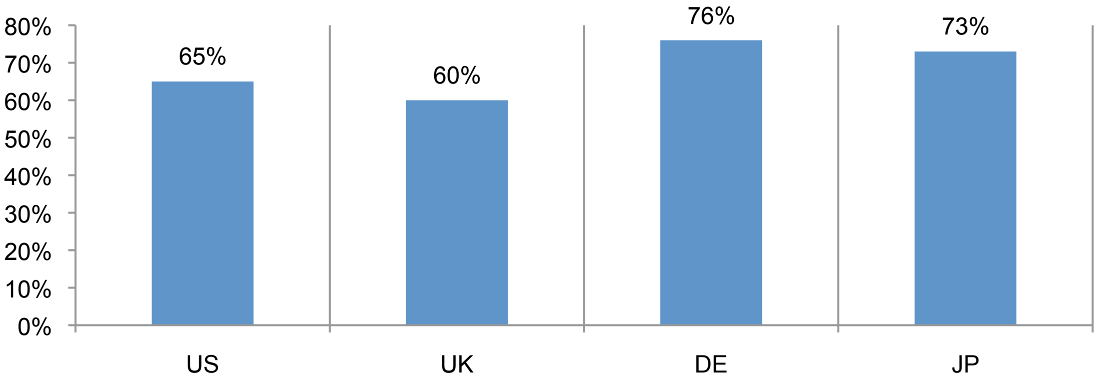


Figure 13 summarizes the very important and important response to the question, “How important is compliance with high security standards such as AES/FIPS 197 to your organization’s decision to select a disk encryption solution?” As can be seen, the very important and important responses in all four countries are high, thus corroborating the finding that strong security is important to the full disk encryption product evaluation and selection decision.

Figure 13. Importance of compliance with high security standards
Very important and important response combined



[4] The rank ordering used for the question was cast from 1 = most important attribute to 6 = least important attribute. For exposition purposes, this graph shows results re-ranked in the opposite order.

Part 6. Methods

Table 15 summarizes the sample response for four separate country studies. As can be seen, the total number of individuals invited to participate in all four countries was 74,886 and ranged from 24,600 in the US to 14,701 in Japan. This resulted in total returns of 2,069. We then reduced the sample by 734 returns because of reliability checks and further screening criteria. This resulted a final sample of 425 in the US, 339 in the UK, 353 in Germany and 218 in Japan (totaling 1,355 bona fide respondents with an overall response rate of 1.78 percent.

We recognized that certain questions about the TCO of full disk encryption could require input or collaboration from others in the respondent's organization. Hence, our administrative procedure allowed respondents to freeze[5] the survey window in order to collect additional details or obtain feedback from other knowledgeable individuals if deemed necessary. About 45 percent of all surveys completed utilized this freeze procedure.

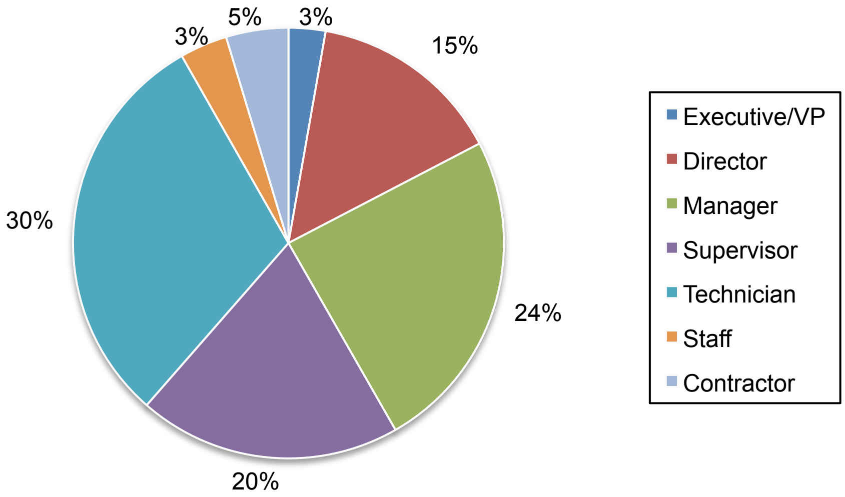
Table 15	United States	United Kingdom	Germany	Japan	
Sample response	**US**	**UK**	**DE**	**JP**	**Total**
Sampling frame	24,600	18,701	16,884	14,701	74,886
Total returns	645	534	518	372	2,069
Rejected surveys	109	89	67	54	319
Screened surveys	111	106	98	100	415
Final sample	425	339	353	218	1,335
Response rate	1.73%	1.81%	2.09%	1.48%	1.78%

Table 16 shows the total years of relevant work experience for respondents in all four countries. As can be seen, respondents are highly experienced, ranging from 10.03 years in the UK to 8.99 years in Japan.

Table 16. Total years of relevant experience (mean years)	**US**	**UK**	**DE**	**JP**
Total years of IT or security experience	9.82	10.03	9.56	8.99
Total years in current position years	5.6	4.89	6.07	5.55

Pie Chart 1 reports the respondents' self-report position level within their organization. As shown, more than 62 percent of respondents hold positions at or above the supervisory level.

