THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS

BENCHMARK STUDY OF MULTINATIONAL ORGANIZATIONS

Sponsored by Globalscape
Independently conducted by Ponemon Institute LLC
Publication Date: December 2017

globalscape
by HelpSystems

CONTENTS

PART 1

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 that include process, people and technologies. In this year's study, companies expressed concern about achieving compliance with the EU's General Data Protection Regulation (GDPR) by May 25, 2018.

> Thekeytakeawayfromthisstudyisthatit pays to invest in compliance. Specifically, if companies spent more on compliance activities such as audits, enabling technologies, training and expert staffing, it would be less costly than if they were in non-compliance with data protection regulations.

Ponemon Institute and Globalscape conducted The True Cost of Compliance with Data Protection Regulations to determine the full economic impact of compliance activities for a representative sample of 53 multinational organizations. An earlier study was completed in 2011 and those findings are compared to this year's results.[1]

The objective of this research is to determine the full costs associated with an organization's compliance efforts, including the cost of non-compliance with laws, regulations and policies. In order to be as accurate as possible in our cost estimates, we interviewed 237 individuals involved in compliance activities in benchmarked organizations.

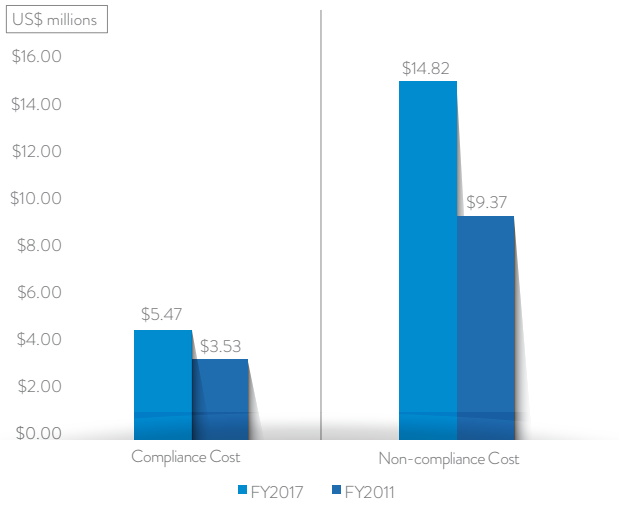
COMPANIES ARE SPENDING MORE ON COMPLIANCE AND THE CONSEQUENCES OF NON-COMPLIANCE

As shown in Figure 1, while the average cost of compliance for the organizations in our current study is $5.47 million, a 43 percent increase from 2011, the cost of not being in compliance is much greater.[2]

> The average cost for organizations that experience non-compliance problems is $14.82 million, a 45 percent increase from 2011.

Thus, investing in the compliance activities described in this study can be beneficial in avoiding such non-compliance problems as business disruption, declines in productivity, fees, penalties and other legal and non-legal settlement costs.

Figure 1. Difference between Compliance and Non-compliance Cost



THE COST OF BEING IN COMPLIANCE

Companies invest in compliance activities because of laws and regulations and not necessarily to improve their security posture. Regulations that are a priority are the EU's General Data Protection Regulation (GDPR), PCI DSS, HIPAA and various state privacy and data protection laws, country-specific laws and Sarbanes-Oxley.

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

Following are typical compliance costs:

- Data protection and enforcement activities
- Incident response plans
- Compliance audits and assessments
- Policy development
- Communications & training
- Staff certification
- Redress activities
- Investments in specialized technologies to protect data assets such as threat intelligence, managed file transfer, identity and access governance, cyber analytics, data loss prevention, encryption and more

THE COST OF NON-COMPLIANCE

Non-compliance costs are those that result when a company fails to comply with rules, regulations, policies, contracts and other legal obligations. Following are costs due to non-compliance.

These costs, as shown in this report, are 2.71 times the cost of compliance:

- Business disruption
- Productivity losses
- Revenue losses
- Fines, penalties and settlement costs

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

Understandably, organizations in heavily regulated industries such as financial services and healthcare have the highest compliance costs. Such costs are also affected by the amount of sensitive and confidential information an organization must secure.

> The cost of compliance varies significantly by the organization's industry sector, ranging from $7.7 million for media to more than $30.9 million for financial services.

