THE TRUE COST OF COMPLIANCE

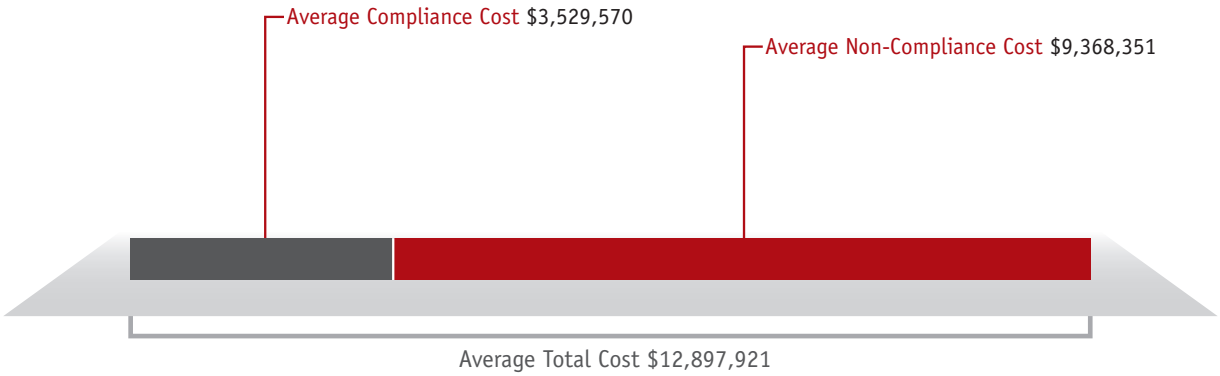
A Benchmark Study of Multinational Organizations

Research Report

Independently Conducted by Ponemon Institute LLC

January 2011

Ponemon INSTITUTE



I
EXECUTIVE SUMMARY

Multinational organizations in all industries must comply with privacy and data protection laws, regulations and policies designed to protect individuals' sensitive and confidential information. Compliance requires organizations to adopt and implement a variety of costly activities related to process, people and technologies. These activities include ensuring that they have professional staff dedicated to compliance as well as enabling technologies to curtail risk. They also require organizations to allocate funds to pay legal and non-legal penalties for non-compliance.

The Ponemon Institute and Tripwire, Inc. conducted this study to determine the full economic impact of compliance activities for a representative sample of 46 multinational organizations. This benchmark study is the first to use empirical data to estimate the full cost of an organization's compliance efforts, including the cost of non-compliance with laws, regulations and policies. To be as accurate as possible in this estimate, 160 functional leaders were interviewed in these organizations.

We learned that while the average cost of compliance for the organizations in our study is $3.5 million, the cost of non-compliance is much greater. The average cost for organizations that experience non-compliance related problems is nearly $9.4 million. Thus, investing in the compliance activities described in this study can help avoid non-compliance problems such as business disruption, reduced productivity, fees, penalties and other legal and non-legal settlement costs.

The findings also suggest that organizations view meeting legal and regulatory requirements as more important than meeting compliance with internal policies and procedures. In terms of external compliance, respondents indicated that the most important and difficult requirements to comply with are those of the PCI DSS, various state privacy and data protection laws, the European Union Privacy Directive, and Sarbanes-Oxley.

THE COST OF NON-COMPLIANCE CAN BE MORE EXPENSIVE THAN INVESTING IN COMPLIANCE ACTIVITIES

The extrapolated average cost of compliance for 46 organizations in our study is more than $3.5 million, with a range of $446,000 to over $16 million. Adjusting total cost by organizational headcount (size) yields a per capita compliance cost of $222 per employee.

The extrapolated average cost of non-compliance for 46 organizations is nearly $9.4 million, with a range of $1.4 million to nearly $28 million. Adjusting total cost by organizational headcount (size) yields a per capita non-compliance cost of $820 per employee.

Data protection and enforcement activities are the most costly compliance activities. In terms of the direct expense categories, data protection technologies and incident management top the list. The lowest compliance cost activities concern policy development and communications. In terms of direct expense categories, staff certification and redress are the lowest.

Business disruption and productivity losses are the most expensive consequences of non-compliance. The least expensive consequences are fines, penalties and other settlement costs.

On average, non-compliance cost is 2.65 times the cost of compliance for the 46 organizations. With the exception of two cases, non-compliance cost exceeded compliance cost.

All organizations in the study experienced both compliance and non-compliance costs. However the study strongly suggests that organizations that invest more in compliance enjoy lower non-compliance costs by avoiding many of the negative consequences of non-compliance. However, given that non-compliance costs cannot be avoided entirely, there is obviously some point after which further investment in compliance fails to yield a reduction in non-compliance costs.

INDUSTRY AND ORGANIZATIONAL SIZE AFFECT THE COST OF COMPLIANCE AND NON-COMPLIANCE

Results show that the total cost of compliance varies significantly by the organization's industry segment, with a range of $6.8 million for education and research to more than $24 million for energy. The difference between compliance and non-compliance cost also varies by industry. Energy shows the smallest difference at $2 million, and technology shows the largest difference at $9.4 million.

When adjusting compliance and non-compliance costs by each organization's headcount, we see smaller-sized companies (5,000 or fewer employees) as incurring substantially higher per capita compliance costs than larger-sized companies (more than 5,000 employees).

While the study found that the cost of compliance is affected by organizational size, it is also affected by the number of regulations and the amount of sensitive or confidential information an organization is required to safeguard.

THE GAP BETWEEN COMPLIANCE AND NON-COMPLIANCE COST IS RELATED TO NUMBER OF RECORDS LOST OR STOLEN IN DATA BREACHES

We tested the premise that increasing the amount of compliance spending offsets the cost of non-compliance. Our findings show a positive correlation between the percentage difference between compliance and non-compliance costs and the number of lost or stolen records during a 12-month period. In other words, the smaller the gap between compliance and non-compliance costs, the fewer compromised records.

The size of the gap can be explained in a couple of ways. First, when a data breach occurs, non-compliance costs will rise. However, it is important to note that when an organization spends less on compliance costs, this also increases the size of the gap.

Almost all of the organizations in the study experienced a data breach, with the resulting number of records compromised varying widely. For compliance spending to result in strong data protection and minimize data breaches, organizations must invest in compliance wisely. As we show in the discussion of the next finding, compliance investments that improve security effectiveness rather than simply meeting audit requirements can result in more effective data protection.

THE MORE EFFECTIVE AN ORGANIZATION'S SECURITY STRATEGY IS, THE LOWER THE COST OF NON-COMPLIANCE

We used a well-known indexing method called the security effectiveness score (SES)[1] to assess an organization's security posture. The methodology, which has been developed over the last five years and used in numerous Ponemon Institute studies, measures each organization's security posture against 25 security best practices.

We determined that the SES is unrelated to compliance cost. However, the SES appears to be inversely related to non-compliance cost. In other words, an organization with a higher SES, or a better security posture, will experience lower non-compliance costs. These findings suggest that improving security does indeed lower the costs of non-compliance.

A related finding showed that per capita non-compliance cost is inversely related to the percentage of compliance spending in relation to the total IT budget. In other words, the more an organization spent on the consequences of non-compliance, the smaller the amount of the IT budget the organization had allocated to compliance costs. ***Clearly, when an organization spends a higher percentage of the IT budget on compliance, it reduces the negative consequences and cost of non-compliance.***

ONGOING INTERNAL COMPLIANCE AUDITS REDUCE THE TOTAL COST OF COMPLIANCE

Per capita non-compliance cost—the non-compliance cost adjusted for organization size as determined by headcount—appears to be inversely related to the frequency of internal compliance audits. That is, the more internal audits an organization conducts, the lower its non-compliance cost. In comparison, organizations that do not conduct internal compliance audits experience the highest compliance cost when adjusted for size.

The study indicates that those organizations that conduct more internal audits can more effectively manage their compliance burden. This in turn could reduce the costs of non-compliance. In addition, organizations that embrace a culture of compliance most likely are also more security and privacy conscious.

LAWS AND REGULATIONS ARE THE MAIN DRIVERS FOR INVESTMENT IN COMPLIANCE ACTIVITIES

Finally, results suggest that compliance with laws and regulations (external focus) appears to be the most important mission of compliance efforts. Regulations that are a priority include the Payment Card Industry Data Security Standard (PCI DSS), various state privacy and data protection laws (such as MA 201 in Massachusetts), the European Union Privacy Directive, and Sarbanes-Oxley. Organizations are investing in specialized technologies to protect their data, such as file integrity monitoring, security information and event management, access management, data loss prevention, and encryption.

In particular, the greatest number of organizations in the study identified PCI DSS as the most important and most difficult regulation with which to comply. This finding may be due partially to two facts: Almost every organization has some component of cardholder data in their organization, and PCI DSS requirements are among the most prescriptive.

[1] The Ponemon Institute initially developed the Security Effectiveness Score (SES) in its 2005 Encryption Trends Study. The purpose of the SES is to define the security posture of responding organizations. The SES is derived from the rating of 25 leading information security and data protection practices. This indexing method has been validated by more than 30 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). An index value above zero is net favorable.

II
KEY FINDINGS

The key findings presented below are based on the benchmark analysis of 46 organizations. We obtained information about each organization's total compliance cost utilizing an activity-based costing method and a proprietary diagnostic interviewing technique involving 160 functional leaders. Our research methods captured information about direct and indirect costs associated with compliance activities during a 12-month period. We define a compliance activity as one that organizations use to meet the specific rules, regulations, policies and contracts that are intended to protect information assets.

Our benchmarking efforts also captured the direct, indirect and opportunity costs associated with non-compliance events during a 12-month period. We define non-compliance cost as the cost that results when an organization fails to comply with rules, regulations, policies, contacts, and other legal obligations. Part IV of this report discusses our benchmarking methods in greater detail.

In the course of interviewing functional leaders we determined key trends and commonalities about total compliance cost. For many organizations, compliance has a very broad scope that includes global privacy, financial data integrity, data loss notification, credit cardholder protection, and other regulatory mandates. It also includes self-regulatory standards, including ISO, NIST and others.

In the course of our research, we learned that many organizations face multiple and sometimes competing compliance mandates. These mandates require constant monitoring and frequent audits. As a result, compliance can be a significant cost burden that includes the need for dedicated professional staff, enabling technologies to curtail risk and allocation of funds to pay legal and non-legal penalties for non-compliance.

Figure 1: Average Compliance and Non-Compliance Costs

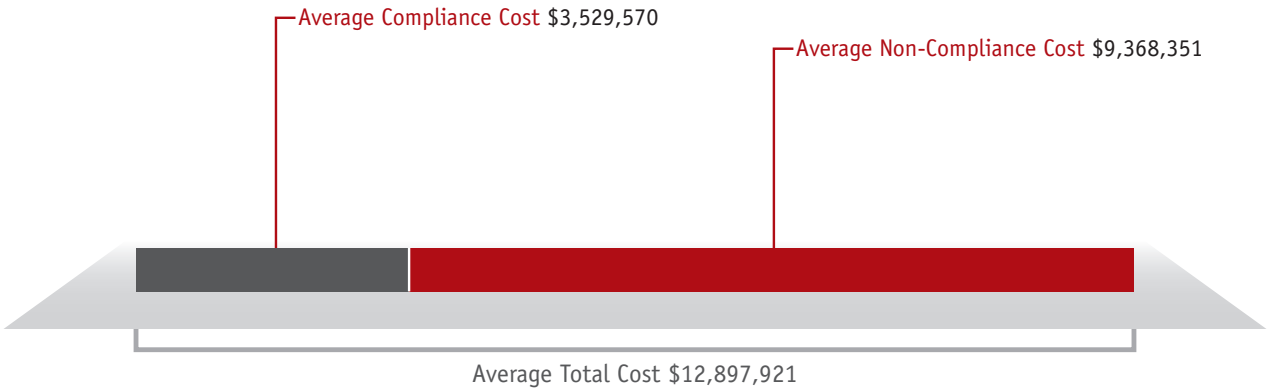


Figure 1 shows the average extrapolated cost of compliance and non-compliance based on the cost framework described in Part 3. According to the figure, non-compliance costs are 2.65 times higher than compliance costs, with a difference of nearly $6 million.

