Ponemon INSTITUTE

The TCO of Software vs. Hardware-based Full Disk Encryption Summary

Sponsored by WinMagic

Independently conducted by Ponemon Institute LLC

Publication Date: April 2013

Industry Co-Sponsors

intel LSI Storage. Networking. Accelerated. Micron PLEXTOR Never compromise. SAMSUNG Seagate TOSHIBA Leading Innovation

The TCO of Software vs. Hardware-based Full Disk Encryption

Ponemon Institute, April 2013

Part 1. Introduction

This paper extends the findings of the *Total Cost of Ownership for Full Disk Encryption* (FDE), sponsored by WinMagic and independently conducted by Ponemon Institute published in July 2012, The purpose of this original research was to learn how organizations deploy full disk encryption solutions for desktop and laptop computers as well as the determination of total cost and benefits for organizations using this technology.[1] A reanalysis of this research allows us to formulate new findings that compare the total cost of ownership of software versus hardware-based full disk encryption solutions.

Disk encryption is important in 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 that may have a significantly higher TCO than commercial products.

In this paper, we use the term hardware-based full disk encryption and self-encrypting drives (SEDs) interchangeably. Prior Ponemon Institute research shows that SEDs provide hardware-based data security, full disk encryption and enhanced secure erase capabilities.[2] 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.

About the previous study

Ponemon Institute surveyed 1,335 respondents in four separate country samples: the United States (US), United Kingdom (UK), Germany (DE) and Japan (JP) representing a variety of industry sectors. Respondents held bona fide credentials in IT, IT security or data protection, and had nearly 10 years of relevant experience on average. Key findings from this earlier research were:

- Expected benefits of full disk encryption exceeded cost in all four countries by a factor ranging from 4 to 20 times cost.
- TCO varied inversely by organizational size: The organizations with fewer than 50 employees had the highest TCO for full disk encryption.
- TCO varied by industry. Heavily regulated industries such as financial services and healthcare had the highest ownership costs.
- The most expensive component of TCO was the value of diminished user productivity incurred operating a desktop or laptop with encryption.

Our reanalysis of the TCO of software versus hardware-based full disk encryption consists of eleven components: (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.

Cost differences between software and hardware FDE solutions center on four components in the TCO framework, as follows:

- Licensing cost paid to software or hardware vendors on average per year
- OPAL fees (only applicable to hardware-based full disk encryption
- Value of end-user downtime associated with the initial encryption of the hard disk
- Value of excess end-user time operating a full disk encrypted computer

The next section shows each cost component, comparing software and hardware-based FDE cost considerations. Our analysis also includes cost components where software and hardware-based FDE have identical cost implications.

[1] In the context of this paper, full disk encryption means that every bit of data that goes on a disk is encrypted.

[2] See Perceptions about Self-Encrypting Drives: A Study of IT Practitioners. Trusted Computing Group and Ponemon Institute, May 2011.

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.[3] 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	UK	DE
Fully loaded hourly cost of technician time incurred while handling computing devices*	$35	$41
Fully loaded hourly cost of end-users	$64	$72
Approximate useful life of laptops or desktops assigned to end-users in years	3.1	3.0
Average number of 8-hour workdays per year#	235	225

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

The numbers for the summaries below can be seen in the chart following the 11 individual summaries. For a full look at the breakdown within each summary, please refer to the full whitepaper.

Licensing cost

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. Specifically, software licensing appears to be about three to four times more expensive than hardware licensing costs in all four countries.

Annual maintenance cost

The average annual maintenance cost is expressed as a percentage of the total licensing cost, shown separately for software and hardware-based FDE. Using the estimated average licensing cost we calculate the maintenance cost for four country samples. The percentage of annual maintenance cost is derived from one survey question. Once again, extrapolated costs appear to be substantially higher for software versus hardware-based FDE – that is, five times more expensive for annual maintenance costs.

OPAL fees[4]

We computed the incremental licensing fee for OPAL, which only applies to hardware-based encrypted drives or SEDs. As can be seen, we assume software-based full disk encryption does not entail any comparable fee.