The percentage net increase in total compliance cost between 2011 and 2017 also varies by industry. Healthcare organizations and technology and software organizations experienced the highest growth in cost at 106 percent and 99 percent, respectively. Energy, utilities and retail companies show the lowest growth in total compliance cost at 6 percent and 40 percent, respectively, between 2011 and 2017.

When adjusting compliance and non-compliance costs by each organization's headcount, smaller-sized companies (less than 5,001 employees) incur substantially higher per-capita compliance costs than larger companies (more than 5,000 employees).

THE FOLLOWING FACTORS LOWER THE TOTAL COST OF COMPLIANCE

The more effective an organization's security posture is, the lower the cost of non-compliance. Using a well-known indexing method that measures each organization's security posture, called the security effectiveness score (SES), we determined that security effectiveness is unrelated to compliance cost. However, SES appears to be inversely related to non-compliance cost. Thus, organizations with a higher score (more favorable security posture) experience a lower cost of non-compliance.

Corporate investment in compliance reduces the negative consequences and cost of non-compliance. Per capita non-compliance cost is inversely related to the percentage of compliance spending in relation to the total IT budget. Clearly, a higher percentage for compliance spending relative to the total IT budget is an indication that corporate investment in compliance reduces the negative consequences and cost of non-compliance.

Ongoing compliance audits reduce the total costs of compliance. Per capita non-compliance cost appears to be inversely related to the frequency of compliance audits, whereas organizations that do not conduct compliance audits experience the highest compliance cost when adjusted for size.

PART 2
KEY FINDINGS

In this section, we provide a deeper analysis of what affects the cost of compliance and non-compliance and why non-compliance costs are significantly higher. The report is organized according to the following topics:

- The cost of compliance
- The cost of non-compliance
- The impact of governance and regulations on the cost of compliance
- The impact of security posture on the cost of compliance

The key findings presented below are based on the benchmark analysis of 53 multinational organizations located in the United States. We obtained information about each organization's data compliance cost utilizing an activity-based costing method and a proprietary diagnostic interviewing technique involving 237 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, standards, 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 a company fails to comply with rules, regulations, policies, contracts, and other legal obligations. The Appendix of this report discusses our benchmarking methods in greater detail.

In the course of interviewing functional leaders, we determined key trends and commonalities between both compliance and non-compliance costs. 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 frameworks including ISO, NIST and others.

THE COST OF COMPLIANCE

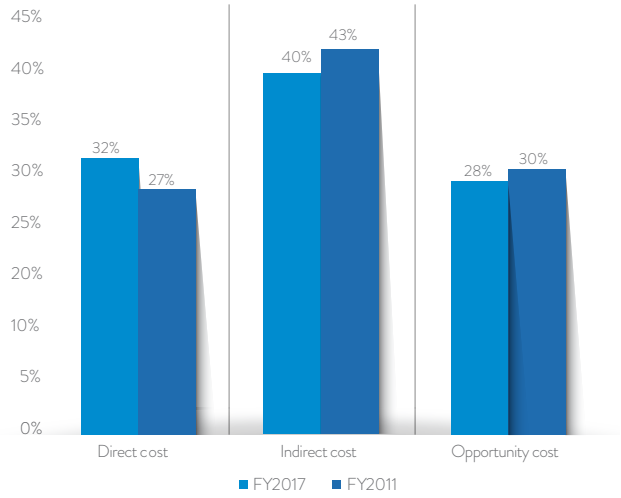
Organizations spend the most on administering their compliance programs. Figure 2 reports how costs are allocated on a percentage basis for all data compliance cost activities combined.

As shown, indirect costs, such as administrative overhead, account for 40 percent of compliance cost activities. Direct costs such as payments to consultants, auditors or other outside experts represents 32 percent, which increased by five percent between 2011 and 2017. Opportunity costs, such as an organization's inability to execute a marketing campaign because of consumer privacy concerns, represent 28 percent.

> Data security has the highest costs with policy representing the lowest costs; the average cost of data security is $2 million.

Figure 2. Percentage cost structure for compliance costs

Computed from 53 benchmarked companies



As discussed previously, the cost of compliance can range from $5.5 million to almost $22 million. Table 1 summarizes the total, average, median, maximum and minimum compliance costs for each of the six activity centers defined in our cost framework in Part 5. Please note that these cost statistics are defined for a 12-month period. Data security represents the largest cost center, while policy represents the smallest center of cost activities for the benchmark sample.

