Ponemon INSTITUTE

The Billion Dollar Lost Laptop Problem

Benchmark study of U.S. organizations

Sponsored by Intel

Independently conducted by Ponemon Institute LLC

Publication Date: 30 September 2010

The Billion Dollar Lost Laptop Problem

A Benchmark Study of U.S. Organizations

Ponemon Institute, September 30, 2010

Part 1. Executive Summary

What do you think your organization would do if it realized that each year it is losing millions of dollars because of the carelessness of employees and contractors entrusted with laptops? While organizations may be aware of the lost laptop problem, we do not believe they understand fully the adverse affect it may be having on their bottom line. If they did, we believe they would be more diligent in protecting these devices.

For this reason, Intel and Ponemon Institute decided to conduct *The Billion Dollar Lost Laptop Problem,* an independent benchmark study of 329 private and public sector organizations located in the United States. The purpose of the study is to determine the economic consequences to organizations when laptops used by employees and contractors are lost or stolen.

According to the findings, the number of lost or stolen laptops is huge. Participating organizations reported that in a 12 month period 86,455 laptops were lost or missing. The average number of lost laptops per organization was 263.

To calculate the total economic impact we referred to *The Cost of a Lost Laptop* benchmark study released in 2009 and also sponsored by Intel. In that study we were able to determine that the average value of one lost laptop is $49,246.[1]

The Cost of a Lost Laptop study conducted by Ponemon Institute and sponsored by Intel was the first benchmark study to estimate the full cost associated with a lost or stolen laptop. The benchmark analysis focuses on representative samples of organizations in the US that have experienced laptop loss or theft within the last 12 months. In total, 138 separate cases involving a lost laptop computer used by an employee, temporary employee or contractor.

It is important to point out that the smallest cost component is the replacement cost of the laptop. There are seven cost components used to arrive at the average value. These are: replacement costs, detection, forensics, data breach, lost intellectual property costs, lost productivity and legal, consulting and regulatory expenses. In the cases we studied in 2009, the occurrence of a data breach represents 80 percent of the cost of a lost laptop.

We then applied the $49,246 value to the 86,455 laptops reported lost by the 329 organizations in this study. We then calculated that the total cost is a staggering $2.1 billion or an average of $6.4 million per organization.

Using benchmarking methods, we examined organizations that ranged in size from less than 1,000 to greater then 75,000 employees and represented more than 12 industry sectors. The three largest sectors participating in the study include financial services, public sector and industrial.

Our benchmarks focused on the actual number of laptop computers lost or stolen over the past 12 months. We recruited a proprietary panel of organizations that shared confidential information. By design our instrument uses a fixed format template to ensure response objectivity and high accuracy. According to the organizations participating in this study, the total number of laptop computers assigned to employees and contractors on an annual basis is approximately 3.7 million. The average number of laptops for each organization is 11,174. Please note that our sample is skewed to larger-sized companies. Albeit a voluntary (judgmental) sample, we believe our results are representative of many organizations located in the United States.

[1] See *The Cost of a Lost Laptop*, Ponemon Institute, February 9, 2009

Following are the key variables collected by the researcher for all participating companies.

- Number of laptops to employees, temporary employees and contractors
- Number of laptops recorded as missing over the past year
- Number of laptops known to be stolen over the past year
- Number of laptops likely to be stolen over the past year
- Number of laptops missing (not believed to be stolen)
- Number of laptops recovered over the past year

In addition to frequency information on laptop loss, theft and recovery, we examined other normatively important variables:

- Average useful life of assigned laptops
- Source of the laptop loss (in-transit, remote use, workplace theft and so forth)
- Percentage of laptops with disc encryption
- Percentage of laptops with anti-theft device or software
- Percentage of laptops with backup (imagining) device or software
- Percentage of laptops containing sensitive or confidential information

The two primary dependent variables calculated for each company and used in our analysis involves ratio measures, defined as follows:[2]

- One-year loss ratio = $\Sigma^{n=329}$ {Total missing laptops} / {Total assigned laptops}
- Useful life loss ratio = $\Sigma^{n=329}$ {One year loss ratio} X {Average useful life of the lost laptop}

In addition to these loss ratios per company, we utilized the percentage theft rate as a covariate measure. This is defined as follows:

- Percentage theft rate = $\Sigma^{n=329}$ {Total laptops known to be stolen} / {Total missing laptops}

Finally, for tabled (chi-squared) analysis, is transformed the percentage theft rate into a theft index from ranging from 1 (low) to 4 (high) based on the quartile position of each company.