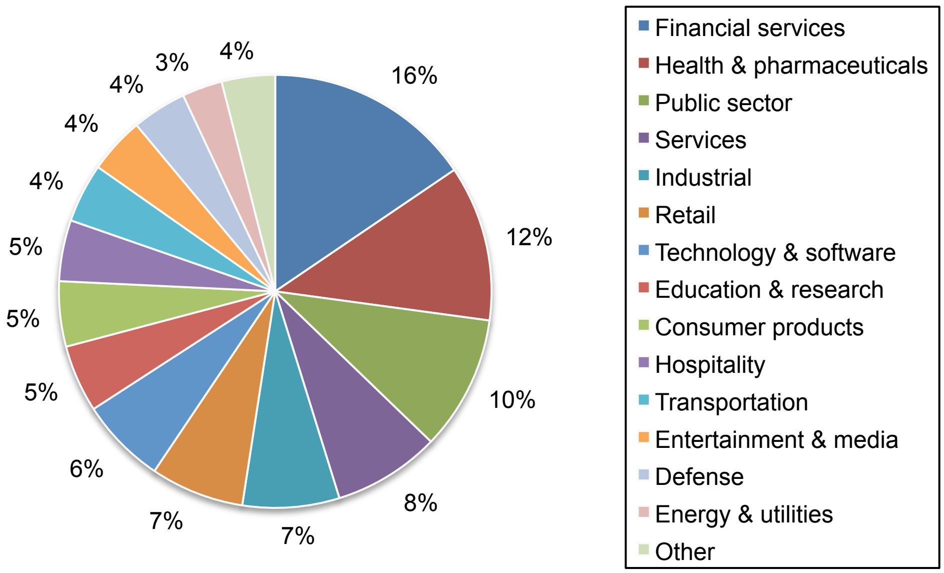
Pie Chart 1. Respondent's position level combined for four countries



[5] This procedure allowed respondents to temporarily leave the survey and return to the survey window at any time, thus permitting them to stop and re-start the survey without loosing any items already completed. Respondents could re-start as many times as deemed necessary to collect all the relevant facts.

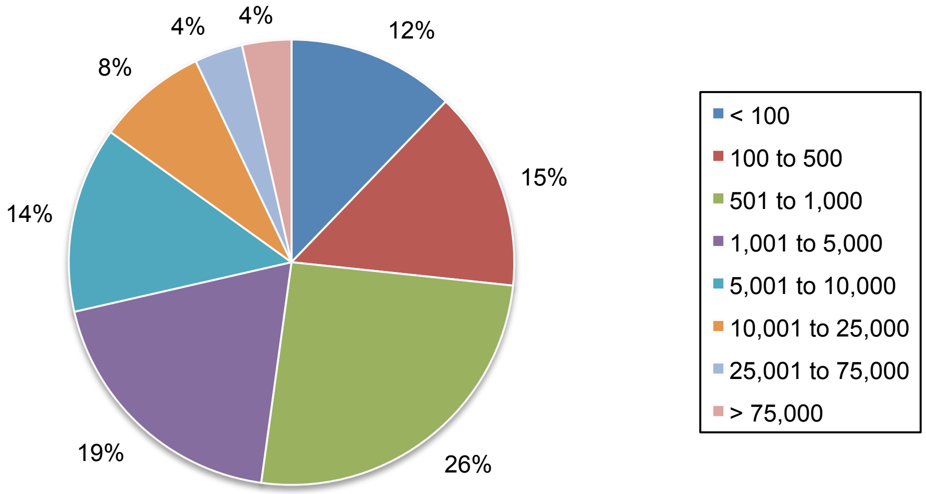
Pie Chart 2 reports the approximate industry classification for respondents' organizations. The top three industries include financial services (16 percent), health & pharmaceuticals (12 percent) and public sector organizations (10 percent). Financial services include companies in banking, investment management, brokerage, insurances, and credit card/payments. Health companies include health service providers, insurers, medical technologies, health IT and others. Public sector includes national and local government entities.

Pie Chart 2. Industry classification of organizations combined for four countries



Pie Chart 3 summarizes the organizational headcount of respondents' organizations. About 47 percent of respondents' companies have 1,000 or more employees. Approximately 27 percent of companies are small-to-medium sized businesses (SMBs) with headcount at or below 500 people.

Pie Chart 3. Organizational headcount (size) for four countries



Part 7. Limitations and conclusion

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 and IT security located in four countries, 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 or perceptions about data protection activities 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 and IT security 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.

Conclusion

Despite a potential total cost burden, the value of full disk encryption far outweighs the cost by a factor 4 to 20 depending on the country. The user and IT cost of deploying and running a full disk encryption solution is much higher than the pure software cost. This sheds a new light on allegedly “free” encryption solutions that come with operating systems. These may have significantly higher TCO compared to commercial full disk encryption solutions that have minimal impact on IT processes and end-user productivity.

Appendix 1: Detailed Survey Responses

The following survey questions were fielded in June 2012. Additional debriefing procedures were completed in late June and early July 2012. Respondents in all four countries were tested to determine the adequacy of their credentials and reliability of their responses.