Although all organizations that participated in this study experienced both compliance and non-compliance costs, the findings demonstrate the value of investing in activities that may help an organization reduce the reactive costs of non-compliance. These activities could include conducting internal audits, implementing enabling technologies, investing in compliance training and expert staffing and others. It is likely that an organization could recoup its expenditures on these activities and possibly more as a result of reduced non-compliance costs.

Figure 2: Percentage Cost Structure for Compliance Costs

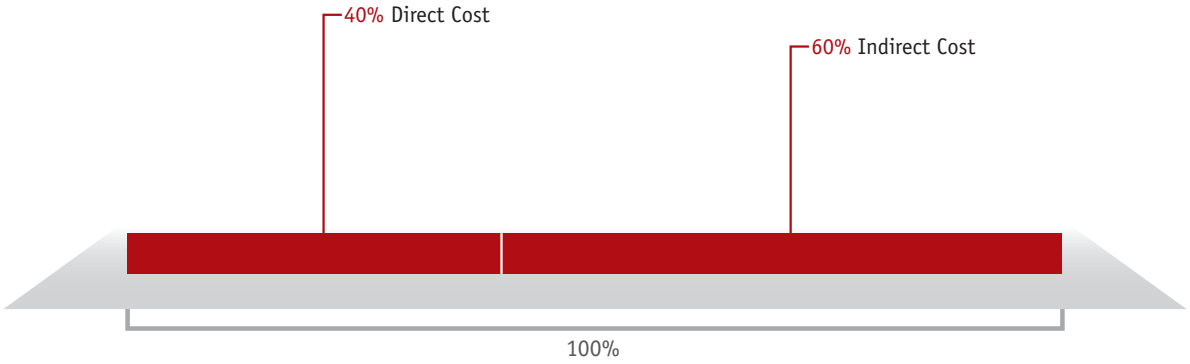


Figure 2 reports the cost structure on a percentage basis for all data compliance cost activities combined. The figure shows that indirect costs such as administrative overhead account for 60 percent of compliance cost activities. Direct costs such as payments to consultants, auditors or other outside experts account for 40 percent.

Table 1: Key statistics on the cost of compliance for six activity centers (USD)

Activity centers	Total	Average	Median	Maximum	Minimum
Policy	13,703,854	297,910	148,675	1,686,805	13,796
Communications	15,783,469	343,119	166,363	2,009,736	13,732
Program management	20,325,527	441,859	246,576	2,168,351	48,628
Data security*	47,570,815	1,034,148	793,352	3,753,816	135,685
Compliance monitoring	29,280,953	636,542	326,181	3,186,971	32,872
Enforcement	35,695,589	775,991	266,753	4,488,671	31,731
Total	**162,360,207**	**3,529,570**	**2,023,111**	**16,049,151**	**445,697**

*Sixty-four percent of this center pertains to the direct and indirect costs associated with enabling security technologies.

Table 1 summarizes the total, average, median, maximum and minimum compliance costs for a 12-month period for the six activity centers defined in our cost framework in Part IV. These activity centers include people, processes and technology. Data security represents the largest cost center for the benchmark sample, while policy represents the smallest.

The following two figures show the average compliance cost activities for 46 organizations. As shown in Figure 3, compliance costs relating to data protection technologies and incident management represent the two largest expenditure categories.

Figure 3: Compliance Costs by Expense Categories

Figure 4: Compliance Costs by Functional Areas

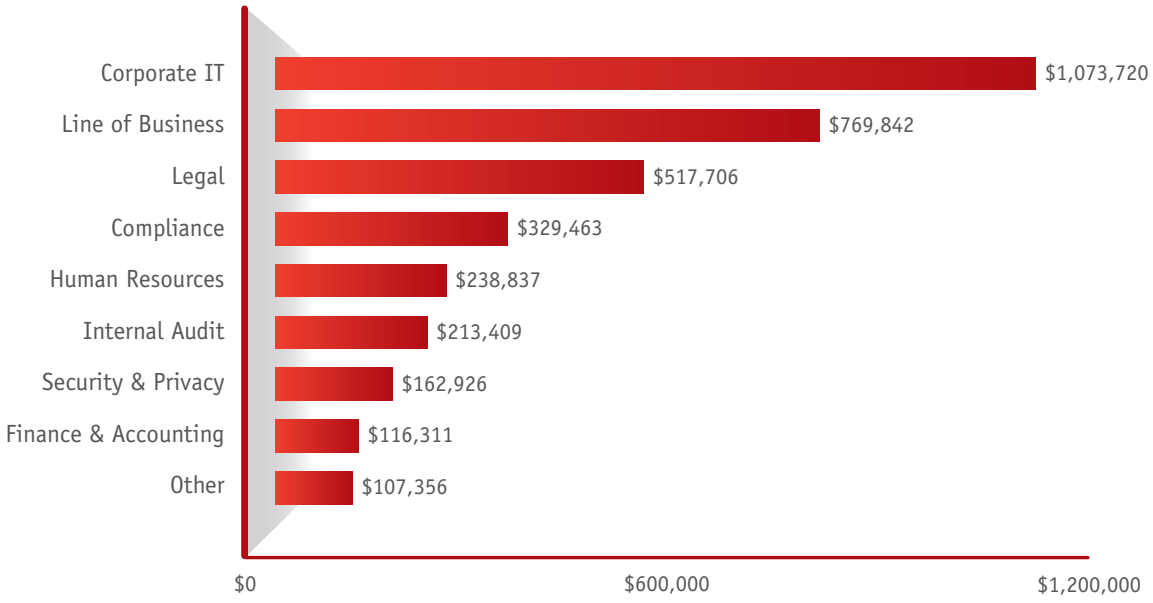


Figure 4 shows IT lines of business and legal as the functional areas most likely to control data compliance expenditures.

Figure 5: Percentage Cost Structure for Non-Compliance Costs

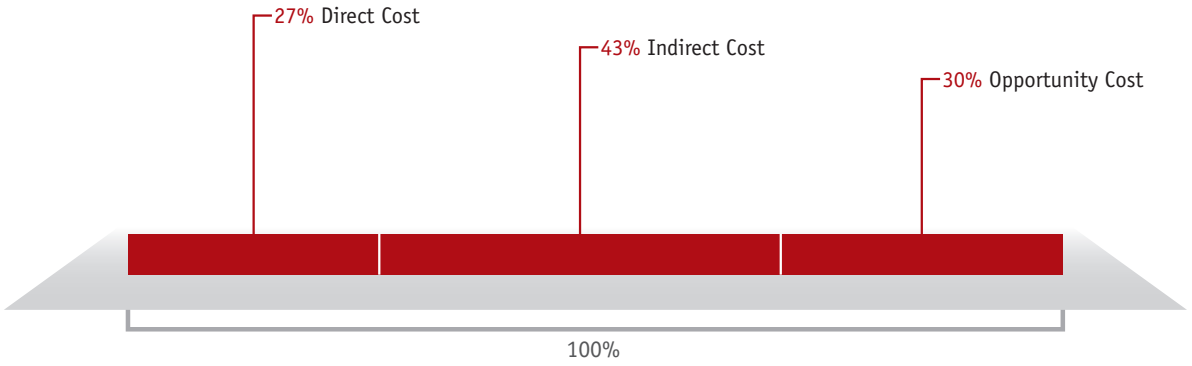


Figure 5 breaks down non-compliance costs on a percentage basis of total non-compliance cost. As shown, indirect costs such as data center downtime or diminished employee productivity accounts for 43 percent of non-compliance cost. Indirect costs are resources used, like administrative overhead, but not paid for as a direct cash outlay for a specific activity. Opportunity costs represent 30 percent. These costs are lost business opportunities that result from compliance infractions, and they often diminish the organization's reputation. An example of an opportunity cost is an organization's inability to execute a marketing campaign due to consumer privacy concerns. Direct costs such as revenue loss or customer churn represent 27 percent of non-compliance costs. Direct costs are expenses associated directly with a specific activity.

Table 2: Cost of non-compliance for four consequences

Cost consequences	Total	Average	Median	Maximum	Minimum
Business disruption	151,691,110	3,297,633	2,432,126	16,552,877	-
Productivity loss	112,138,567	2,437,795	2,324,717	6,446,758	-
Revenue loss	100,324,880	2,180,976	1,983,464	6,538,555	154,675
Fines, penalties & other	66,789,568	1,451,947	1,075,627	7,493,699	80,384
Total	**430,944,126**	**9,368,351**	**9,336,084**	**27,974,860**	**1,386,758**

Table 2 summarizes the total, average, median, maximum and minimum non-compliance cost for each one of four consequences defined in our framework for a 12-month period. Business disruption represents the most costly consequence, while fines, penalties and other settlement costs represent the least costly consequences of compliance failure. Non-compliance costs impact the business because they often require employees to deal with non-compliance issues rather than performing their regular duties.

Figure 6: Compliance and Non-Compliance Costs

Ascending order by total compliance cost

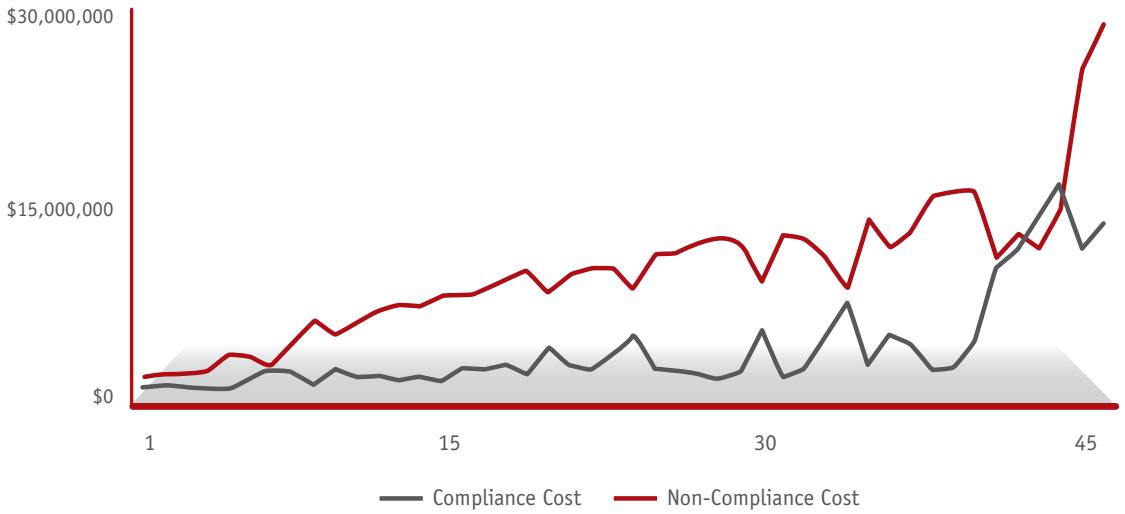


Figure 6 shows compliance and non-compliance costs for 46 organizations. These observations are presented in ascending order of the total compliance cost (with a range of $2 million to over $40 million per annum). The figure shows that in all but two cases, non-compliance costs exceed compliance costs.

It is our belief that the gap between compliance and non-compliance provides evidence that organizations do not spend enough resources on core compliance activities. In other words, if companies spent more on compliance in areas such as audits, enabling technologies, training, expert staffing and more, they would recoup those expenditures and possibly more through a reduction in non-compliance cost.

Figure 7: Compromised Sensitive or Confidential Records Lost or Stolen Over 12 Months

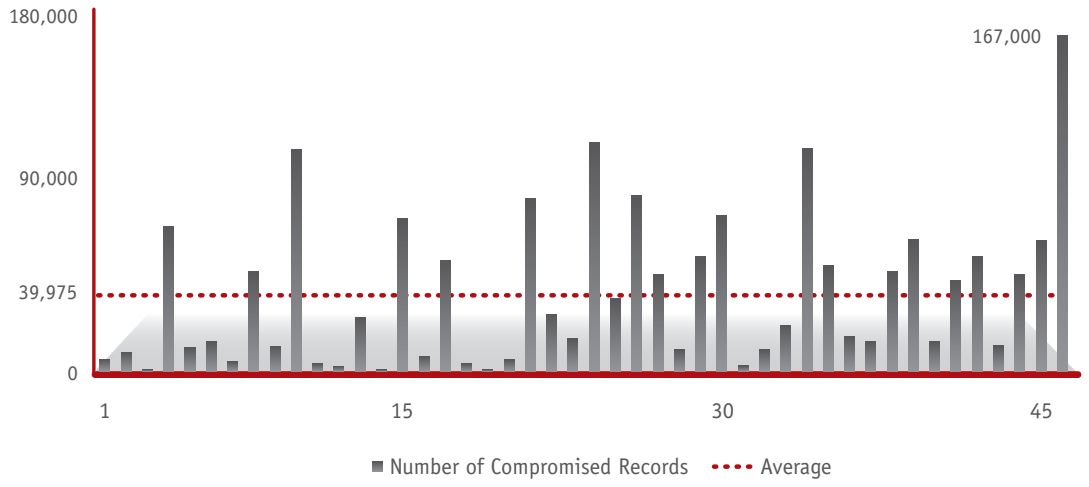


Figure 7 reports the approximate number of compromised sensitive or confidential records over the past 12 months as experienced by 46 organizations. Note that almost all organizations experienced some size of data breach. The number of lost or stolen records varies widely, ranging from a low of zero to a high of 167,000, and having an average of nearly 40,000.