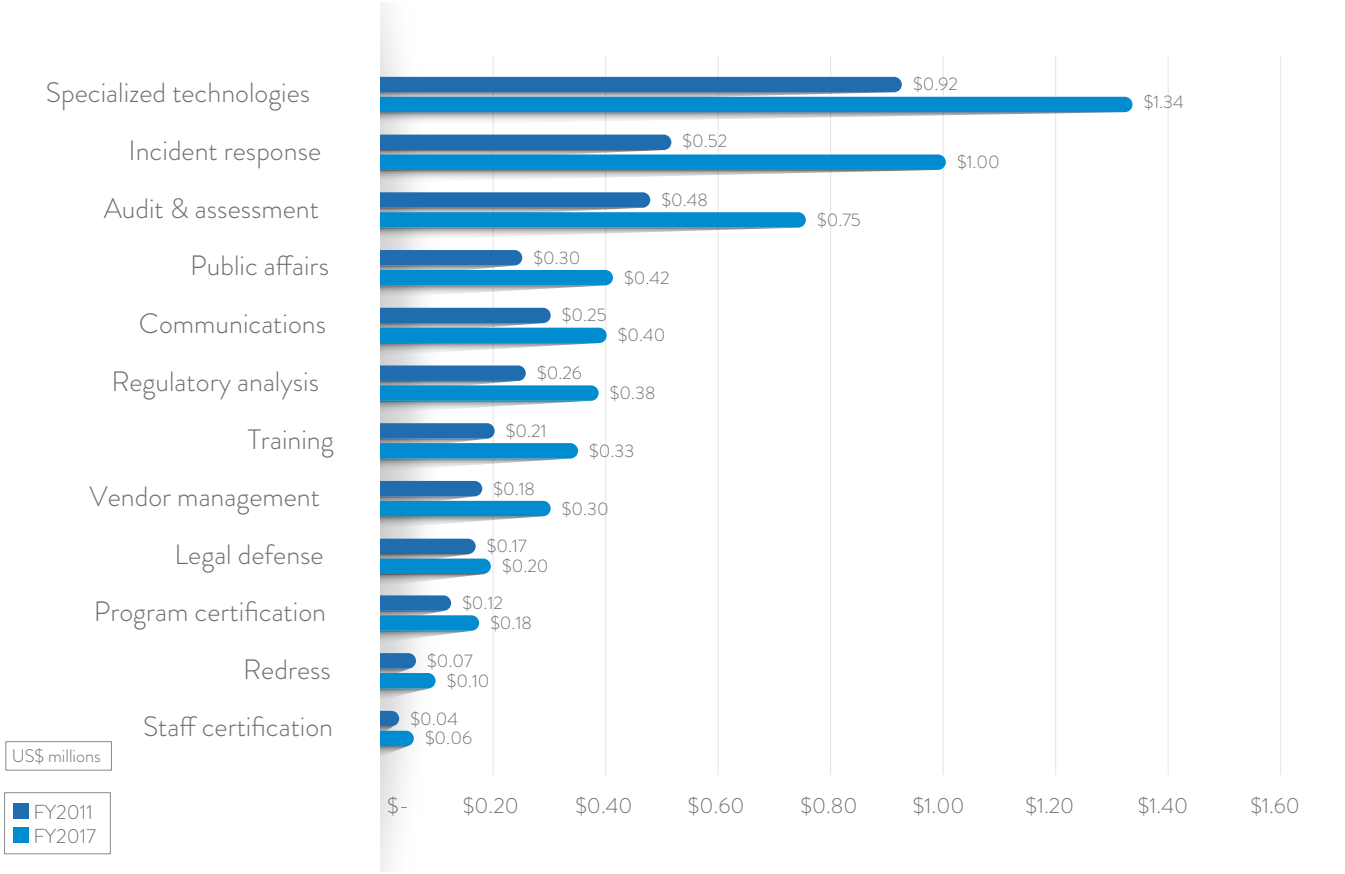
Table 1. Key statistics on the cost of compliance for six activity centers