The following table summarizes several of our key statistics from this research:

Table 1: Key statistics from our sample	Sample average	Sample total
Sample of benchmarked companies		329
Number of assigned laptops	11,174	3,676,195
Recorded as missing over past year	263	86,455
Known theft	66	21,812
Likely theft	38	12,474
Missing	159	52,169
Recovered	12	3,936
Average useful life of laptops	3.1	
One-year loss ratio	2.32%	
Useful life loss ratio	7.12%	

[2] Our unit of analysis is the organizational unit or entity. Many of these are subsidiaries of larger parent entities. The sample of 329 participating organizations are part of 138 are companies.

Part 2. Key Findings: Understanding the billion dollar problem

The following are the key findings from the benchmark interviews and illustrate the experience of the 329 private and public sector organizations in the study. Pie Chart 1 summarizes the sample of participating organizations by organizational size (full-time equivalent headcount). Table 2 provides the percentage frequency distribution of participating organizations by industry sector.

Pie Chart 1: Distribution of participating companies by global headcount

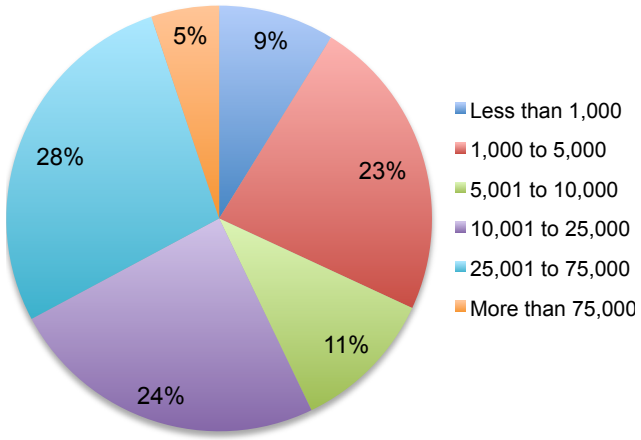
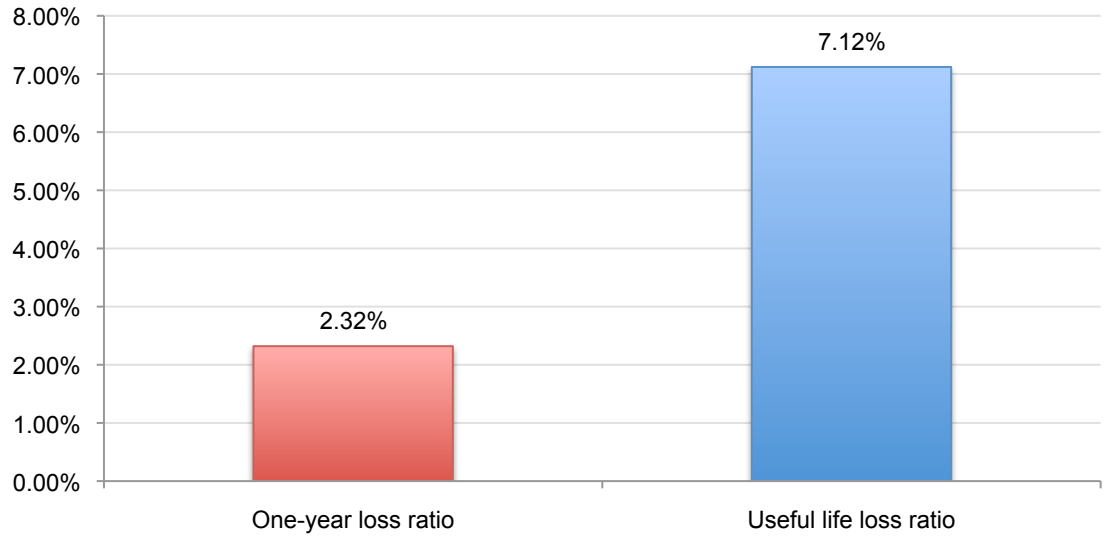