Figure 8: Compromised Records in Ascending Order by the Percentage

Ascending order by the percentage gap between compliance and non-compliance cost

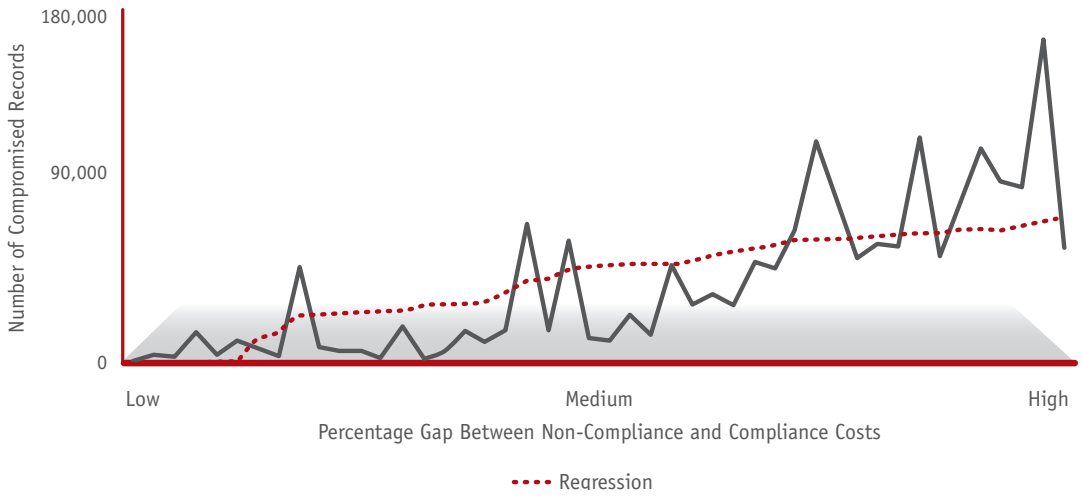


Figure 8 shows the number of compromised records as shown in Figure 7, but re-orders them from left to right by the smallest to largest percentage gap between compliance and non-compliance costs. In other words, on the left side of the figure, we have the number of records for organizations that had a smaller gap between the two costs. On the right, we have the number of records for organizations with the largest gap between the two costs. As you move from left to right, the upward sloping regression line shows that as the gap between the costs increases, so does the number of compromised records.

As a result of these findings, we hypothesize that the wider the gap between non-compliance and compliance cost, the greater the data loss. The slope of the regression line supports this hypothesis, and suggests that organizational data loss is related to the relative size of the gap between compliance and non-compliance cost.

It is important to note that both paying non-compliance costs and not spending on compliance impact the size of the gap.

Figure 9: Total Compliance Cost by Industry in Millions of USD

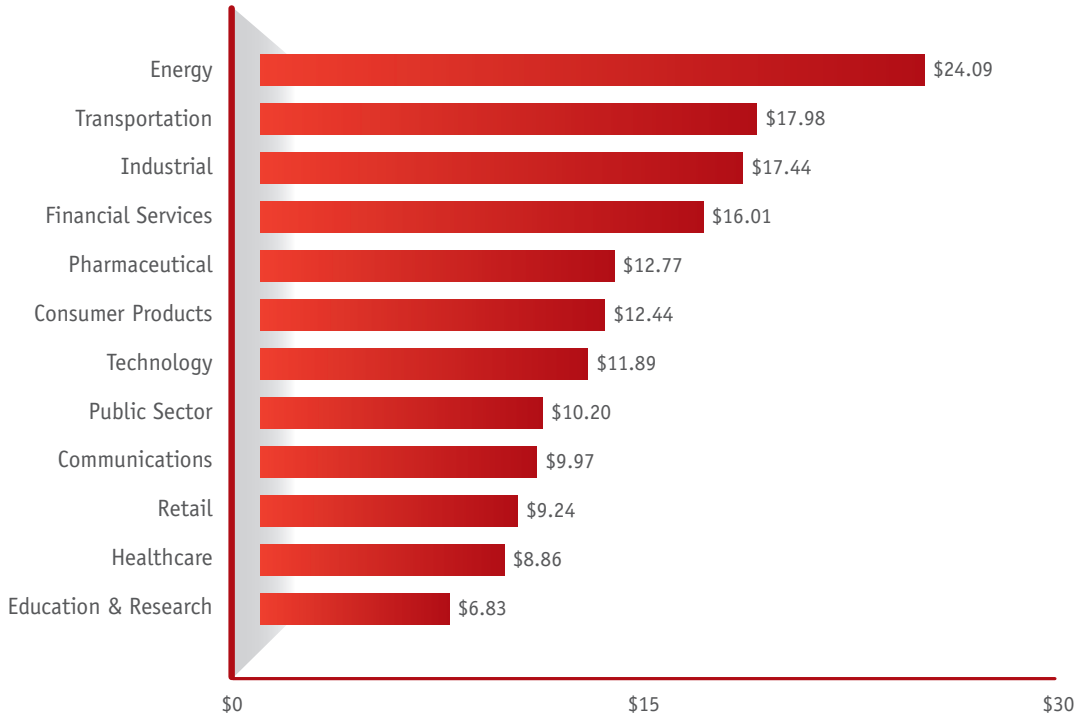


Figure 9 provides the total compliance cost for 12 industry segments included in our benchmark sample. The analysis by industry is limited because of a small sample size; however, it is interesting to see wide variation across segments ranging from a high of more than $24 million (energy) to a low of $6.8 million (education and research).

Figure 10: Percentage Gap Between Non-Compliance and Compliance Cost by Industry

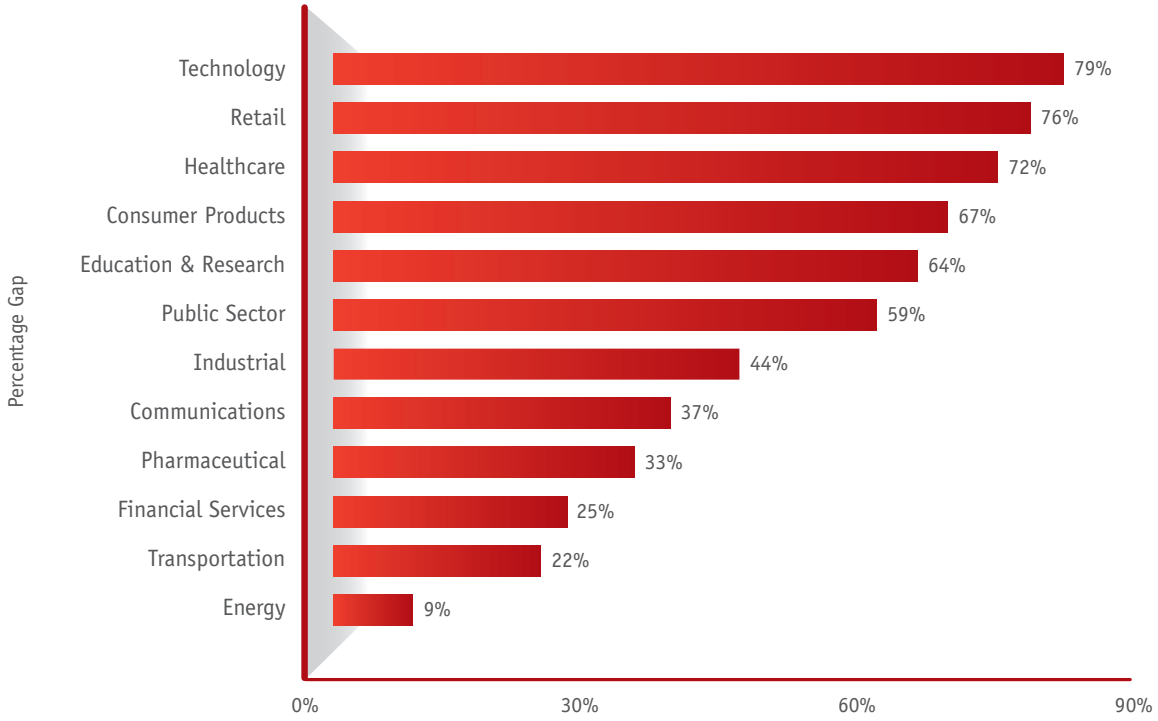


Figure 10 reports the percentage gap between compliance and non-compliance costs by industry. In contrast to the above analysis, energy also has the smallest percentage gap at nine percent and the technology segment has the largest gap at 79 percent.

Figure 11: Average Number of Compromised Records by Industry

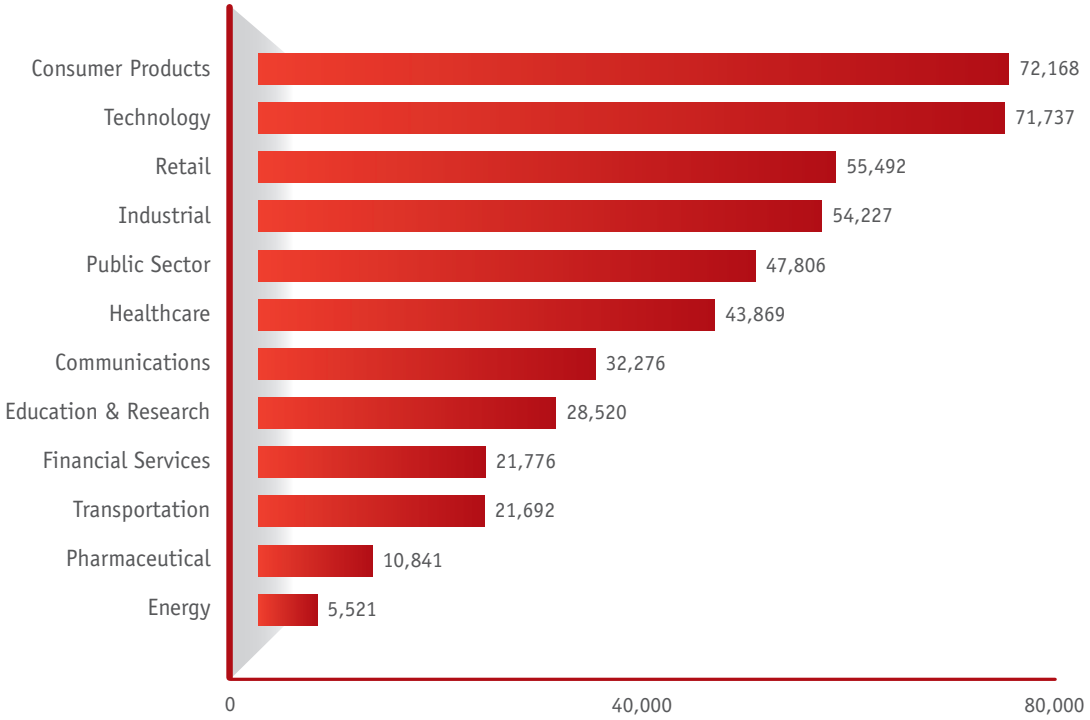


Figure 11 reports the average number of compromised records over a 12-month period by industry classification. Though not a perfect match, there appears to be a close relationship between the average number of lost or stolen records and the percentage gap by industry shown in Figure 10.