Activity centers	Average	Median	Maximum	Minimum
Policy	$399,601	$296,032	$583,421	$0
Communications & training	$378,590	$289,669	$1,711,992	$45,600
Program management	$673,010	$530,219	$3,305,664	$89,104
Data security*	$2,010,800	$1,359,257	$6,592,051	$287,556
Forensics & monitoring	$1,089,455	$832,145	$6,241,897	$356,212
Enforcement	$917,703	$663,839	$7,126,414	$106,000
Overall	$5,469,159	$3,971,161	$21,561,439	$1,431,425

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

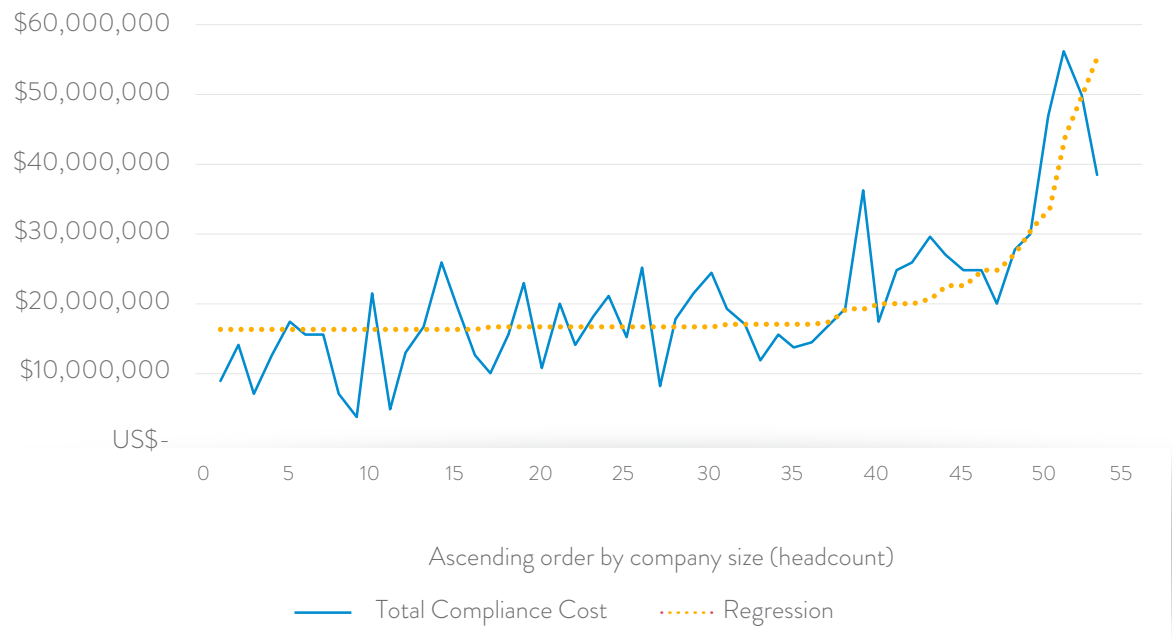
Companies invest most in compliance-related technologies and incident response. The following two figures show the average compliance cost activities for 53 organizations. As shown in Figure 3, compliance costs relating to compliance technologies and incident response represent the two largest expenditure categories. This chart also shows an increase in the amount spent on all expense categories. Between 2011 and 2017, the amount spent on technologies increased by 36 percent, and the amount spent on incident response increased by 64 percent.

Figure 3. Compliance costs by expense categories
Computed from 53 benchmarked companies



Organizational size affects total compliance costs. Figure 4 shows total compliance cost, which is the combination of compliance cost and non-compliance cost, for 53 benchmarked organizations. The chart and regression line reveals a strong linear relationship between size and cost.