Table 2: Distribution of participating companies by industry classification

Industry	Pct%
Financial services	15%
Public sector	14%
Health & pharmaceutical	10%
Industrial	10%
Consumer	9%
Education & research	8%
Technology & software	8%
Retail	8%
Communications	7%
Services	7%
Transportation	3%
Other	1%
Total	100%

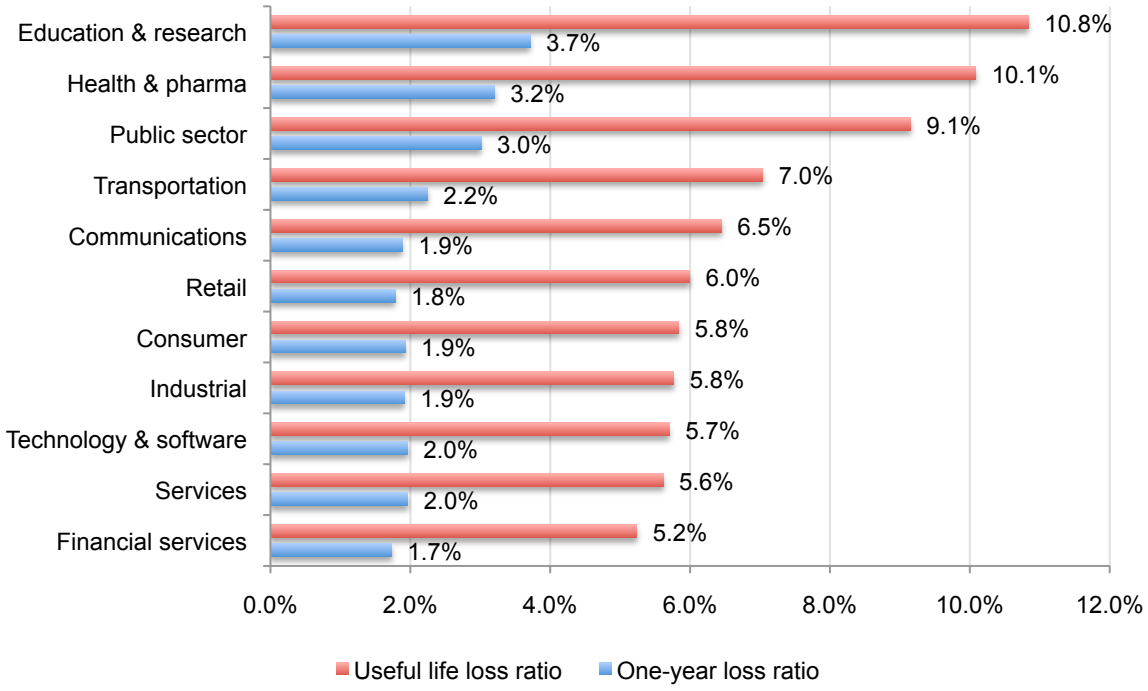
Bar Chart 1 reports the average one-year and useful life loss ratios for benchmarked companies. As shown, 2.3 percent of all laptops assigned to employees, temporary employees or contractors become missing each year. The average loss ratio over the laptop's useful life is 7.12 percent. Hence, more than seven percent of all assigned laptops in benchmarked companies will be lost or stolen sometime during their useful life.