Figure 12: Compliance Cost and Non-Compliance Cost by Headcount in Millions of USD

Figure 12 reports the average compliance and non-compliance costs by the approximate global headcount (size) of benchmark companies. Not surprisingly, compliance and non-compliance costs increase according to the organization's size.

Figure 13: Per Capita Compliance Cost and Non-Compliance Cost by Headcount in USD

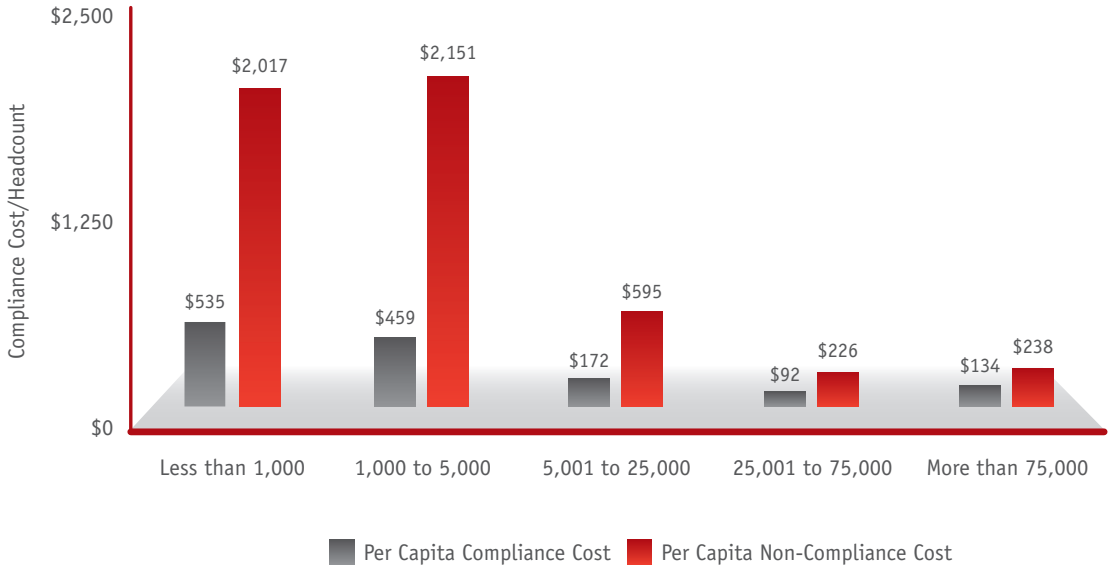


Figure 13 provides an analysis of compliance and non-compliance cost on a per capita basis. This figure shows an economy of scale. Specifically, when adjusted by headcount (size), both compliance and non-compliance costs are highest for organizations with fewer than 5,000 employees and smallest for organizations with 25,000 to 75,000 employees. This result may be partially explained by the fact that organizations hold or have access to vast amounts of sensitive or confidential information irrespective of size. In addition, the per capita difference is much more significant for non-compliance than compliance cost, wherein per capita non-compliance cost is about ten times higher for organizations with fewer than 5,000 employees versus organizations with more than 25,000 employees.

Figure 14: Benchmark Sample in Ascending Order by Security Effectiveness Score

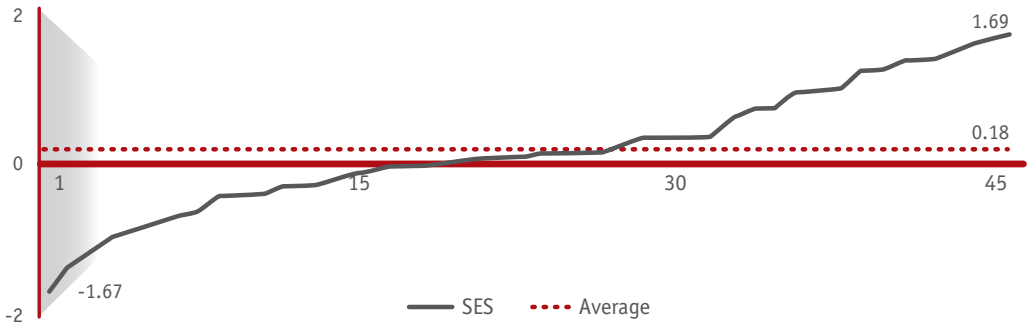


Figure 14. In this benchmark study, we utilized an indexing methodology known as the Security Effectiveness Score (SES) to measure an organization's ability to meet reasonable security objectives. Recent research shows that the higher the SES index, the more effective the organization is in protecting information assets and critical infrastructure.

As with prior Ponemon Institute research, we measured the security posture of participating organizations as part of the benchmarking process for this study. Figure 15 reports each benchmark company's SES in ascending order of security effectiveness. The SES range of possible scores is -2 (minimum score) to +2 (maximum score). Index results for the present benchmark sample vary from a low of -1.67 to a high of +1.69, with a mean value of 0.18.

Figure 15: Security Effectiveness Score for 12 Industry Segments

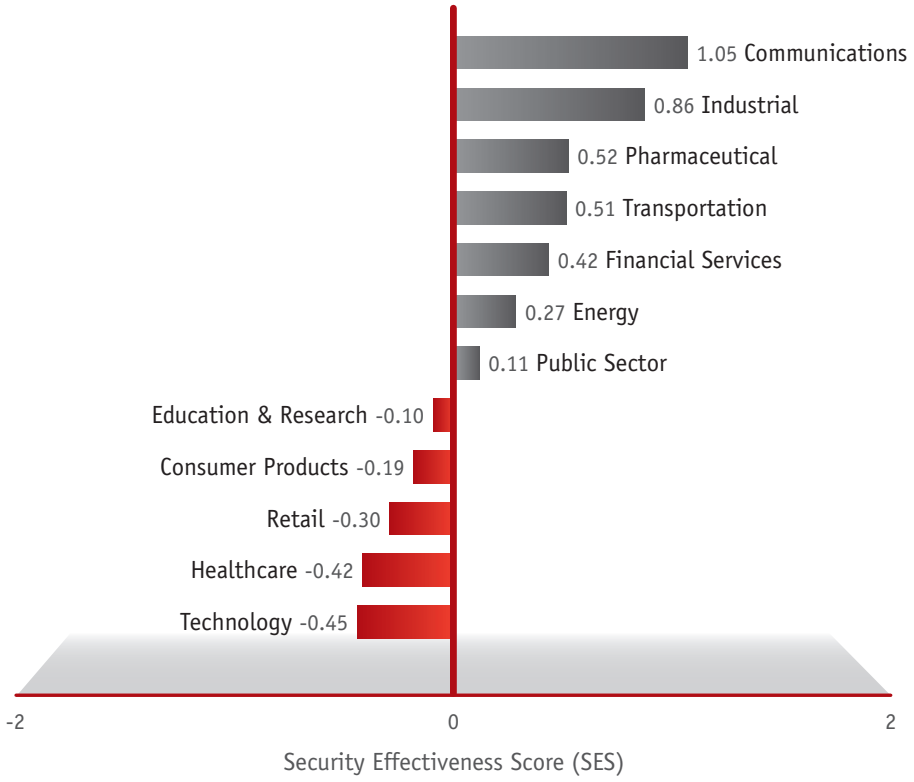


Figure 15 shows the average SES index for 12 industry segments. Although the sample size is too small to draw definitive conclusions about industry effects, these results do show marked variation in index values from a high of 1.05 for companies in the communications industry to a low of -0.45 for companies in the technology sector.

Figure 16: Pilot and Regression for Security Effectiveness Score and Per Capita Compliance Cost

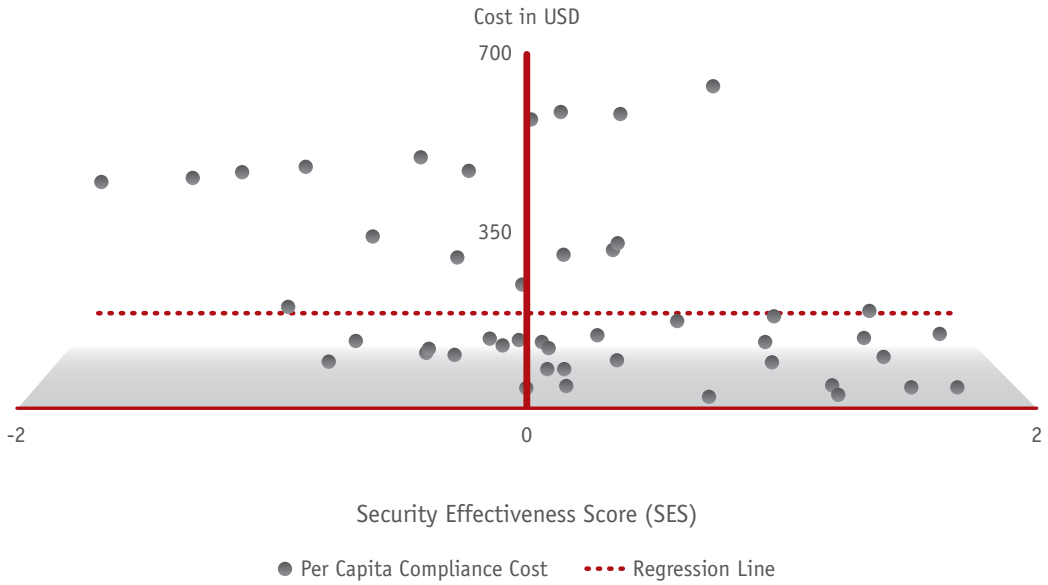


Figure 16 plots the SES index against each organization's per capita compliance cost. The graph also provides a regression line for this series. The regression slope is nearly flat, suggesting no apparent relationship between compliance cost and security effectiveness.

Figure 17: Pilot and Regression for Security Effectiveness Score and Per Capita Non-Compliance Cost

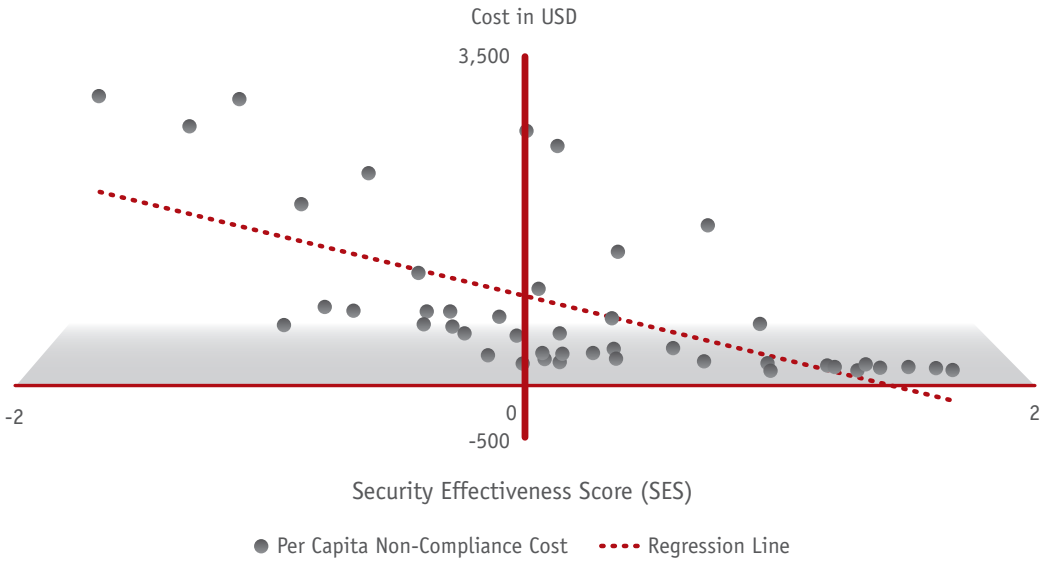
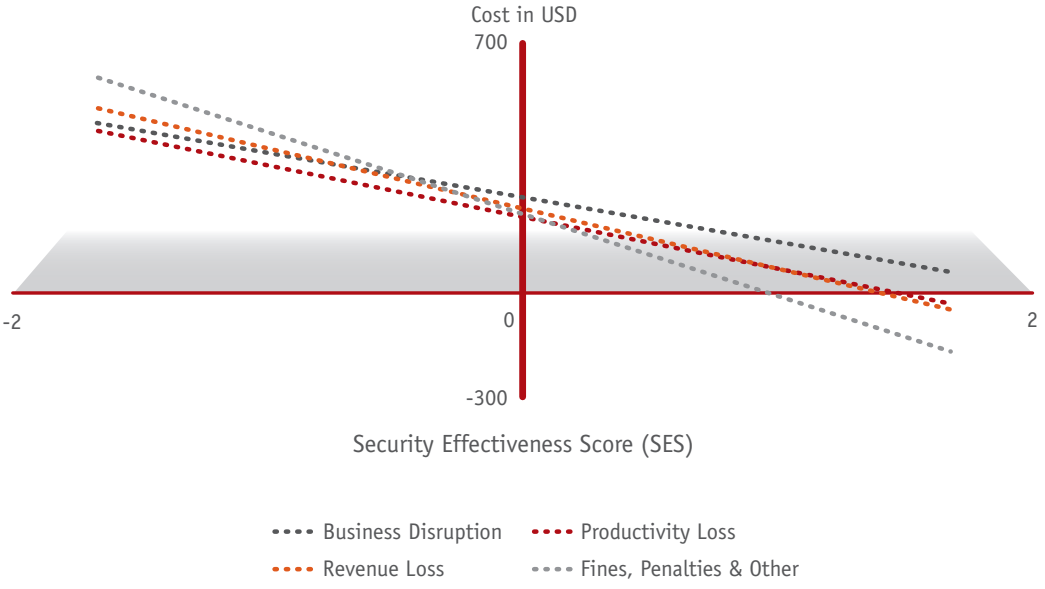