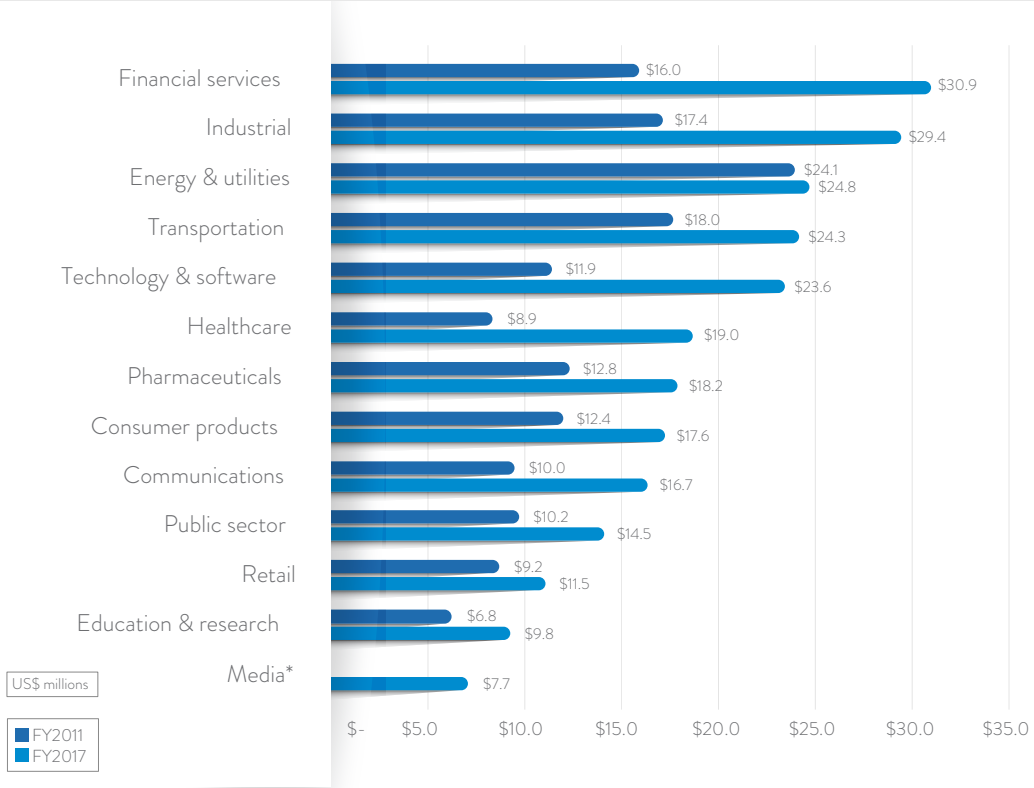
Figure 4. Total compliance cost by organizational headcount (size)
Computed from 53 benchmarked companies



Compliance costs increase the most for financial services and industrial companies. Figure 5 provides total compliance cost for 13 industries 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 $30.9 million in financial services to a low of $7.7 million for media companies. It is also important to note that total compliance cost for each industry segment increased between 2011 and 2017.

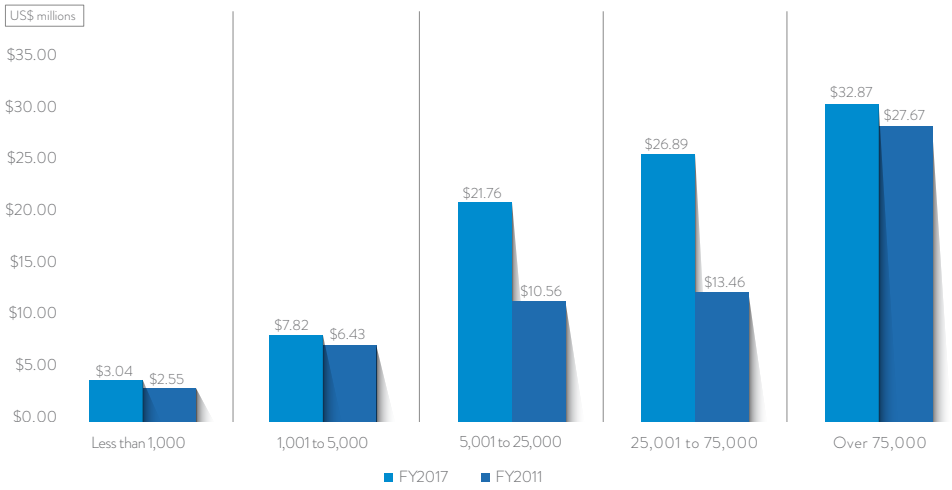
Figure 5. Total compliance cost by industry

*Computed from 53 benchmarked companies | *2011 data is not available*



Larger companies have higher compliance costs. Figure 6 reports the average total compliance costs by the approximate global headcount (size) of benchmark companies. As seen here, total compliance costs increase by organizational size in 2011 and 2017.