Pre-provisioning cost

This analysis computes the cost associated with pre-provisioning an encrypted versus an unencrypted laptop or desktop computer. In this analysis, we assume software and hardware-based FDE will have the same productivity impact on pre-provisioning cost. Thus, incremental time calculated is independent of the full disk encryption method deployed by respondents' organizations.

Staging cost

We looked at the costs associated with the staging of an encrypted and unencrypted laptop or desktop computer. Here again, we assume software and hardware-based FDE will have the same productivity impact on staging cost.

[3] Our comparative analysis of software and hardware FDE is based on a sample of 1,335 knowledgeable respondents in four countries. One-third of respondents say their organizations are presently deploying hardware-based FDE. A further extrapolation shows six (6) percent of all desktops or laptops issued by respondents' organizations contain OPAL compliant hardware-based FDE or SEDs. These use statistics are consistent with an earlier study (see Footnote 2).
[4] Ibid. Footnote 2.

Tech cost for password resets

Here we look at the value of tech time associated with resetting passwords for both encrypted and unencrypted laptop or desktop computers. This analysis shows that it takes more tech time to perform a password reset for a full disk encrypted computer than a comparable unencrypted device. Similar to the previous analysis, we assume that the method of encryption (software versus hardware) has no impact on the productivity cost for password resets.

User idle cost for password resets

In this instance we compute the cost of end-user idle time waiting for the resetting of passwords for both encrypted and unencrypted laptop or desktop computers. Our analysis reveals it takes more time, and therefore a longer wait, to perform a password reset for a full disk encrypted computer. With respect to the idle time resulting from password resets, the method of encryption (software versus hardware) has no impact on end-user productivity.

Tech cost to encrypt after re-imaging

In this area we compute 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. Further, our TCO framework assumes software and hardware-based FDE require an identical level of effort (tech time) to re-image a hard disk. Hence, the different between software and hardware FDE is quite small.

User idle cost for initial encryption

This section 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 analysis of downtime associated with the initial encryption of the desktop or laptop's disk shows marked differences between software and hardware-based FDE. Clearly, software FDE is approximately three expensive than hardware FDE.

User excess operating cost

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 further analyze time differences for software and hardware-based FDE. This analysis of end-user productivity clearly shows marked differences between software and hardware FDE. Once again, we see software-based FDE as much more expensive than hardware-based FDE in terms of users' productivity in the normal use of their desktops or laptops in the workplace.

Tech cost for providing special administration to encrypted drives

Here we look to summarize our final TCO cost component for full disk encryption (both software and hardware combined). 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, the full disk encryption method (software vs. hardware) does not impact costs associates with special administrative tasks.

This table provides a recap of 11 total cost of ownership components, and a calculated difference between software and hardware-based FDE. Each panel shows cost estimates for one of four country samples on a per computer basis.

US Sample	Hardware FDE	Software FDE	Difference
Licensing cost	2.5	8.1	5.6
Annual maintenance	1.0	5.0	4.0
OPAL fee	7.9	-	(7.9)
Tech cost to pre-provision computer	1.3	1.3	-
Tech cost to stage computer	12.0	12.0	-
Tech cost to reset passwords	4.5	4.5	-
Value of idle time for password resets	22.2	22.2	-
Tech cost to re-encrypt after re-imaging	-	1.8	1.8
Value of idle time on initial encryption	-	30.0	30.0
Value of excess time operating computer	23.1	323.4	300.3
Tech cost of special administration	0.3	0.3	-
Total	$74.8	$408.6	$333.8