Part 1. Screening questions				
S1. Does your organization deploy full or whole disk encryption solutions for desktops and laptops?	**US**	**UK**	**DE**	**JP**
Yes	425	339	353	218
No	111	106	98	100
Total	536	445	451	318

S2. How familiar are you with self-encrypting drives (SED) and the Trusted Computing Group's OPAL standards?	**US**	**UK**	**DE**	**JP**
Very familiar	129	92	93	37
Somewhat familiar	219	178	205	132
Not familiar	56	49	41	36
No knowledge	21	20	14	13
Total	425	339	353	218

	US	**UK**	**DE**	**JP**
Final sample size	425	339	353	218

Part 2. Total cost of ownership				
Q1. Approximately, what range best reflects the number of desktops and laptops used by employees in your organization for work-related purposes? Please exclude desktops and laptops that are owned by employees.	**US**	**UK**	**DE**	**JP**
< 50	7%	9%	7%	6%
50 to 100	9%	11%	10%	13%
101 to 500	9%	10%	11%	14%
501 to 1,000	14%	16%	13%	12%
1,001 to 5,000	15%	19%	15%	16%
5001 to 10,000	17%	16%	18%	16%
10,001 to 25,000	19%	14%	15%	13%
> 25,000	10%	5%	11%	10%
Total	100%	100%	100%	100%

Q2a. Does your organization deploy self-encrypting drives (SEDs)?	**US**	**UK**	**DE**	**JP**
Yes	36%	26%	40%	28%
No	64%	74%	60%	72%
Total	100%	100%	100%	100%

Q2b. At present, what range best reflects the percentage of desktops and laptops used by employees in your organization that are enabled with self-encrypting (SED) or OPAL-based disk drives?	US	UK	DE	JP
< 1%	65%	69%	60%	62%
1 to 5%	12%	23%	15%	21%
6 to 10%	6%	3%	12%	6%
11 to 20%	5%	2%	5%	7%
21 to 40%	6%	2%	3%	2%
41 to 60%	3%	1%	2%	1%
61 to 80%	2%	0%	2%	0%
81 to 99%	1%	0%	0%	1%
All drives (100%)	0%	0%	1%	0%
Total	100%	100%	100%	100%

Q2c. In the **next 12 months**, what range best estimates the percentage of desktops and laptops used by employees in your organization that are enabled with self-encrypting (SED) or OPAL-based disk drives?	US	UK	DE	JP
< 1%	49%	55%	52%	51%
1 to 5%	15%	17%	19%	24%
6 to 10%	12%	12%	14%	11%
11 to 20%	16%	11%	6%	6%
21 to 40%	2%	2%	3%	2%
41 to 60%	1%	0%	2%	2%
61 to 80%	2%	1%	1%	1%
81 to 99%	2%	1%	2%	2%
All drives (100%)	1%	1%	1%	1%
Total	100%	100%	100%	100%

Q3. Approximately, what is the useful life of desktops and laptops used by employees in your organization?	US	UK	DE	JP
1 year	0%	0%	0%	1%
2 years	31%	28%	29%	33%
3 years	50%	45%	52%	50%
4 years	13%	16%	14%	12%
5 years	5%	8%	5%	3%
> 5 years	1%	3%	0%	1%
Total	100%	100%	100%	100%

Q4a. What is the licensing cost or fee on a per desktop and laptop basis for **hardware**-based disk encryption solutions used by your organization?	US	UK	DE	JP
None	25%	26%	28%	25%
$1 to $5	24%	22%	29%	23%
$6 to $10	21%	26%	23%	21%
$11 to $15	14%	11%	4%	15%
$16 to $20	13%	12%	12%	11%
$21 to $30	2%	1%	0%	1%
$31 to $40	1%	2%	0%	2%
$41 to $50	0%	0%	2%	1%
> $50	0%	0%	2%	1%
Total	100%	100%	100%	100%

Q4b. What is the licensing cost or fee on a per desktop and laptop basis for **software**-based disk encryption solutions used by your organization?	US	UK	DE	JP
None	0%	0%	0%	0%
$1 to $5	2%	0%	1%	0%
$6 to $10	3%	8%	5%	2%
$11 to $15	13%	15%	12%	13%
$16 to $20	25%	30%	28%	34%
$21 to $30	32%	21%	25%	23%
$31 to $40	19%	21%	18%	21%
$41 to $50	5%	5%	4%	6%
> $50	1%	0%	7%	1%
Total	100%	100%	100%	100%

Q5. As a percentage to the upfront licensing cost or fee (indicated above), what range best reflects the **annual maintenance cost** for desktop or laptop disk encryption solutions used by your organization?

Hardware-based encryption solutions	US	UK	DE	JP
< 1%	1%	0%	1%	0%
1 to 5%	19%	17%	14%	20%
6 to 10%	22%	24%	20%	21%
11 to 15%	25%	26%	29%	30%
16 to 20%	14%	13%	12%	13%
21 to 25%	10%	9%	12%	5%
26 to 30%	6%	5%	7%	5%
31 to 40%	1%	2%	2%	3%
41 to 50%	2%	3%	2%	2%
> 50%	0%	1%	1%	1%
Total	100%	100%	100%	100%

Software-based encryption solutions	US	UK	DE	JP
< 1%	0%	0%	0%	0%
1 to 5%	0%	0%	0%	1%
6 to 10%	11%	10%	12%	10%
11 to 15%	15%	21%	16%	19%
16 to 20%	31%	23%	33%	23%
21 to 25%	15%	16%	12%	21%
26 to 30%	17%	12%	13%	12%
31 to 40%	6%	10%	11%	8%
41 to 50%	5%	8%	3%	6%
> 50%	0%	0%	0%	0%
Total	100%	100%	100%	100%