Figure 17 plots the SES against each organization's per capita non-compliance cost. Similar to the previous figure, the graph provides a regression line for the series. Here the regression line slopes downward, suggesting an inverse relationship between non-compliance cost and security effectiveness. ***In other words, organizations with a strong security posture experience a lower non-compliance cost.***

Figure 18: Regressions for Security Effectiveness Score and Four Non-Compliance Cost Components



To better understand the inverse relationship shown above, we regressed the four component parts of non-compliance cost against the SES. As shown in Figure 18, each non-compliance cost component is inversely sloping, suggesting that security effectiveness moderates the cost of business disruption, productivity loss, and revenue loss, as well as fines, penalties and other settlement costs.

Figure 19: Per Capita Non-Compliance Cost by Security Effectiveness Score Quartile in USD

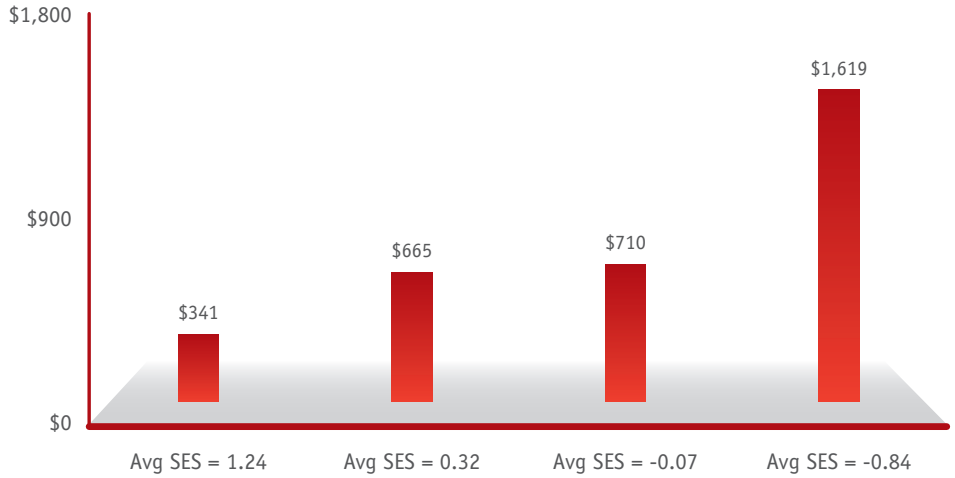
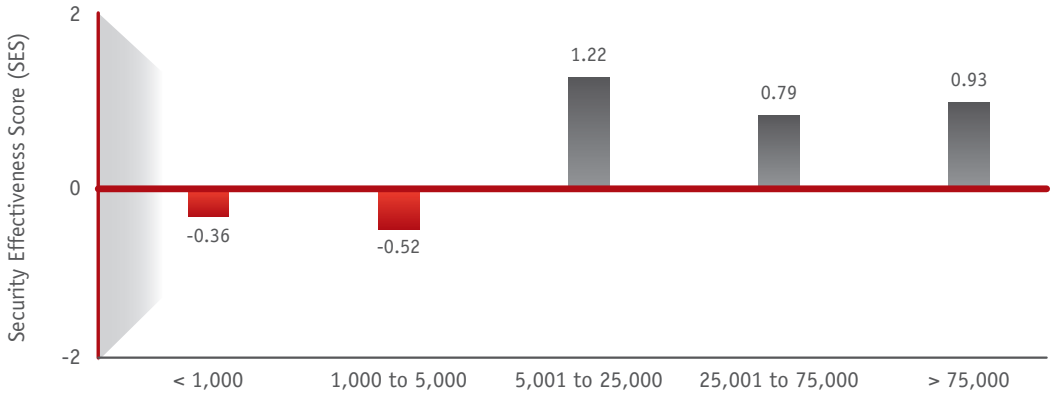


Figure 19 reports the average per capita non-compliance cost by four SES quartiles. As clearly indicated, the first quartile (with the highest SES quartile average at +1.24) achieves an average per capita non-compliance cost of only $341. The fourth quartile (with the lowest SES quartile average at -0.84) experiences an average per capita non-compliance cost of $1,619.

Figure 20: Average Security Effectiveness Score by Organizational Headcount (Size)



In Figure 20, we compare the average SES according to five organizational headcount ranges. As previously noted, larger-sized companies appear to enjoy a much lower per capita cost of both compliance and non-compliance. This chart shows companies with more than 5,000 employees achieve a higher level of security effectiveness than companies with less than 5,000 employees. This finding may partially explain why the per capita compliance and non-compliance costs of smaller-sized companies were substantially higher than larger-sized companies.

Figure 21: Internal Audit Frequency

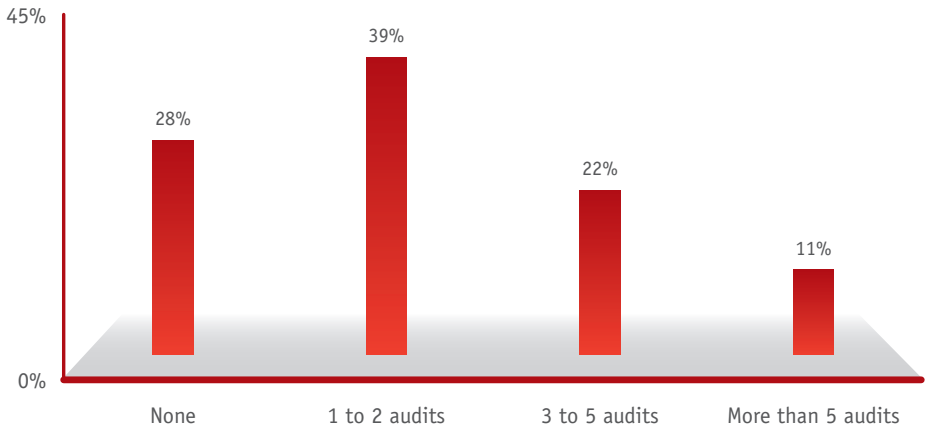


Figure 21 reports the internal compliance audit frequency of participating benchmark companies on an annual basis.[2] Surprisingly, 28 percent of companies say they do not conduct compliance audits, and only 11 percent say they conduct more than five audits each year.

[2] Please note that all audits examined in this analysis were all internally conducted either by in-house or contract (outsourced) staff.

Figure 22: Per Capita Compliance and Non-Compliance Cost by Audit Frequency in USD

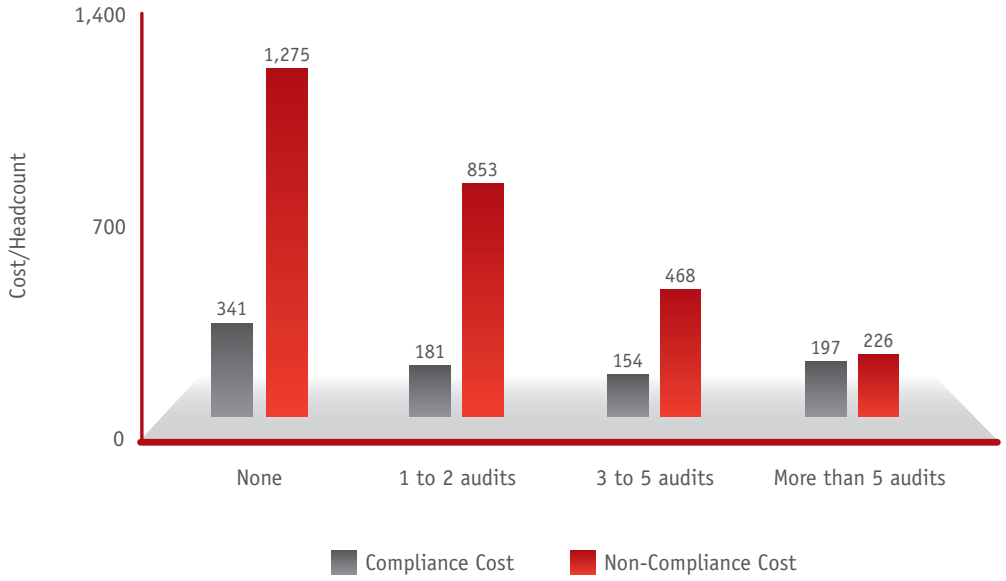


Figure 22 shows the relationship between per capita compliance and non-compliance cost and internal audit frequency. Organizations that conduct three to five internal compliance audits per year have the lowest per capita compliance cost (average $154). The highest compliance cost (average $341) is associated with organizations that do not conduct any internal compliance audits.

This figure shows an inverse relationship between per capita non-compliance cost and audit frequency. Here, the highest per capita non-compliance cost (average $1,275) is associated with organizations that do not conduct audits. The lowest per capita non-compliance cost (with an average of $226) is associated with organizations that conduct five or more audits.

Figure 23: Percentage of Compliance Spending to the Total IT Budget

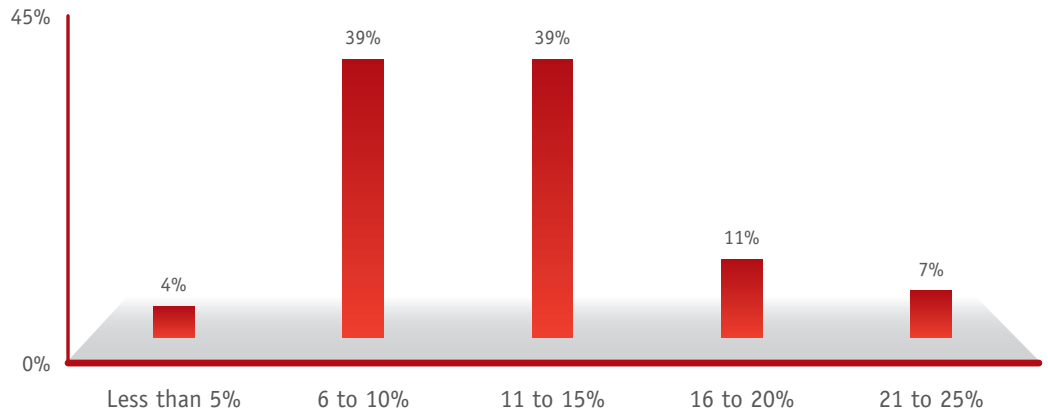


Figure 23 reports the percentage of compliance spending with respect to each organization's total IT budget. The extrapolated average percentage for all 46 benchmarked companies is 11.9 percent.