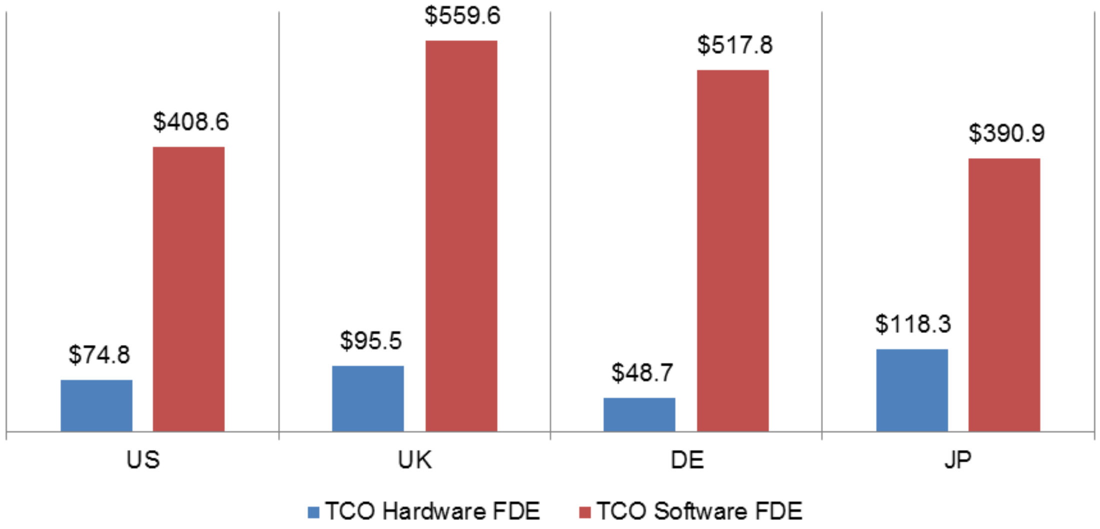
UK Sample	Hardware FDE	Software FDE	Difference
Licensing cost	2.3	9.8	7.5
Annual maintenance	1.0	5.0	4.0
SED Incremental cost	6.8	-	(6.8)
Tech cost to pre-provision computer	3.9	3.9	-
Tech cost to stage computer	18.5	18.5	-
Tech cost to reset passwords	3.8	3.8	-
Value of idle time for password resets	8.6	8.6	-
Tech cost to re-encrypt after re-imaging	-	1.7	1.7
Value of idle time on initial encryption	-	31.5	31.5
Value of excess time operating computer	50.1	476.3	426.2
Tech cost of special administration	0.5	0.5	-
Total	$95.5	$559.6	$464.1

German Sample	Hardware FDE	Software FDE	Difference
Licensing cost	2.5	10.1	7.6
Annual maintenance	1.1	4.8	3.7
SED Incremental cost	7.1	-	(7.1)
Tech cost to pre-provision computer	6.4	6.4	-
Tech cost to stage computer	16.7	16.7	-
Tech cost to reset passwords	3.8	3.8	-
Value of idle time for password resets	10.6	10.6	-
Tech cost to re-encrypt after re-imaging	-	1.7	1.7
Value of idle time on initial encryption	-	31.2	31.2
Value of excess time operating computer	-	432.0	432.0
Tech cost of special administration	0.5	0.5	-
Total	$48.7	$517.8	$469.1

Japanese Sample	Hardware FDE	Software FDE	Difference
Licensing cost	2.9	8.4	5.5
Annual maintenance	1.2	5.3	4.1
SED Incremental cost	7.7	-	(7.7)
Tech cost to pre-provision computer	3.5	3.5	-
Tech cost to stage computer	17.1	17.1	-
Tech cost to reset passwords	5.3	5.3	-
Value of idle time for password resets	32.1	32.1	-
Tech cost to re-encrypt after re-imaging	-	2.2	2.2
Value of idle time on initial encryption	-	27.6	27.6
Value of excess time operating computer	48.2	289.1	240.9
Tech cost of special administration	0.3	0.3	-
Total	$118.3	$390.9	$272.6

Figure 1 illustrates the marked differences between software and hardware-based full disk encryption in four countries. Taken together, these results provide strong evidence that hardware-based FDE solutions provide a substantially lower total cost of ownership than comparable software-based solutions.

Figure 1. TCO of software and hardware-based full disk encryption for four country samples



Part 3. 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

The reanalysis of TCO provided in this paper finds substantial cost differences between software-based and hardware-based full disk encryption methods. As illustrated in Figure 1, cost differences are significant in all four countries studied. The summary table reports Germany having the largest gap at ($454), while Japan has the smallest gap (at $261). The main source of differences between software and hardware FDE solutions concern IT tech time/labor, end-user productivity and licensing fees. As shown in our original study, irrespective of the method of full disk encryption deployed (software vs. hardware), its benefits outweigh TCO by a factor of 4 to 20 X (depending on the country sample).[5]

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.

[5] See The TCO for Full Disk Encryption: Studies in the US, UK, Germany & Japan. WinMagic and Ponemon Institute, July 2012.