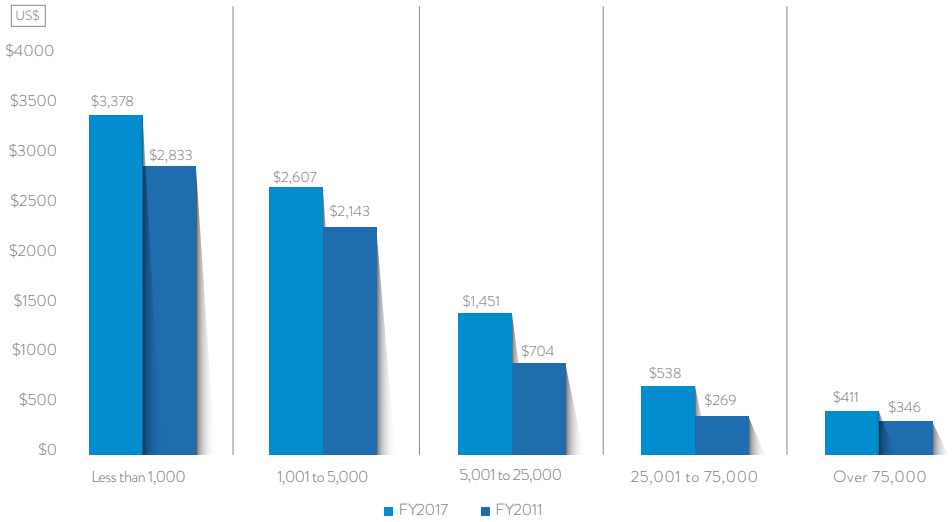
Figure 6. Total compliance cost by headcount
Computed from 53 benchmarked companies



Smaller organizations have higher per capita costs of compliance. Figure 7 provides an analysis of total compliance cost on a per capita basis. When adjusted by headcount (size), compliance costs are highest for organizations with fewer than 1,000 employees and smallest for organizations with 75,000 or more employees.

This result may be explained in part by economy of scale, wherein larger companies have access to leading data protection technologies and highly skilled personnel who have expertise in data protection laws and regulations. Organizations with fewer than 5,000 employees have to rely on expensive external resources such as consultants and lawyers to meet compliance requirements on a global scale.

Figure 7. Per capita total compliance cost by global headcount (size)
Computed from 53 benchmarked companies



THE COST OF NON-COMPLIANCE

Business disruption and productivity loss are the highest costs for non-compliance. 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.

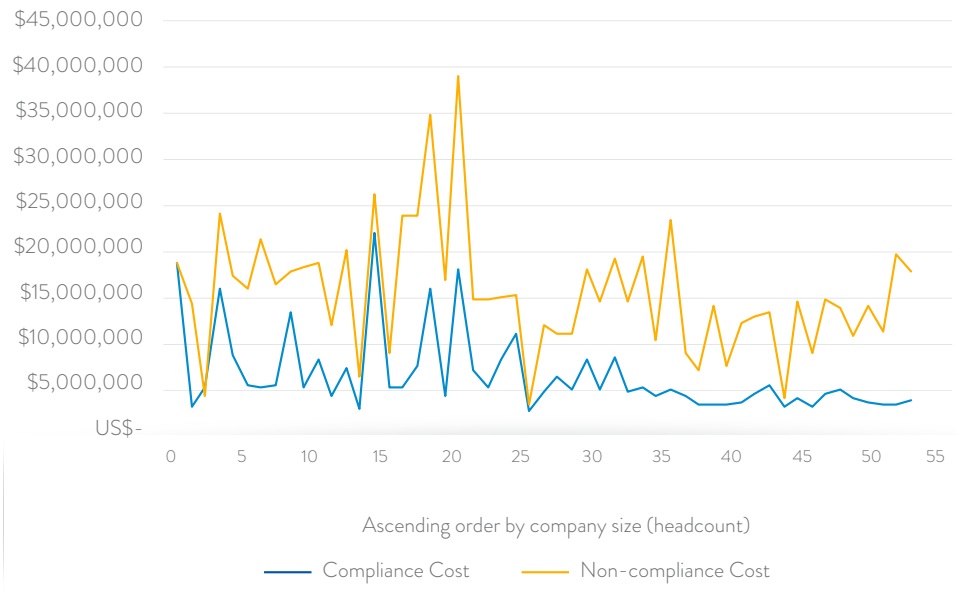
Table 2. Key statistics on the cost of non-compliance for four activity centers