Q6. Approximately, what is the incremental cost or fee on a per desktop and laptop basis for OPAL?	US	UK	DE	JP
None (we don't use OPAL)	34%	41%	38%	37%
$1 to $5	10%	8%	6%	9%
$6 to $10	14%	19%	28%	16%
$11 to $15	25%	19%	13%	19%
$16 to $20	14%	8%	9%	14%
$21 to $25	2%	5%	5%	4%
> $25	1%	0%	1%	1%
Total	100%	100%	100%	100%

Q7. What is your organization's experience on password resets? Approximately, on a per desktop and laptop basis, how many password resets does your organization experience over a **12-month** period?	US	UK	DE	JP
< 1	1%	0%	0%	0%
1 reset	12%	10%	14%	9%
2 resets	33%	41%	35%	31%
3 resets	23%	21%	27%	35%
4 resets	16%	12%	11%	15%
5 resets	8%	12%	10%	6%
6 to 10 resets	3%	2%	3%	1%
11 to 15 resets	3%	2%	0%	3%
> 15 resets	1%	0%	0%	0%
Total	100%	100%	100%	100%

Q8a. Over the **past 12 months**, how many employee-assigned desktop and laptop computers were lost or stolen?	US	UK	DE	JP
None	11%	12%	9%	10%
< 5	23%	25%	35%	26%
5 to 10	23%	27%	20%	26%
11 to 20	15%	14%	13%	24%
21 to 30	12%	10%	16%	8%
31 to 40	6%	5%	2%	3%
51 to 100	5%	3%	2%	0%
101 to 200	2%	1%	3%	1%
> 200	3%	3%	0%	2%
Total	100%	100%	100%	100%

Q8b. What percent of lost or stolen desktop and laptop computers over the **past 12 months** contained full or whole disk encryption?	US	UK	DE	JP
None	38%	45%	23%	37%
< 1%	5%	4%	9%	8%
1 to 5%	1%	2%	6%	5%
6 to 10%	2%	5%	6%	3%
11 to 20%	11%	9%	8%	5%
21 to 40%	8%	6%	5%	10%
41 to 60%	14%	11%	15%	12%
61 to 80%	5%	3%	2%	3%
81 to 99%	2%	3%	1%	2%
All drives (100%)	14%	12%	25%	15%
Total	100%	100%	100%	100%

Q9. Approximately, how many lost or stolen desktop and laptop computers over the past 12 months contained **unencrypted** (i.e., data in clear text) sensitive or confidential business information?	US	UK	DE	JP
None	35%	35%	32%	33%
< 10%	9%	7%	15%	11%
10 to 25%	10%	8%	18%	8%
26 to 50%	15%	14%	16%	13%
51 to 75%	11%	10%	12%	14%
76 to 100%	20%	26%	7%	21%
Total	100%	100%	100%	100%

Q10a. Did any of these lost or stolen desktop or laptop computers result in a data breach incident requiring notification to individuals (a.k.a. data breach victims) as required by laws and regulations.	US	UK	DE	JP
Yes	36%	7%	27%	5%
No	50%	78%	60%	89%
Unsure	14%	15%	13%	6%
Total	100%	100%	100%	100%

Q10b. Approximately how many individual records were lost or stolen? Sum across all data breach incidents.	US	UK	DE	JP
< 100	3%	6%	5%	8%
101 to 1,000	23%	25%	36%	25%
1,001 to 5,000	25%	31%	36%	25%
5,001 to 10,000	29%	21%	18%	26%
10,001 to 50,000	15%	14%	5%	14%
50,001 to 100,000	4%	3%	0%	1%
> 100,000	1%	0%	0%	1%
Total	100%	100%	100%	100%

Q11a. On average, how much **tech time** does it take to **pre-provision** an employee’s full disk encrypted desktop or laptop computer?	US	UK	DE	JP
< 5 minutes	25%	24%	22%	32%
5 to 10 minutes	14%	16%	24%	15%
11 to 15 minutes	9%	12%	9%	8%
16 to 20 minutes	11%	10%	12%	13%
21 to 30 minutes	10%	14%	11%	9%
31 to 40 minutes	11%	9%	7%	8%
41 to 50 minutes	11%	8%	6%	9%
51 to 60 minutes	8%	7%	8%	6%
> 1 hour	1%	1%	1%	1%
Total	100%	100%	100%	100%

Q11b. On average, how much **tech time** does it take to **pre-provision** an employee’s unencrypted desktop or laptop computer?	US	UK	DE	JP
< 5 minutes	33%	34%	42%	39%
5 to 10 minutes	26%	24%	25%	28%
11 to 15 minutes	11%	18%	16%	15%
16 to 20 minutes	2%	8%	10%	1%
21 to 30 minutes	3%	7%	5%	2%
31 to 40 minutes	1%	1%	1%	1%
41 to 50 minutes	6%	5%	1%	8%
51 to 60 minutes	6%	2%	0%	4%
> 1 hour	12%	1%	0%	2%
Total	100%	100%	100%	100%

Q12a. On average, how much **tech time** does it take to **stage** (a.k.a. make ready for employees' use) a desktop or laptop computer with full disk encryption?	**US**	**UK**	**DE**	**JP**
< 10 minutes	1%	2%	2%	3%
11 to 15 minutes	5%	8%	4%	5%
16 to 20 minutes	12%	16%	17%	20%
21 to 30 minutes	21%	15%	20%	17%
31 to 40 minutes	17%	10%	17%	16%
41 to 50 minutes	17%	16%	9%	8%
51 to 60 minutes	8%	6%	8%	9%
1 to 2 hours	7%	1%	8%	3%
> 2 hours	12%	26%	15%	20%
Total	100%	100%	100%	100%