Bar Chart 1: Average one-year and useful life loss ratios



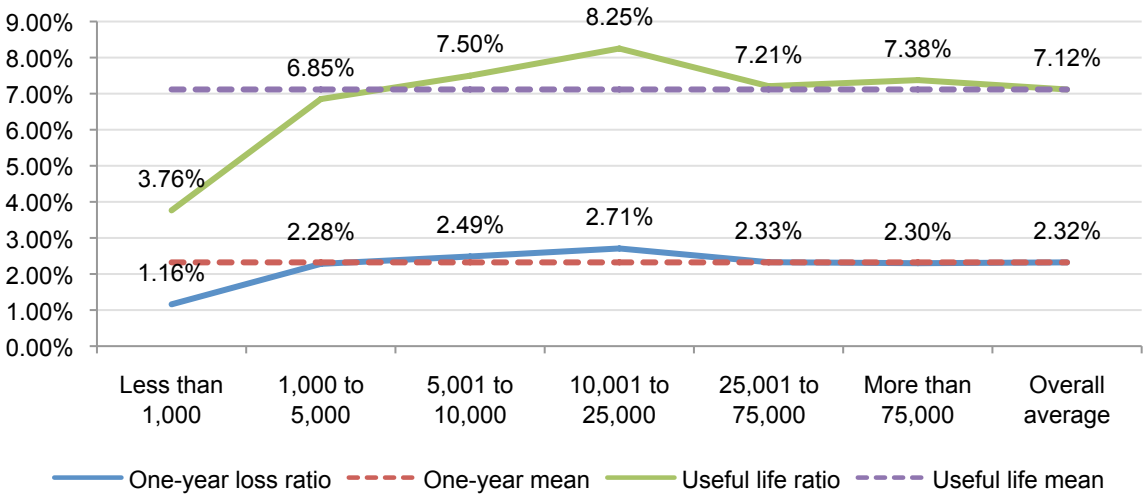
Do lost laptops vary by industry? Results show the rate of laptop loss is related to industry classification. Bar Chart 2 shows marked differences among various industry sectors. Clearly, educational institutions have the highest loss ratios, while financial service companies have the lowest loss ratios.

Bar Chart 2: Lost laptops by industry



Do lost laptops vary by organizational size? Results show the rate of laptop loss is related the size (headcount) of participating companies. Line Chart 1 shows organizations with less than 1,000 employees experience the lowest rate of laptop loss. Organizations with 10,001 to 25,000 employees appear to have the highest rate of laptop loss.

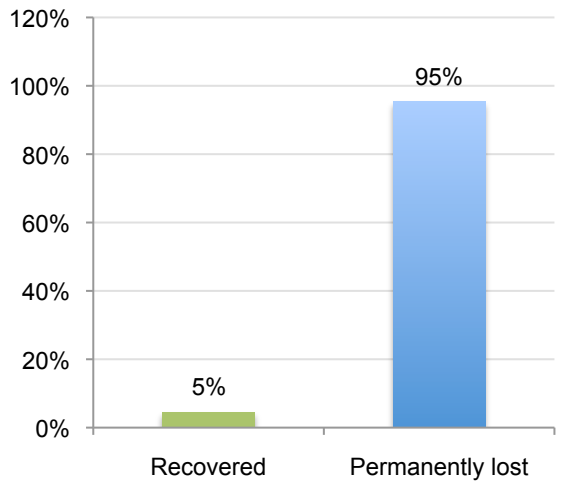
Line Chart 1: One-year and useful life loss ratios by organizational size (headcount).



Pie Chart 2 reports the percentage classification of lost or stolen laptop computers over the past 12 months.[3] For the overall sample, laptops known to be stolen was 21,812, which represents 25 percent of all missing laptops. Another 12,474 laptops, which represent 14 percent, are likely to have been stolen. Finally, 52,169 are classified as missing in action and this represents 60 percent of all missing laptops. The number of recovered laptops is 3,948. As shown in Bar Chart 3, this represents only five percent of all missing laptops over the past 12 months.

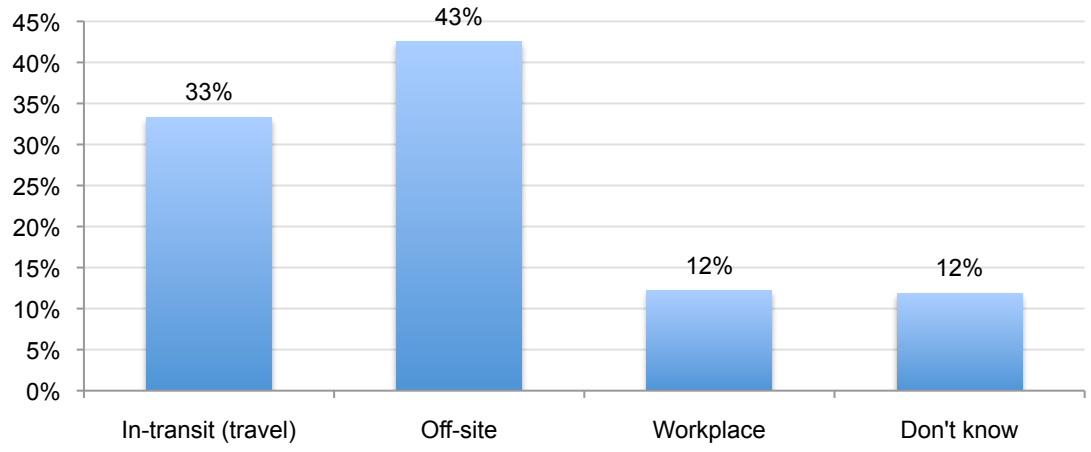
Pie Chart 2: Classification of lost or stolen laptops for the benchmark sample