Figure 24: Per Capita Compliance and Non-Compliance Cost by Percentage of IT Budget in USD

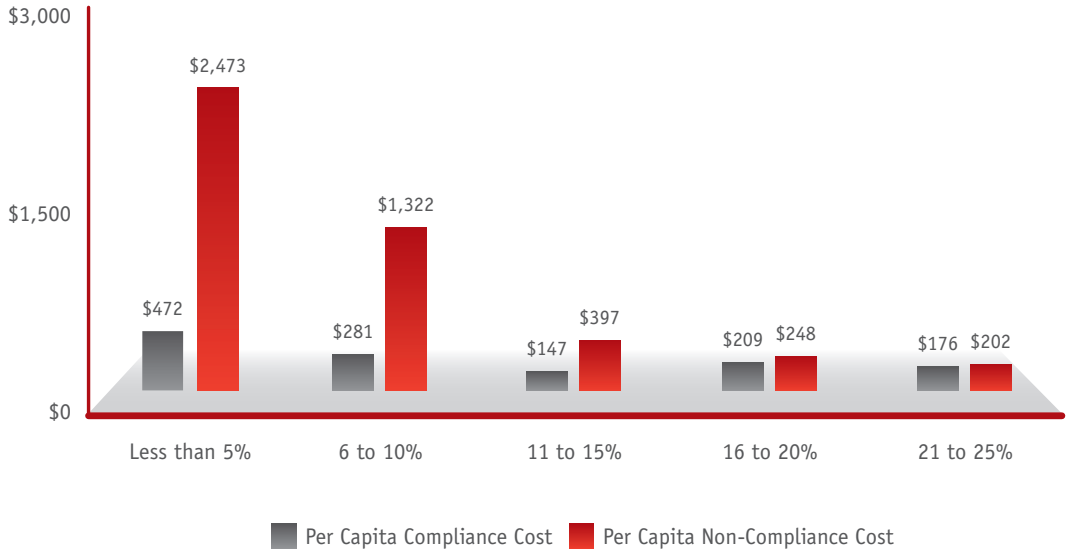


Figure 24 reveals another interesting relationship between the percentage compliance spending and per capita cost. As shown, the gap between compliance and non-compliance cost is inversely related to the percentage of compliance spending in relation to the total IT budget. In other words, spending on core compliance activities reduces the cost of non-compliance—a finding that supports our earlier hypothesis.

Table 3: Perceived importance and difficulty of data compliance regulations					
Regulations	Regulations viewed as most important		Regulations viewed as most difficult to comply with		Priority
	Frequency	Percentage	Frequency	Percentage	
PCI DSS	138	86%	75	47%	1
US state laws for data breach	106	66%	68	43%	2
Sarbanes-Oxley	103	64%	57	36%	3
EU Privacy Directive	86	54%	52	33%	4
HIPAA (including HITECH)	78	49%	19	12%	5
International laws by country	57	36%	18	11%	6
Federal Privacy Act	26	16%	7	4%	7
COPPA	26	16%	6	4%	8
GLBA	24	15%	5	3%	9
FISMA	20	13%	3	2%	10
FACTA	15	9%	3	2%	11
FCRA	11	7%	2	1%	12
CANSPAM	9	6%	1	1%	13
Other	7	4%	0	0%	14

Our final analysis examines how 160 respondents in our sample of 46 benchmarked organizations view different data compliance regulations in terms of importance and difficulty. Although certain regulations like HIPAA and GLBA are industry-specific, the summarized data in Table 3 is for all industries of surveyed respondents. This data clearly shows that PCI DSS, various US state data breach or privacy laws such as Massachusetts, Sarbanes-Oxley and the EU Privacy Directive are of greatest concern to respondents.

Figure 25: Approximate Allocation of Average Compliance Cost by Area of Focus in USD

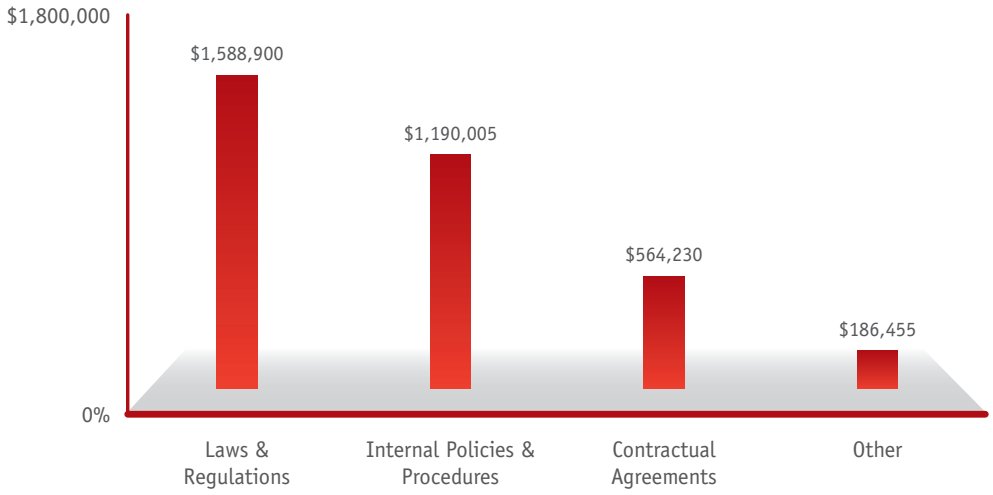


Figure 25 summarizes how compliance dollars are spent by the sample of 46 benchmarked organizations. The largest cost allocation, 45 percent, is for compliance with laws and regulations (such as those listed in the above table). The second largest cost allocation, 34 percent, is for compliance with internal policies and procedures. The remaining compliance cost allocation pertains to contractual agreements with various parties, including business partners, vendors and data protection authorities (16 percent), or other miscellaneous issues.

III
SAMPLE OF PARTICIPATING ORGANIZATIONS

Figure 26: Industry Classification of the Benchmark Sample

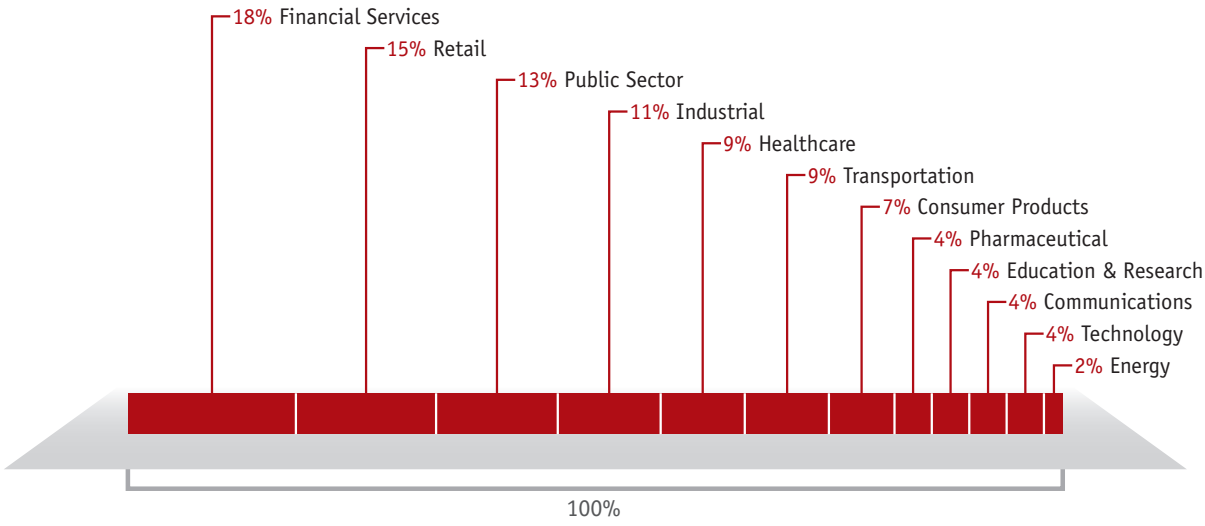


Figure 26 reports the percentage of companies by industry that participated in the benchmark study. Our final sample, which included a total of 46 organizations, served as the basis for our analysis. Financial services, retail and public sector organizations represent the three largest segments.

Figure 27: Participating Respondents by their Approximate Job Function or Title

Computed from 160 separate interviews

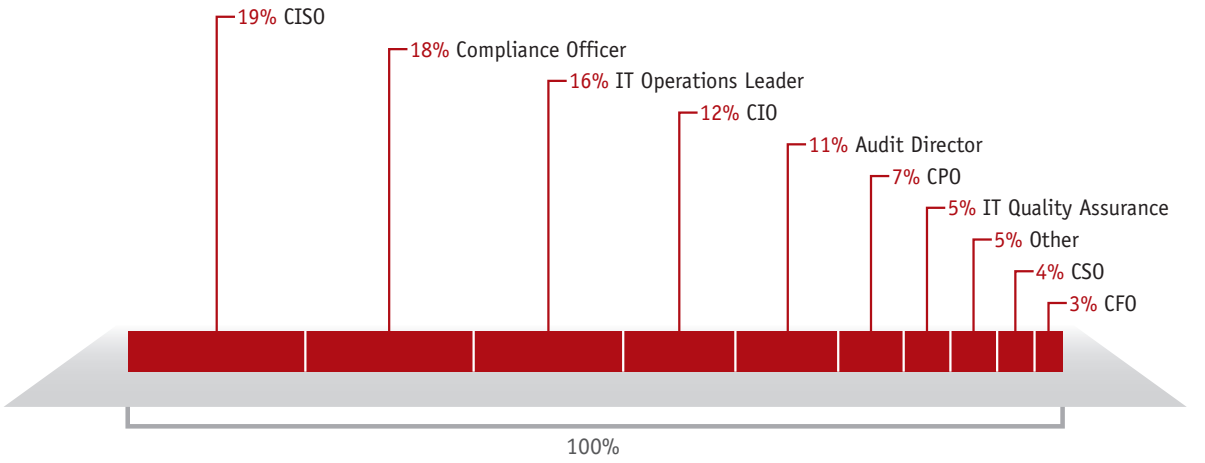
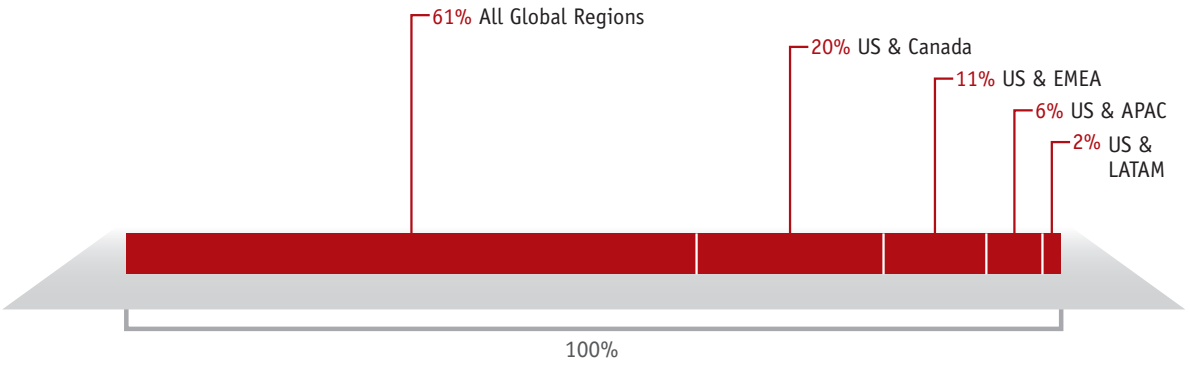


Figure 27 reports the approximate job functions or titles of participants who completed the diagnostic interview. In total, 160 individuals with responsibility for data protection and compliance activities were engaged in the benchmark research process.

Figure 28: Distribution of Participating Organizations by Global Region



On average, benchmark methods required between three and four interviews to capture enough information to extrapolate compliance and non-compliance costs. Respondents in information security, compliance, and IT operations represent the top three functional areas participating in these diagnostic interviews.

Figure 28 reports the percentage frequency of multinational companies based on their global footprint. While all 46 organizations operate in more than one country, 61 percent operate in all global regions. Twenty percent operate in the United States and Canada.