Q12b. On average, how much **tech time** does it take to **stage** (a.k.a. make ready for employees' use) an unencrypted desktop or laptop computer?	**US**	**UK**	**DE**	**JP**
< 10 minutes	10%	12%	19%	22%
11 to 15 minutes	13%	28%	24%	16%
16 to 20 minutes	22%	24%	19%	20%
21 to 30 minutes	22%	18%	15%	13%
31 to 40 minutes	18%	9%	12%	10%
41 to 50 minutes	5%	2%	4%	9%
51 to 60 minutes	7%	5%	2%	5%
1 to 2 hours	3%	3%	4%	4%
> 2 hours	0%	0%	1%	2%
Total	100%	100%	100%	100%

Q13a. On average, how much **tech time** does it take to perform a **password reset** for a user's desktop or laptop computer with full disk encryption? Please include remote password resets in your estimation.	**US**	**UK**	**DE**	**JP**
< 5 minutes	0%	1%	0%	0%
5 to 10 minutes	14%	16%	12%	15%
11 to 15 minutes	38%	35%	32%	33%
16 to 20 minutes	21%	23%	21%	24%
21 to 30 minutes	11%	16%	15%	13%
31 to 40 minutes	5%	2%	4%	1%
41 to 50 minutes	7%	3%	9%	7%
51 to 60 minutes	3%	3%	4%	6%
1 hour	1%	1%	3%	1%
Total	100%	100%	100%	100%

Q13b. On average, how much **tech time** does it take to perform a **password reset** for a user's unencrypted desktop or laptop computer? Please include remote password resets in your estimation.	US	UK	DE	JP
< 5 minutes	0%	0%	0%	0%
5 to 10 minutes	18%	21%	15%	18%
11 to 15 minutes	41%	36%	29%	35%
16 to 20 minutes	23%	23%	21%	21%
21 to 30 minutes	6%	17%	18%	15%
31 to 40 minutes	4%	3%	10%	6%
41 to 50 minutes	6%	0%	5%	3%
51 to 60 minutes	1%	1%	2%	1%
> 1 hour	0%	0%	0%	1%
Total	100%	100%	100%	100%

Q14a. On average, how much **user time** is incurred waiting for a **password reset** of their desktop or laptop computer with full disk encryption? Please include remote password resets in your estimation.	US	UK	DE	JP
< 5 minutes	10%	12%	15%	6%
5 to 10 minutes	11%	10%	21%	7%
11 to 15 minutes	12%	13%	15%	12%
16 to 20 minutes	9%	12%	13%	12%
21 to 30 minutes	18%	11%	18%	15%
31 to 40 minutes	11%	7%	5%	9%
41 to 50 minutes	10%	11%	1%	13%
51 to 60 minutes	11%	13%	5%	15%
1 to 2 hours	5%	10%	2%	10%
> 2 hours	3%	1%	5%	1%
Total	100%	100%	100%	100%

Q14b. On average, how much **user time** is incurred waiting for a **password reset** of their unencrypted desktop or laptop computer? Please include remote password resets.	US	UK	DE	JP
< 5 minutes	14%	0%	4%	4%
5 to 10 minutes	12%	9%	11%	10%
11 to 15 minutes	14%	16%	19%	12%
16 to 20 minutes	21%	21%	23%	21%
21 to 30 minutes	10%	10%	31%	24%
31 to 40 minutes	16%	15%	7%	19%
41 to 50 minutes	1%	13%	2%	2%
51 to 60 minutes	8%	12%	3%	5%
1 to 2 hours	2%	3%	0%	3%
> 2 hours	2%	0%	0%	0%
Total	100%	100%	100%	100%

Q15a. What percent of desktop or laptop computers are re-imaged each year?	US	UK	DE	JP
None	10%	15%	16%	14%
< 10%	56%	50%	55%	50%
10 to 25%	25%	26%	25%	28%
26 to 50%	3%	5%	2%	2%
51 to 75%	5%	4%	2%	3%
76 to 100%	1%	0%	0%	3%
Total	100%	100%	100%	100%

Q15b. On average, how much **tech time** does it take to **re-encrypt** a desktop or laptop computer after re-imaging a hard disk?	**US**	**UK**	**DE**	**JP**
< 5 minutes	0%	0%	0%	0%
5 to 10 minutes	16%	21%	15%	19%
11 to 15 minutes	30%	29%	23%	28%
16 to 20 minutes	24%	20%	21%	22%
21 to 30 minutes	16%	15%	20%	16%
31 to 40 minutes	4%	2%	12%	5%
41 to 50 minutes	4%	0%	2%	0%
51 to 60 minutes	0%	1%	4%	0%
1 hour	6%	12%	3%	9%
Total	100%	100%	100%	100%

Q16a. On average, how much of an end-user's productive time is lost during the initial encryption of the drive? Assume a **hardware**-based full disk encryption solution is provided.	**US**	**UK**	**DE**	**JP**
< 10 minutes	8%	1%	11%	10%
11 to 15 minutes	18%	22%	14%	15%
16 to 30 minutes	35%	38%	39%	42%
31 to 45 minutes	21%	22%	22%	19%
46 to 60 minutes	13%	11%	10%	12%
1 to 2 hours	2%	2%	2%	1%
2 to 4 hours	2%	1%	1%	1%
4 to 8 hours	1%	2%	0%	0%
> 8 hours (1 full workday)	0%	1%	1%	0%
Total	100%	100%	100%	100%