Bar Chart 3: Percentage recovery rate among lost or stolen laptops for the benchmark sample



Where are laptops lost? Thirty-three percent say laptops are lost in transit or travel, 43 percent say the are lost off-site (for example, working from a home office or hotel room) 12 percent are lost in the workplace and 12 percent could not be determined where the loss actually occurred.

Bar Chart 4: Where laptops are lost



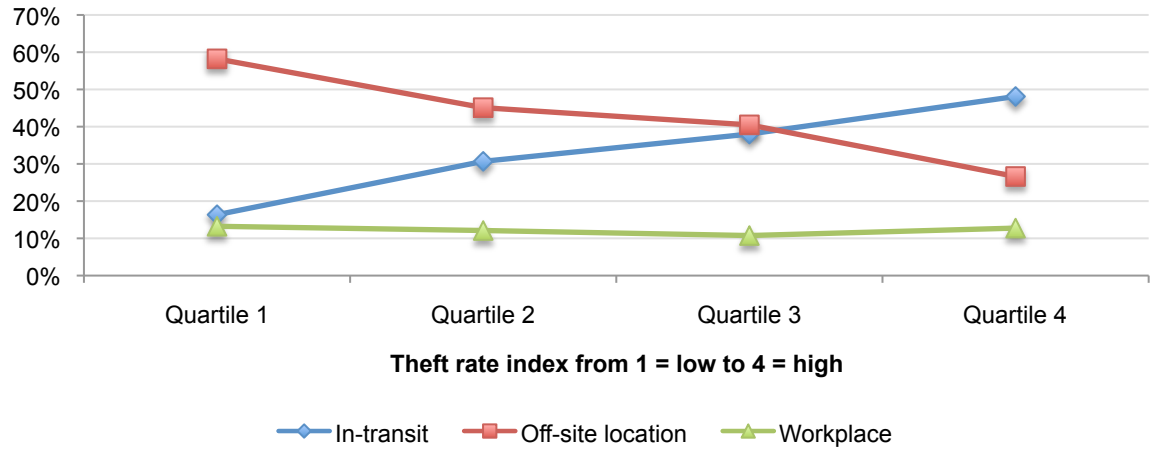
[3] Working in collaboration with the organization's security or IT personnel, the researchers evaluated the proper classification of known theft. While this determination is based on objective factors such as police reports there is a possibility that the true theft rate is lower because of over-reporting by employees.

What is the greatest cause of laptop theft? As mentioned above, the theft rate was converted into an index and placed into one of four quartiles where 1 = lowest theft rate to 4 = highest theft rate. Table 3 records the percentage of laptop theft cases according to one of three venues. Line Chart 2 provides a graph of these percentages according to the theft index (quartile).

As can be seen, traveling laptops seem to be most vulnerable to theft. Organizations that report the largest number of stolen laptops have the highest percentage of laptops in transit. Conversely, the lowest theft rates appear to occur in the workplace. The pattern shown in the chart suggests theft rates are correlated with high rates of in-transit employees, and inversely correlated with high rates of employees working from off-site locations such as a home office.