Non-compliance cost consequences	Average	Median	Maximum	Minimum
Business disruption	$5,107,206	$4,232,786	$20,396,716	$1,100,745
Productivity loss	$3,755,401	$4,667,300	$17,336,500	$997,600
Revenue loss	$4,005,116	$3,995,194	$19,176,931	$ –
Fines, penalties & other	$1,955,674	$1,100,500	$5,301,500	$ –
Overall	$14,823,397	$13,995,780	$39,223,575	$2,200,868

Companies are not spending enough on core compliance activities. Figure 8 shows compliance, non-compliance and total compliance costs for 54 organizations. The range for compliance cost is $0.58 million to $21.56 million. The range for non-compliance cost is $2.20 million to $39.22 million. As seen here, in all but two cases, non-compliance costs exceeded compliance costs.

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 such as audits, enabling technologies, training, expert staffing and more, they would experience a more than commensurate reduction in non-compliance cost.

Figure 8. Compliance and non-compliance costs
Computed from 53 benchmarked companies
Figure 8



COMPLIANCE SPENDING AND BUDGET

Figure 9 reports the percentage of compliance spending with respect to the organization's total IT budget. The extrapolated average percentage in 2011 is 11.8 percent. In 2017, the extrapolated average percentage is 14.3 percent.

Figure 9. Percentage of compliance spending to the total IT budget
Computed from 53 benchmarked organizations

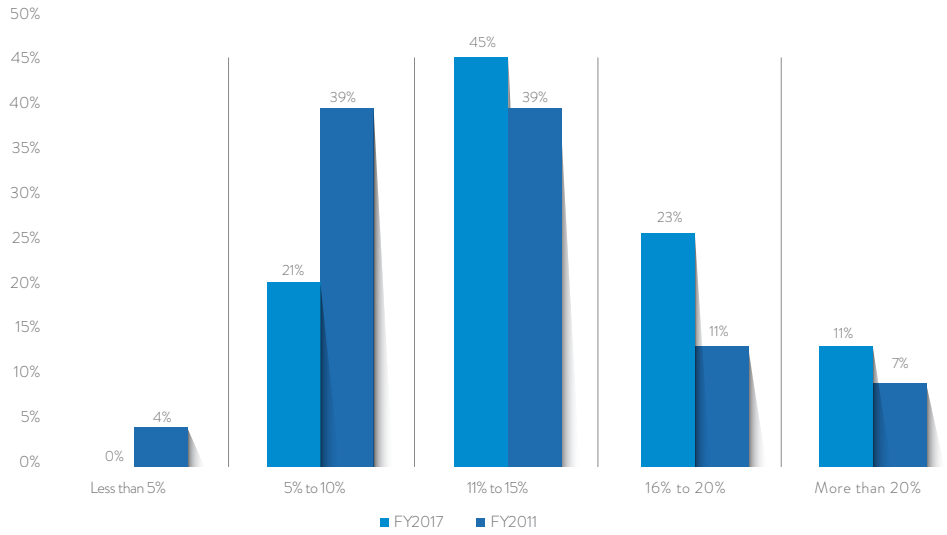
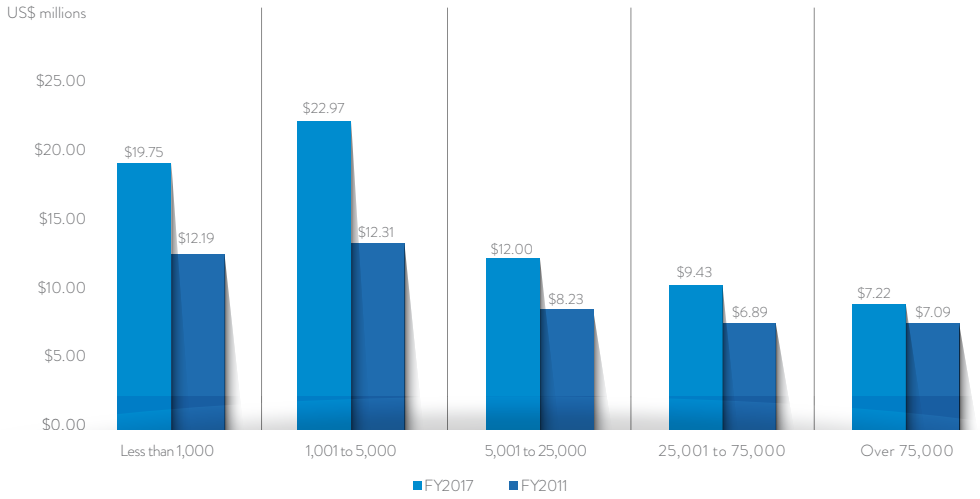