Q16b. On average, how much of an end-user's productive time is lost during the initial encryption of the drive? Assume a **software**-based full disk encryption solution is provided.	**US**	**UK**	**DE**	**JP**
< 10 minutes	0%	0%	0%	0%
11 to 15 minutes	6%	4%	0%	5%
16 to 30 minutes	13%	12%	19%	10%
31 to 45 minutes	13%	14%	11%	12%
46 to 60 minutes	28%	32%	32%	34%
1 to 2 hours	18%	20%	26%	26%
2 to 4 hours	13%	11%	7%	7%
4 to 8 hours	7%	3%	4%	5%
> 8 hours (1 full workday)	2%	4%	1%	1%
Total	100%	100%	100%	100%

Q17. On average, how much **user time** is incurred operating a desktop or laptop under three separate scenarios: (1) no encryption, (2) software-based encryption and (3) hardware-based encryption (SEDs)? Please estimate the time it takes each day for an average employee to start-up, shutdown and hibernate their computers during the "typical" workday.

Encryption is not deployed	**US**	**UK**	**DE**	**JP**
No time	0%	0%	0%	0%
Less than 30 seconds	11%	12%	11%	10%
31 to 60 seconds	35%	36%	36%	34%
1 to 2 minutes	24%	15%	18%	22%
2 to 3 minutes	13%	23%	20%	21%
3 to 5 minutes	11%	8%	11%	9%
5 to 10 minutes	5%	6%	4%	2%
> 10 minutes	1%	0%	0%	2%
Total	100%	100%	100%	100%

Software-based encryption	**US**	**UK**	**DE**	**JP**
No time	0%	0%	4%	1%
Less than 30 seconds	4%	5%	3%	2%
31 to 60 seconds	8%	8%	7%	10%
1 to 2 minutes	36%	31%	30%	32%
2 to 3 minutes	21%	24%	26%	27%
3 to 5 minutes	15%	9%	10%	12%
5 to 10 minutes	7%	4%	11%	10%
> 10 minutes	9%	18%	9%	6%
Total	100%	100%	100%	100%

Hardware-based encryption	**US**	**UK**	**DE**	**JP**
No time	3%	0%	0%	0%
Less than 30 seconds	7%	9%	17%	8%
31 to 60 seconds	36%	38%	36%	32%
1 to 2 minutes	23%	18%	20%	24%
2 to 3 minutes	15%	19%	16%	21%
3 to 5 minutes	10%	8%	7%	9%
5 to 10 minutes	3%	7%	4%	3%
> 10 minutes	3%	1%	0%	4%
Total	100%	100%	100%	100%

Q18a. Does this ever happen in your organization? A system administrator needs to gain access to an encrypted drive on a desktop or laptop computer. However, because the administrator does not have the proper credential (such as a token) to access this particular drive, he or she is required to use other secondary means to gain access. Approximately, over the past 30 days, how often has this situation happened in your organization?	**US**	**UK**	**DE**	**JP**
Never	20%	23%	32%	31%
1 to 5	58%	52%	49%	51%
6 to 10	9%	10%	5%	8%
11 to 25	4%	3%	5%	2%
26 to 50	5%	2%	1%	2%
51 to 100	2%	1%	2%	3%
More than 100	2%	3%	5%	2%
Cannot determine	0%	6%	1%	1%
Total	100%	100%	100%	100%

Q18b. On average, how much incremental **tech time** is incurred by system administrators in gaining access to encrypted drives without having the proper access credentials (such as a token) to access these drives. Please provide an estimate on the basis of time the encrypted drive requires access.	US	UK	DE	JP
No time	20%	18%	15%	12%
< 60 seconds	23%	28%	26%	25%
1 to 5 minutes	21%	15%	20%	32%
6 to 10 minutes	11%	9%	8%	10%
11 to 15 minutes	3%	8%	6%	5%
16 to 30 minutes	2%	5%	2%	3%
31 to 60 minutes	11%	9%	8%	10%
> 60 minutes	9%	8%	15%	3%
Total	100%	100%	100%	100%

Part 3. Other questions

Q19. What types of stored data on disk drives (data-at-rest) are normally encrypted in your organization? Please check all that apply.	US	UK	DE	JP
Consumer data	13%	10%	18%	3%
Customer data	21%	38%	42%	45%
Employee records	21%	25%	52%	40%
Non-financial confidential documents	9%	12%	33%	36%
Financial confidential documents	32%	34%	51%	45%
Source code	4%	2%	8%	4%
Trade secrets	30%	37%	56%	42%
Other intellectual properties	20%	28%	39%	32%
Other (please specify)	1%	0%	0%	1%
Total	151%	186%	299%	249%

Q20. How important is compliance with high security standards (such as AES/FIPS 197) to your organization's decision to select a disk encryption solution?	US	UK	DE	JP
Very important	26%	25%	40%	32%
Important	39%	35%	36%	41%
Somewhat important	15%	25%	15%	20%
Not important	12%	9%	8%	4%
Irrelevant	8%	6%	1%	3%
Total	100%	100%	100%	100%