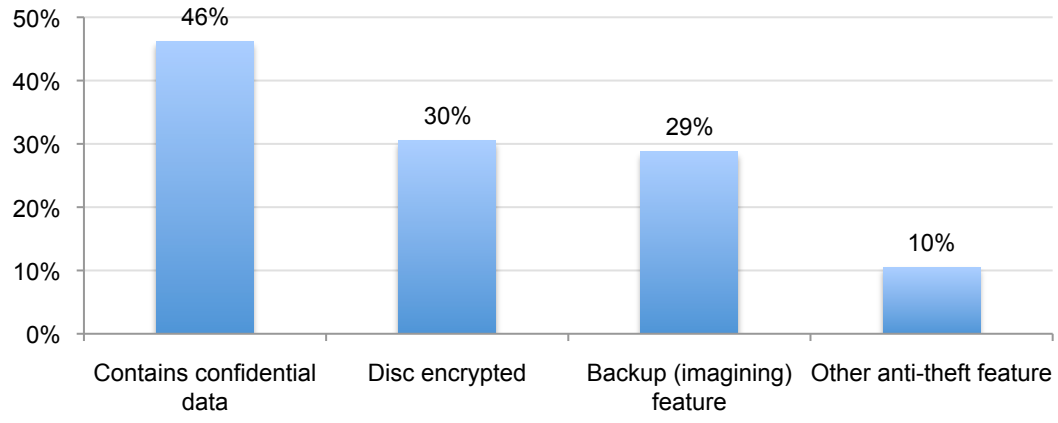
Table 3: Theft index	Quartile 1	Quartile 2	Quartile 3	Quartile 4
In-transit	16%	31%	38%	48%
Off-site location	58%	45%	40%	27%
Workplace	13%	12%	11%	13%

Line Chart 2: Three venues of laptop theft and theft index quartile



What protections or safeguards do these lost laptops have? Bar Chart 5 shows 30 percent of laptops lost had disc encryption, 10 percent say they had some other anti-theft feature, and 29 percent say the laptops lost had backup imaging feature. Forty-six percent say the lost laptops contained sensitive or confidential data.

Bar Chart 5: Percentage safeguards in-place the rate containing confidential data

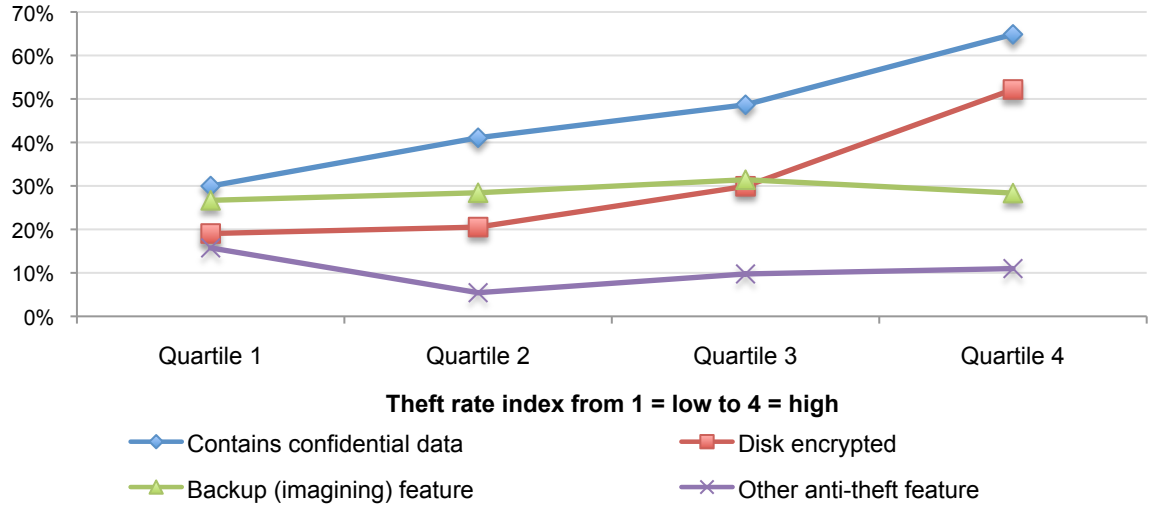


What laptops are most likely to have disc encryption? Laptops with the most sensitive and confidential data are the most likely to be stolen. However, these laptops also are more likely to have disc encryption.

Using the theft index as mentioned above, we calculated the percentage of laptop safeguards into one of four quartiles where 1 = lowest theft rate to 4 = highest theft rate. Table 4 records the percentage of laptop theft cases according to safeguards and confidential data at risk. Line Chart 3 provides a graph of these percentages according to the theft index (quartile).