Figure 29: Distribution of Participating Organizations by Global Headcount

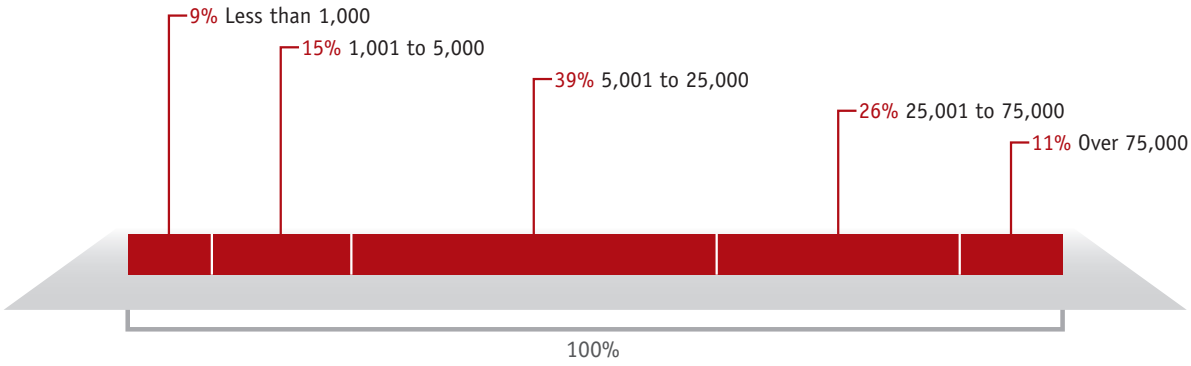


Figure 29 summarizes the global headcount of participating organizations, wherein the largest segment includes organizations with 5,001 to 25,000 full-time equivalent employees. Accordingly, headcount is used as a means of inferring organizational size in this research.

IV
COST FRAMEWORK

Our primary method for determining the total cost of compliance relies on the objective collection of cost data. Using a well-known cost accounting method, we were able to segment detailed cost data into discernible activity centers that explain the entire data protection and compliance mandate within benchmarked companies.[3] We determined that the following six cost activity centers span the full economic impact of compliance costs associated with protecting data. Within each center we compile the direct and indirect costs associated with each activity.

Compliance policies: Activities associated with the creation and dissemination of policies related to the protection of confidential or sensitive information such as customer data, employee records, financial information, intellectual properties and others.

Communications: Activities and associated costs that enable a company to train or create awareness of the organization's policies and related procedures for protecting sensitive or confidential information. This activity includes all downstream communications to employees, temporary employees, contractors and business partners. It also includes the required notifications about policy changes and data breach incidents.

Program management: Activities and associated costs related to the coordination and governance of all program activities within the enterprise, including direct and indirect costs related to privacy and IT compliance.

Data security: All activities and technologies used by the organization to protect information assets. Activities include professional security staffing, implementation of control systems, backup and disaster recovery operations and others.

Compliance monitoring: All activities deployed by the organization to assess or appraise compliance with external, internal and contractual obligations. It includes costs associated with internal audits, third-party audits, technology, verification programs, professional audit staffing and others.

Enforcement: Activities related to detecting non-compliance, including incident response. These activities also include redress activities such as hotlines, remedial training of employees who violate compliance requirements, and voluntary self-reporting to regulators.

In addition to the above internal activities, most companies incur tangible costs and opportunity losses as a result of non-compliance with data protection requirements and laws. An example of a non-compliance event includes end-user violations of company policies such as the misuse of Internet applications or use of insecure devices in the workplace. Other examples include contractual violations with vendors or business partners, organizational changes imposed by regulators, data loss incidents, theft of intellectual properties and many others. Our total compliance cost framework includes the four broadly defined consequences of non-compliance as follows:

Business disruption: The total economic loss that results from non-compliance events or incidents such as the cancellation of contracts, business process changes imposed by regulators, shutdowns of business operations and others.

Productivity loss: The time for accomplishing work-related responsibilities that employees lose (and related expenses) because the systems and other critical processes they rely on experience downtime.

Lost revenues: The loss in revenue sustained as a result of non-compliance with data protection requirements and laws. This includes customer turnover and diminished loyalty due to lost trust and confidence in the organization.

Fines, penalties and other settlement costs: The total fines, penalties and other legal or non-legal settlements associated with data protection non-compliance issues. This includes expenditures for engaging legal defense and other experts to help resolve issues associated with compliance infractions and data breaches.

[3] Ponemon Institute's cost of data breach studies conducted over the past six years utilizes activity-based cost to define the total economic impact of data loss or theft that requires notification. See, for example, 2009 Cost of Data Breach, Ponemon Institute January 2010.

Figure 30: Total Compliance Cost Framework

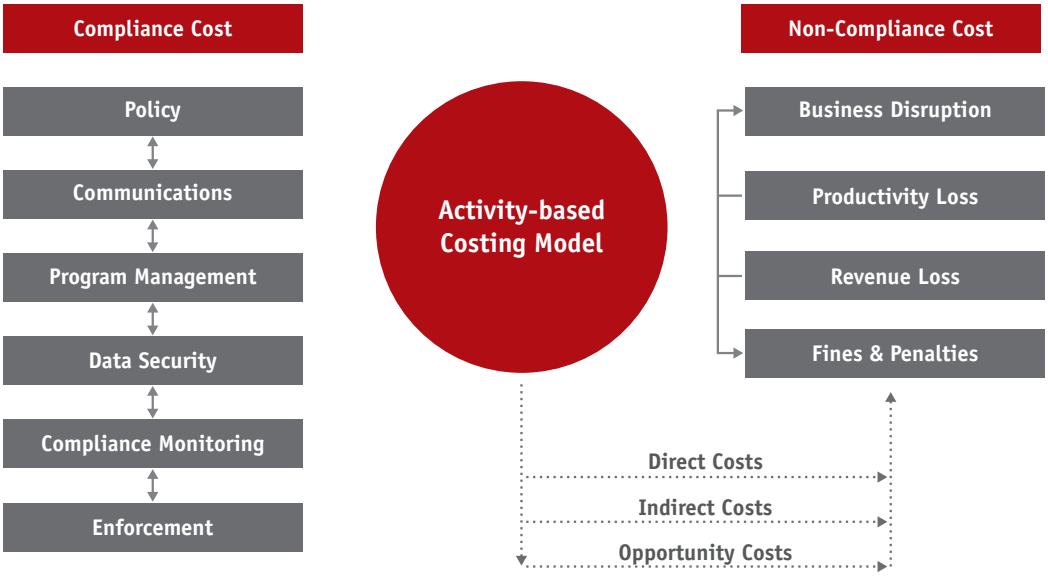


Figure 30 presents the activity-based costing framework used in this research. The framework consists of six cost center activities denoted as "compliance costs," and four cost consequences denoted as "non-compliance costs." As shown, the six compliance costs are policy, communications, program management, data security, compliance monitoring and enforcement.

Each of these activities generates direct, indirect and opportunity costs. The consequences for failing to comply with data compliance requirements include business disruption, productivity losses, and revenue losses, as well as fines, penalties and other cash outlays. In the study, we used two sets of costs for each benchmarked organization, which combined make up the total cost of compliance.

V
BENCHMARK METHODS

To obtain information about each organization's total compliance cost, the researchers utilized an activity-based costing method and a proprietary diagnostic interviewing technique. Following are the approximate titles of the 160 functional leaders from the benchmarked organizations that participated in our study:

- Chief Information Officer
- Chief Information Security Officer
- Chief Compliance Officer
- Chief Financial Officer
- Chief Privacy Officer
- Internal Audit Director
- IT Compliance Leader
- IT Operations Leader
- Human Resource Leader
- Data Center Management

The benchmark instrument contains a descriptive cost for each one of the six cost activity centers. Within each activity center, the survey requires respondents to specify a cost range that estimates direct cost, indirect cost and opportunity cost, which are defined as follows:

Direct cost – the direct expense outlay to accomplish a given activity.

Indirect cost – the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.

Opportunity cost – the cost resulting from lost business opportunities as a result of compliance infractions that diminish the organization's reputation and goodwill.

Our research methods captured information about all costs grouped into six core compliance activities:

- Policy development and upstream communication
- Training, awareness and downstream communication
- Data protection program activities
- Data security practices and controls
- Compliance monitoring
- Enforcement

Our benchmark instrument was designed to collect descriptive information from individuals who are responsible for data protection efforts within their organizations. The research design relies upon a shadow costing method used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of individuals within participating organizations. Hence, the costs we extrapolated are those incurred directly or indirectly by each organization as a result of their efforts to achieve compliance with a plethora of data protection requirements. Our methods also permitted us to collect information about the economic consequences of non-compliance.

The benchmark framework in Figure 1 presents the two separate cost streams used to measure the total cost of compliance for each participating organization. These two cost streams pertain to cost center activities and consequences experienced by organizations during or after a non-compliance event. Our benchmark instrument also contained questions designed to elicit the actual experiences and consequences of each incident. This cost study is unique in addressing the core systems and business activities that drive a range of expenditures associated with a company's efforts to comply with known requirements.

Within each category, cost estimation is a two-stage process. First, the survey requires individuals to provide direct cost estimates for each cost category by checking a range variable. A range variable is used instead of a point estimate to preserve confidentiality (in order to ensure a higher response rate). Next, the survey requires participants to provide a second estimate that indicates indirect cost and separately, opportunity cost. These estimates are calculated based on the magnitude of these costs relative to a direct cost within a given category. Finally, we conducted a follow-up interview to validate the cost estimates provided by the respondents, and when necessary, to resolve potential discrepancies).

The size and scope of survey items is limited to known cost categories that cut across different industry sectors. In our experience, a survey that focuses on process yields a higher response rate and higher quality results. We also use a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

To maintain complete confidentiality, the survey instrument does not capture company-specific information of any kind. Research materials do not contain tracking codes or other methods that could link responses to participating companies.

To keep the benchmark instrument to a manageable size, we carefully limited items to only those cost activities we consider crucial to the measurement of data protection compliance costs rather than all IT compliance costs. Based on discussions with subject matter experts, the final set of items focus on a finite set of direct and indirect cost activities. After collecting benchmark information, each instrument is examined carefully for consistency and completeness. In this study, two companies were rejected because of incomplete, inconsistent or blank responses.

The study was launched in November, 2010 and fieldwork concluded in January, 2011. The recruitment started with a personalized letter and a follow-up phone call to 209 organizations for possible participation in our study. While 69 organizations initially agreed to participate, 46 organizations permitted researchers to complete the benchmark analysis.

The time period used in the analysis of compliance costs was 12 months. Because we collected information only during this continuous 12-month time frame, the study cannot gauge seasonal variation on specific cost categories.

VI
CONCLUSION

To reduce the total cost of compliance and offset the risk of non-compliance, security strategies should integrate enabling technologies with people, policies and operational processes. The following attributes are most strongly correlated with creating an effective security posture while meeting an organization's compliance goals. Table 4 reports the ten attributes from the security effectiveness score instrument that have the highest inverse correlation with non-compliance cost (as computed from the 46 benchmark companies). In other words, these 10 attributes lend the greatest support to a strong compliance culture.

Table 4: Security effectiveness attributes with the highest negative correlation to non-compliance cost

Security effectiveness scoring attributions	Correlation*
Monitor and strictly enforce security policies	-0.34
Conduct audits or assessments on an ongoing basis	-0.32
Attract and retain professional security personnel	-0.31
Ensure minimal downtime or disruptions to systems resulting from security issues	-0.30
Prevent or curtail viruses, malware and spyware infections	-0.29
Measure the effectiveness of security program components	-0.28
Ensure security program is consistently managed	-0.27
Know where sensitive or confidential information is physically located	-0.26
Secure endpoints to the network	-0.25
Identify and authenticate end-users before granting access to confidential information	-0.23

*Non-parametric correlation method utilized because of small sample size

Many of the 10 security effectiveness attributes pertain to governance and oversight of the organization's security initiatives. Organizations can adopt the following steps to achieve a governance infrastructure that supports compliance across the enterprise:

- Appoint a high-level individual to lead activities around compliance with data protection laws and requirements
- Ensure board-level oversight of compliance activities (through the board's audit committee)
- Ensure the budget for compliance is adequate to meet specific goals and objectives
- Establish a cross-functional steering committee to oversee local compliance requirements
- Implement metrics that define compliance program success
- Ensure senior executives receive critical reports when compliance issues reach crisis levels

Achieving critical and complex goals related to compliance requires holistic and integrated security solutions that seamlessly address every area of the organization that compliance impacts. Recent benchmark research conducted by Ponemon Institute provides insights from information security leaders on how to build an integrated and holistic security strategy.