Q21. Why does your organization encrypt data-at-rest? Please select your top two choices.	US	UK	DE	JP
Comply with state or federal/national data protection laws	36%	26%	35%	23%
Comply with self-regulatory programs such as PCI DSS, ISO, NIST and others	30%	25%	33%	40%
Minimize end-user data mishaps resulting from lost computers	25%	19%	28%	26%
Comply with vendor or business partner agreements	11%	15%	13%	27%
Avoid harms to customers resulting from data loss or theft	20%	22%	28%	21%
Minimize the cost of data breach	23%	15%	19%	15%
Minimize the affect of cyber attacks	9%	11%	14%	6%
Improve security posture	15%	28%	25%	13%
Other (please specify)	2%	1%	0%	2%
Total	171%	162%	195%	173%

Q22. In evaluating full encryption solutions for your organization, how important is each attribute listed below? Please rank the following six attributes from 1 = most important to 6 = least important to your organization.	US	UK	DE	JP
Performance/speed	1.96	2.20	2.71	2.35
Strong security	1.87	2.96	1.88	0.80
Scalability	2.77	3.93	2.63	2.91
Interoperability	4.41	4.77	3.38	3.68
Ease of use	3.67	2.23	2.83	3.27
Total cost of ownership	3.40	3.03	3.74	2.35
Average	3.01	3.19	2.86	2.56

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

Q23a. Ease of deployment: Encryption key is generated in the factory	US	UK	DE	JP
Very important	23%	25%	22%	21%
Important	32%	30%	34%	29%
Somewhat important	30%	29%	26%	28%
Not important	12%	10%	12%	14%
Irrelevant	3%	6%	6%	8%
Total	100%	100%	100%	100%

Q23b. Transparency: Once unlocked, it functions as a regular drive	US	UK	DE	JP
Very important	25%	24%	21%	24%
Important	31%	25%	34%	30%
Somewhat important	29%	32%	27%	26%
Not important	13%	9%	10%	15%
Irrelevant	2%	10%	7%	5%
Total	100%	100%	100%	100%

Q23c. Ease of management: Streamlines the IT process by assisting with resetting passwords, recovering devices and unattended software updating	US	UK	DE	JP
Very important	28%	25%	20%	22%
Important	31%	26%	39%	34%
Somewhat important	27%	34%	30%	25%
Not important	10%	8%	11%	10%
Irrelevant	5%	7%	0%	8%
Total	100%	100%	100%	100%

Q23d. Life-cycle costs: Lower initial and on-going costs	US	UK	DE	JP
Very important	26%	25%	21%	25%
Important	27%	24%	35%	30%
Somewhat important	24%	29%	26%	27%
Not important	13%	15%	15%	13%
Irrelevant	9%	8%	3%	5%
Total	100%	100%	100%	100%

Q23f. Disposal or re-purposing cost: Erasure made easy	US	UK	DE	JP
Very important	26%	27%	21%	27%
Important	27%	23%	42%	26%
Somewhat important	22%	28%	25%	36%
Not important	15%	16%	10%	9%
Irrelevant	10%	6%	2%	2%
Total	100%	100%	100%	100%

Q23g. Re-encryption: With self-encrypting drives, there is no need to ever re-encrypt the data	US	UK	DE	JP
Very important	26%	25%	19%	23%
Important	22%	25%	40%	28%
Somewhat important	27%	26%	29%	34%
Not important	13%	18%	12%	11%
Irrelevant	12%	7%	0%	4%
Total	100%	100%	100%	100%

Q23h. Performance: No degradation in self-encrypting drive (SED) performance	US	UK	DE	JP
Very important	26%	21%	23%	24%
Important	28%	32%	38%	26%
Somewhat important	28%	25%	27%	26%
Not important	12%	20%	12%	22%
Irrelevant	6%	3%	0%	2%
Total	100%	100%	100%	100%

Q23i. Standardization: Whole drive industry is building to the TCG/OPAL specifications	US	UK	DE	JP
Very important	26%	21%	27%	23%
Important	18%	23%	37%	23%
Somewhat important	27%	36%	28%	36%
Not important	11%	15%	5%	14%
Irrelevant	18%	5%	3%	3%
Total	100%	100%	100%	100%

Q23j. Compatibility with other security software and encryption key management platforms	US	UK	DE	JP
Very important	21%	28%	25%	26%
Important	24%	22%	33%	30%
Somewhat important	35%	34%	28%	25%
Not important	12%	14%	9%	13%
Irrelevant	8%	2%	5%	6%
Total	100%	100%	100%	100%

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-encrypted drives, self-encrypting drives . . .

Q24a. Prevent end-user tampering or disablement of encryption feature.	US	UK	DE	JP
Strongly agree	30%	26%	35%	22%
Agree	27%	23%	30%	26%
Unsure	28%	31%	23%	36%
Disagree	13%	14%	9%	11%
Strongly disagree	2%	6%	3%	5%
Total	100%	100%	100%	100%

Q24b. Make it easier for managing encryption and authentication keys.	US	UK	DE	JP
Strongly agree	33%	29%	34%	23%
Agree	29%	19%	32%	29%
Unsure	28%	30%	21%	34%
Disagree	10%	14%	6%	6%
Strongly disagree	0%	8%	6%	8%
Total	100%	100%	100%	100%

Q24c. Provide a faster setup time because no initial encryption is required.	US	UK	DE	JP
Strongly agree	34%	21%	38%	19%
Agree	30%	24%	26%	24%
Unsure	24%	29%	24%	33%
Disagree	12%	15%	12%	9%
Strongly disagree	0%	12%	0%	15%
Total	100%	100%	100%	100%