Table 4: Theft index	Quartile 1	Quartile 2	Quartile 3	Quartile 4
Contains confidential data	30%	41%	49%	65%
Whole disk encrypted	19%	21%	30%	52%
Backup (imagining) feature	27%	28%	31%	28%
Other anti-theft feature	16%	5%	10%	11%

Line Chart 3: Confidential data at risk and security safeguards in-place



As can be seen, both confidential data at risk and the rate of disc encryption is correlated with theft rate. Thus, our results suggest companies experiencing a higher theft rate are more likely to use disc encryption as a safeguard. In addition, companies choosing disc encryption are likely to have employees who routinely carry sensitive or confidential data on their laptop computers.

Part 3: Calculus for economic impact

Table 5 provides the variables used to extrapolate the total economic impact of the lost or stolen laptop computers benchmarked in this study of 329 organizations. The average costs used to determine the economic impact is derived from our earlier research. The analysis divides the sample of missing laptops into three trenches: total encrypted laptops, total non-encrypted laptops and the total of laptops not carrying confidential data.

As shown below, the total economic value or cost to the 329 benchmarked organizations is approximately $2.1 billion. The average economic value or cost for each benchmarked organization is nearly $6.4 million.

Table 5: Calculation of economic impact	Amount
Total lost laptops	86,455
Total lost laptops not encrypted	60,518
Not encrypted carrying confidential data	27,838
Average cost of lost laptops not encrypted*	$56,165.00
Economic value for benchmark sample	$1,563,521,270
Total encrypted lost laptops	25,937
Encrypted carrying confidential data	11,931
Average cost of encrypted lost laptops*	$37,443
Economic value for benchmark sample	$446,732,433
Total laptops not carrying confidential data	46,686
Average cost of laptops without confidential data*	$4,078
Economic value for benchmark sample	190,385,508
Total economic value for benchmark sample	$2,200,639,211
Average cost per lost laptop	$25,454.16
Minus value of recovered laptops	$100,187,565
Adjusted total value for benchmark sample	$2,100,451,646
Average value per benchmarked organization	$6,384,352

*Value obtained from previous research on the average cost of a lost or stolen laptop computer (see footnote 1).

Part 4: Caveats

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- Non-statistical results: The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations – all U.S.-based entities experiencing laptop losses over the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.

- Non-response: The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a reference group of organizations, all believed to have experienced laptop losses over the past 12 months. A total of 329 companies provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the loss containment and recovery process, as well as the underlying costs involved.
- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward larger-sized companies with more mature information security programs.
- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- Unmeasured factors: To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- Estimated cost results. The quality of survey research is based on the integrity of confidential responses received from companies. While certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.

Part 5. Implications for organizations

We believe this study is important because it reveals the significant cost to organizations as a result of lost or missing laptops. Based on previous Ponemon Institute research completed in May 2009, the total economic impact of one lost laptop is $49,256. If we apply the figures from this earlier research to the present sample, this would be a combined cost of $2.1 billion for the 329 organizations participating in our study. This yields $6.4 million per organization, on average.

In addition to convincing employees and contractors of the importance of keeping a careful watch over their laptops, it is also important to protect the sensitive data contained on the computer. Not surprisingly, lost or stolen laptops are costly to organizations. But it is not the replacement cost that should have companies concerned. Rather it is the data and the risk of a data breach that can have serious financial implications for companies. The cost of a data breach, as we determined in the 2009 study, represents 80 percent of the total cost of a lost laptop compared to two percent for replacing the computer. We also found that encryption on average can reduce the cost of a lost laptop by more than $20,000.

We also recommend training and awareness programs for all employees who have laptops. Only 12 percent are lost in the workplace. Thus, special attention should be paid to instructing employees who take their laptops off-site such as when traveling or working from home.

Another important recommendation is to have policies that require employees to report a lost or stolen laptop as soon as possible. In addition, anti-theft and data protection solutions are available to secure laptops and the sensitive and confidential information they contain. Based on the costly consequences of lost laptops, the business case can be made for allocating the necessary resources to stop the loss and protect the data.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49629 USA
1.800.887.3118
research@ponemon.org

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.