Today's security initiatives require organizations to anticipate how changing threats will affect their organization's ability to comply with external, internal and contractual demands. We have identified four primary security areas that affect all organizations: external and internal threats to security, the changing workforce, changing business models and processes, and the changing world. Understanding the implications of these security challenges can help organizations succeed in aligning their core practices and technologies across the enterprise in ways that minimize the risk of compliance failure. Organizations can respond to these individual security challenges in the following ways:

- Changing threats require an organization to make security an integral part of its culture; keep pace with technological advances; build security into business processes to reduce compliance risks; understand the latest threats; and actively assess the insider threat.

- The changing workforce requires organizations to make sure security keeps pace with organizational restructuring and change; audit, grant or withdraw access rights to property and systems; have adequate screening procedures for new employees; and determine if remote workers are securely accessing the network.

- Business changes require organizations to secure business processes during periods of transition; understand operational dependencies; verify that business partners have sufficient security practices in place; secure the transfer of information assets between different organizations; and review, audit, and when necessary, revoke access rights.

- Finally, a quickly changing environment requires organizations to have the technologies and plans in place to deal with attacks upon the critical infrastructure, theft of information assets, and other criminal incidents.

- The implications for an organization that does not manage compliance risks with the right integrated and holistic response to data security and related compliance challenges are a decrease in revenue that results from both the loss of customer trust and loyalty and the inability to deliver services and products.

- Beyond the economic impact, non-compliance increases the risk of losing valuable information assets such as intellectual property, physical property and customer data. Further, non-compliant organizations risk becoming victims of cyber fraud, business disruption, and many other consequences that might lead to business failure.

We believe our study demonstrates that an investment in both external and internal compliance activities is beneficial not only to an organization's security stature, but also to its overall operations. We have shown that while organizations will incur both compliance and non-compliance costs, proactively investing in compliance activities can potentially help organizations reduce the risk created by the consequences and reactive spending of non-compliance. In addition, employing the above practices can allow organizations to experience greater compliance gains for a given level of investment. Further, the results of this study will help corporate IT and lines of business demonstrate the value of investing in their compliance activities.

CAVEATS

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute 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 data centers, all located in the United States. 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 over 200 separate organizations. Forty-six organizations 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 detection, 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 companies with more mature compliance 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 benchmarked organizations. While certain checks and balances can be incorporated into the data capture 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.

[4] Non-parametric correlation method utilized because of small sample size

APPENDIX 1: SUMMARIZED COMPLIANCE COST DATA FOR 46 BENCHMARKED ORGANIZATIONS

The following table summarizes the compliance cost for 46 benchmarked companies (USD).

ID#	Policy	Communication	Program management	Data security	Compliance monitoring	Enforcement	Total
1	550,648	210,864	498,175	1,339,760	776,366	265,287	3,641,100
2	446,557	289,013	630,915	1,776,346	682,628	730,033	4,555,492
3	279,788	659,796	773,779	1,408,469	,330	686,581	4,708,743
4	334,	598,494	544,820	1,340,140	466,457	617,083	3,901,394
5	405,501	421,450	494,041	1,083,907	865,221	776,208	4,046,328
6	96,126	14,264	94,186	149,584	124,343	102,765	581,268
7	1,104,599	1,673,422	1,841,672	3,753,816	3,186,971	4,488,671	16,049,151
8	196,658	151,261	329,446	678,499	458,177	162,888	1,976,929
9	644,957	664,241	621,988	1,613,640	1,389,769	2,105,350	7,039,945
10	91,056	267,731	246,533	666,479	305,448	581,786	2,159,033
11	153,381	209,156	312,915	730,326	233,236	392,165	2,031,179
12	575,667	356,883	370,243	1,140,231	1,057,060	1,034,786	4,534,870
13	31,429	101,884	53,737	135,685	86,520	67,537	476,792
14	143,968	133,568	175,625	578,804	143,736	64,491	1,240,192
15	36,761	25,946	48,628	184,579	90,708	59,075	445,697
16	1,302,120	1,025,146	1,426,657	2,902,498	2,733,365	1,621,399	11,011,185
17	116,859	13,732	171,449	712,128	120,656	31,731	1,166,555
18	130,759	53,267	196,436	671,340	188,658	501,686	1,742,146
19	1,686,805	29,736	1,461,105	2,348,785	1,696,734	4,226,085	13,429,250
20	397,451	613,277	420,593	1,125,598	777,889	1,713,504	5,048,312
21	103,720	141,859	236,323	718,894	270,722	490,152	1,961,670
22	75,844	143,995	239,910	610,412	227,870	129,588	1,427,619
23	743,649	880,959	1,225,	2,561,789	1,469,677	4,118,242	10,999,816
24	92,586	236,968	227,158	759,254	399,243	66,120	1,781,329
25	155,870	116,878	220,896	718,717	181,546	63,768	1,457,675
26	115,633	57,315	286,567	802,614	265,696	83,930	1,611,755
27	105,487	101,770	110,092	589,605	162,345	70,042	1,139,341
28	1,082,810	1,313,210	2,168,351	2,620,405	2,997,309	2,628,795	12,810,880
29	85,199	69,818	153,765	591,023	227,645	145,503	1,272,953
30	77,060	139,531	2845	690,321	340,914	489,621	2,021,452
31	655,531	654,099	1,032,528	1,678,494	1,905,917	3,673,134	9,599,703
32	237,479	382,895	555,232	977,514	398,542	430,848	2,982,510
33	212,083	186,019	254,091	816,294	338,862	210,363	2,017,712
34	68,113	157,859	205,410	610,458	313,499	535,648	1,890,987
35	18,271	39,886	89,562	519,783	88,733	91,805	848,040
36	180,656	87,246	203,693	695,941	282,769	574,464	2,024,769
37	28,992	90,530	79,974	369,153	32,872	34,475	635,996
38	13,796	16,280	107,980	287,030	38,796	281,258	745,140
39	184,477	130,493	147,412	823,775	173,917	202,983	1,663,057
40	109,247	191,817	301,495	938,927	529,364	174,026	2,244,876
41	216,205	228,313	222,848	854,625	296,330	237,655	2,055,976
42	194,550	158,518	246,618	944,863	498,570	111,113	2,154,232
43	31,236	134,658	190,659	805,721	202,001	55,865	1,420,140
44	117,418	332,484	358,327	784,090	563,258	168,706	2,324,283
45	24,705	174,207	220,803	875,848	494,681	268,219	2,058,463
46	47,747	122,731	243,385	584,651	295,603	130,155	1,424,272
Avg	**297,910**	**343,119**	**441,859**	**1,034,148**	**636,542**	**775,991**	**3,529,569**

APPENDIX 2: SUMMARIZED NON-COMPLIANCE COST DATA FOR 46 BENCHMARKED ORGANIZATIONS

The following table summarizes non-compliance cost for 46 benchmarked companies (USD).

ID#	Business disruption	Productivity loss	Revenue loss	Fines, penalties & settlement costs	Total
1	1,894,201	886,772	2,506,798	2,504,853	7,792,624
2	2,530,352	2,961,739	3,254,316	2,451,421	11,197,829
3	3,510,825	3,522,002	2,521,616	978,761	10,533,203
4	7,655,995	1,719,063	2,225,011	707,799	12,307,868
5	6,067,953	4,591,037	3,996,297	811,886	15,467,173
6	530,415	-	546,622	309,721	1,386,758
7	7,712,747	5,402,988	700,438	310,856	14,127,029
8	1,399,309	3,401,988	3,157,199	1,666,473	9,624,969
9	4,747,903	1,663,583	1,606,138	191,044	8,208,668
10	3,804,836	5,150,215	4,552,824	1,938,156	15,446,031
11	465,637	423,498	710,214	704,687	2,304,036
12	3,117,942	3,111,298	1,767,796	80,384	8,077,420
13	535,602	652,483	346,224	383,742	1,918,051
14	-	1,384,147	741,359	799,265	2,924,771
15	765,450	-	540,296	1,763,402	3,069,148
16	16,552,877	53,154	6,538,555	1,344,968	24,489,553
17	1,613,945	2,229,318	1,756,673	1,972,003	7,571,939
18	709,556	1,049,803	1,315,445	1,065,976	4,140,781
19	6,020,835	748,078	1,899,101	2,383,793	11,051,807
20	-	4,501,598	1,571,536	2,390,360	8,463,494
21	2,663,217	6,446,758	2,513,763	3,431,797	15,055,534
22	1,805,479	2,841,799	1,526,188	579,088	6,752,554
23	5,078,817	4,014,515	2,790,129	427,940	12,311,402
24	4,359,921	3,898,962	2,637,710	668,455	11,565,048
25	2,539,821	-	2,444,529	1,382,552	6,366,902
26	2,285,952	2,175,764	4,288,741	2,810,190	11,560,647
27	630,284	1,613,219	2,498,983	2,103,072	6,845,558
28	10,610,045	5,174,955	4,696,161	7,493,699	27,974,860
29	3,878,864	3,135,708	2,067,828	2,841,451	11,923,852
30	2,236,557	3,849,895	3,882,527	1,831,169	11,800,148
31	3,683,109	2,763,377	3,044,502	885,412	10,376,400
32	3,386,634	2,420,115	2,666,676	1,085,278	9,558,703
33	2,178,924	2,158,495	1,726,303	1,809,951	7,873,673
34	5,424,731	1,420,338	2,123,134	1,888,016	10,856,219
35	1,532,994	1,721,369	1,668,480	700,800	5,623,643
36	2,152,478	469,623	1,387,055	526,313	4,535,469
37	1,393,876	-	154,675	146,806	1,695,357
38	328,189	-	557,464	671,041	1,556,694
39	1,955,264	3,536,600	1,304,047	2,689,848	9,485,760
40	2,333,900	3,800,776	1,763,831	869,986	8,768,492
41	1,621,980	5,697,483	2,539,403	795,896	10,654,763
42	6,413,603	3,550,955	3,178,774	147,334	13,290,666
43	3,035,969	204,740	1,478,622	798,862	5,518,192
44	3,383,818	2,603,496	1,201,703	1,997,390	9,186,408
45	2,076,828	1,761,714	2,320,328	1,369,728	7,528,597
46	5,063,475	3,425,150	1,608,866	2,077,943	12,175,433

APPENDIX 3: 24 SECURITY EFFECTIVENESS SCORE (SES) ITEMS

The following table summarizes the average SES by item for 46 benchmarked companies.

Security effectiveness scoring attributions	Item score
Determine the root cause of data loss or theft	0.20
Identity all significant data breach incidents	0.27
Know where sensitive or confidential information is physically located	-0.48
Secure sensitive or confidential data at rest	-0.02
Secure sensitive or confidential data in motion	-0.57
Secure endpoints to the network	0.40
Identify and authenticate end-users before granting access to confidential information	0.42
Protect sensitive or confidential information used by outsourcers	1.05
Prevent or curtail the theft of information assets	0.19
Prevent or curtail external penetration or hacking attempts	0.02
Limit physical access to devices containing sensitive or confidential information	-0.15
Measure the effectiveness of security program components	-0.38
Ensure minimal downtime or disruptions to systems resulting from security issues	0.61
Test (prove) compliance with legal and regulatory requirements	-0.94
Test (prove) compliance with self-regulatory mandates	1.53
Prevent or curtail viruses, malware and spyware infections	-0.01
Ensure security patches are updated in a timely and comprehensive fashion	-0.48
Control all live data used in systems development activities	-0.14
Monitor and strictly enforce security policies	0.57
Attract and retain professional security personnel	1.62
Training and awareness program for all users	-0.16
Conduct audits or assessments on an ongoing basis	1.08
Ensure security program is consistently managed	-0.06
Prevent or curtail denial of service attacks	0.19
Monitor networks, systems and logs for unusual events	-0.14
Average security effectiveness score	**0.18**

Ponemon Institute LLC
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.

This report commissioned by Tripwire, Inc.

Tripwire is a leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Thousands of customers rely on Tripwire's integrated solutions to help protect sensitive data, prove compliance and prevent outages. Tripwire® VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and security event management solutions, is the way organizations can proactively achieve continuous compliance, mitigate risk and improve operational control through Visibility, Intelligence and Automation.

Learn more at tripwire.com/ponemon and at @tripwireinc and #compliancecost on Twitter.

If you have questions or comments about this report, please contact us:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.877.3118
research@ponemon.org

Ponemon INSTITUTE

Follow the conversation on Twitter #compliancecost and @TripwireInc. Scan the code or visit tripwire.com/ponemon.

BRTCOC2a