Q24d. Provide greater interoperability based on industry standards versus unique chipset and processor solutions.	US	UK	DE	JP
Strongly agree	32%	23%	36%	24%
Agree	23%	22%	29%	26%
Unsure	28%	30%	24%	37%
Disagree	11%	20%	9%	9%
Strongly disagree	6%	5%	2%	4%
Total	100%	100%	100%	100%

Q24e. Improve portability because there is no system-level dependency.	US	UK	DE	JP
Strongly agree	30%	25%	28%	23%
Agree	30%	23%	28%	24%
Unsure	31%	36%	25%	38%
Disagree	7%	13%	12%	11%
Strongly disagree	2%	2%	7%	4%
Total	100%	100%	100%	100%

Q24f. Improve system performance because the encryption workload is moved off the processor and chipset and onto the drive.	US	UK	DE	JP
Strongly agree	30%	24%	34%	24%
Agree	30%	25%	29%	22%
Unsure	24%	30%	21%	37%
Disagree	7%	14%	11%	7%
Strongly disagree	9%	7%	5%	9%
Total	100%	100%	100%	100%

Q24g. Hardware-based (full disk) encryption provides a higher level of security than software-based full disk encryption.	US	UK	DE	JP
Strongly agree	29%	29%	34%	27%
Agree	23%	22%	28%	25%
Unsure	24%	32%	21%	36%
Disagree	16%	17%	12%	11%
Strongly disagree	8%	0%	6%	1%
Total	100%	100%	100%	100%

Q24h. File and folder-level encryption is an alternative to full disk encryption.	US	UK	DE	JP
Strongly agree	32%	30%	33%	16%
Agree	30%	23%	31%	29%
Unsure	23%	29%	22%	37%
Disagree	10%	16%	13%	15%
Strongly disagree	6%	2%	2%	3%
Total	100%	100%	100%	100%

Q24i. File and folder-level encryption is an attractive addition to full disk encryption.	US	UK	DE	JP
Strongly agree	26%	20%	33%	22%
Agree	24%	23%	30%	24%
Unsure	27%	26%	26%	29%
Disagree	13%	16%	9%	16%
Strongly disagree	10%	15%	3%	9%
Total	100%	100%	100%	100%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	US	UK	DE	JP
Senior Executive	1%	2%	0%	1%
Vice President	1%	0%	0%	6%
Director	17%	12%	15%	14%
Manager	23%	26%	24%	24%
Supervisor	19%	25%	19%	15%
Technician	30%	28%	34%	29%
Staff	5%	4%	2%	3%
Contractor	3%	3%	6%	7%
Other	1%	0%	1%	0%
Total	100%	100%	100%	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	US	UK	DE	JP
CEO/Executive Committee	1%	0%	0%	0%
Chief Financial Officer	1%	2%	0%	3%
General Counsel	2%	0%	1%	5%
Chief Information Officer	56%	60%	58%	61%
Chief Information Security Officer	21%	17%	18%	15%
Compliance Officer	6%	7%	9%	8%
Human Resources VP	0%	3%	2%	0%
Chief Security Officer	3%	2%	2%	0%
Data Center Management	2%	5%	5%	4%
Chief Risk Officer	7%	4%	5%	5%
Other	1%	0%	0%	0%
Total	100%	100%	100%	100%

D3. Total years of relevant experience (mean years)	US	UK	DE	JP
Total years of IT or security experience	9.82	10.03	9.56	8.99
Total years in current position years	5.6	4.89	6.07	5.55

D4. What industry best describes your organization's industry focus?	US	UK	DE	JP
Agriculture & food services	1%	0%	0%	3%
Communications	3%	0%	0%	0%
Consumer products	3%	6%	6%	5%
Defense	2%	2%	6%	7%
Education & research	4%	7%	3%	6%
Energy & utilities	5%	2%	4%	1%
Entertainment & media	3%	7%	5%	1%
Financial services	16%	13%	18%	15%
Health & pharmaceuticals	11%	14%	12%	10%
Hospitality	4%	6%	4%	4%
Industrial	5%	6%	9%	9%
Public sector	10%	15%	9%	7%
Retail	9%	6%	5%	8%
Services	8%	8%	9%	7%
Technology & software	7%	5%	4%	10%
Transportation	4%	4%	4%	6%
Other	5%	0%	2%	1%
Total	100%	100%	100%	100%

D5. Where are your employees located? (Check all that apply):	US	UK	DE	JP
North America	100%	69%	67%	89%
Europe	67%	100%	100%	58%
Middle East & Africa	39%	40%	38%	32%
Asia-Pacific	54%	59%	59%	100%
Latin America (including Mexico)	48%	46%	43%	40%
Total	308%	315%	308%	319%

D6. What is the worldwide headcount of your organization?	US	UK	DE	JP
< 100	12%	11%	10%	16%
100 to 500	11%	18%	10%	19%
501 to 1,000	26%	28%	19%	29%
1,001 to 5,000	18%	18%	31%	10%
5,001 to 10,000	16%	12%	14%	12%
10,001 to 25,000	8%	7%	9%	8%
25,001 to 75,000	5%	4%	3%	2%
> 75,000	4%	2%	4%	4%
Total	100%	100%	100%	100%
Extrapolated value	8,920	6,460	8,277	7,154

Ponemon Institute

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.