Figure 10 reveals another interesting relationship between compliance spending and non-compliance cost. As shown, non-compliance cost is inversely related to the percentage of compliance spending.

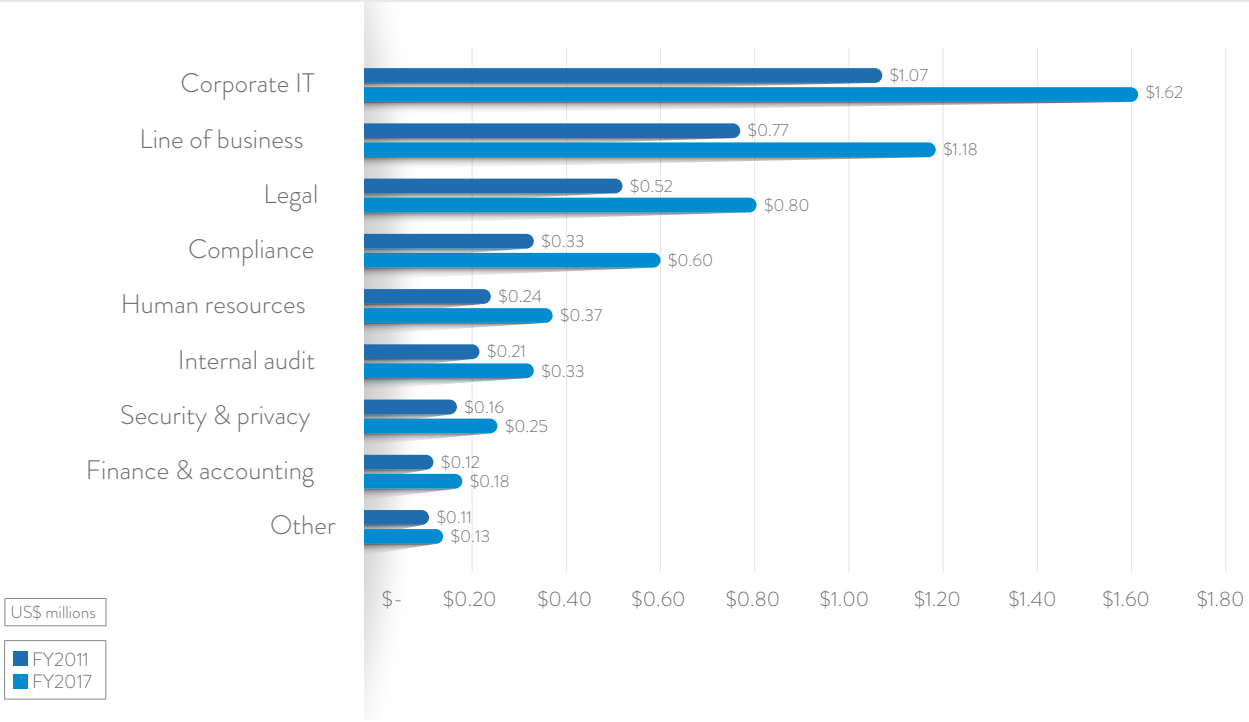
Figure 10. Non-compliance cost by percentage of the IT budget
Computed from 53 benchmarked organizations



THE IMPACT OF GOVERNANCE AND REGULATIONS ON THE TOTAL COST OF COMPLIANCE

Corporate IT, lines of business and legal are most likely to own or influence compliance expenditures relating to data protection and privacy, as shown in Figure 11. It also shows all functions increasing the amount spent on compliance. Here, corporate IT and line of business experienced the highest net increase between 2011 and 2017, at 40 percent and 42 percent, respectively.

Figure 11. Compliance costs by functional area
Computed from 53 benchmarked companies

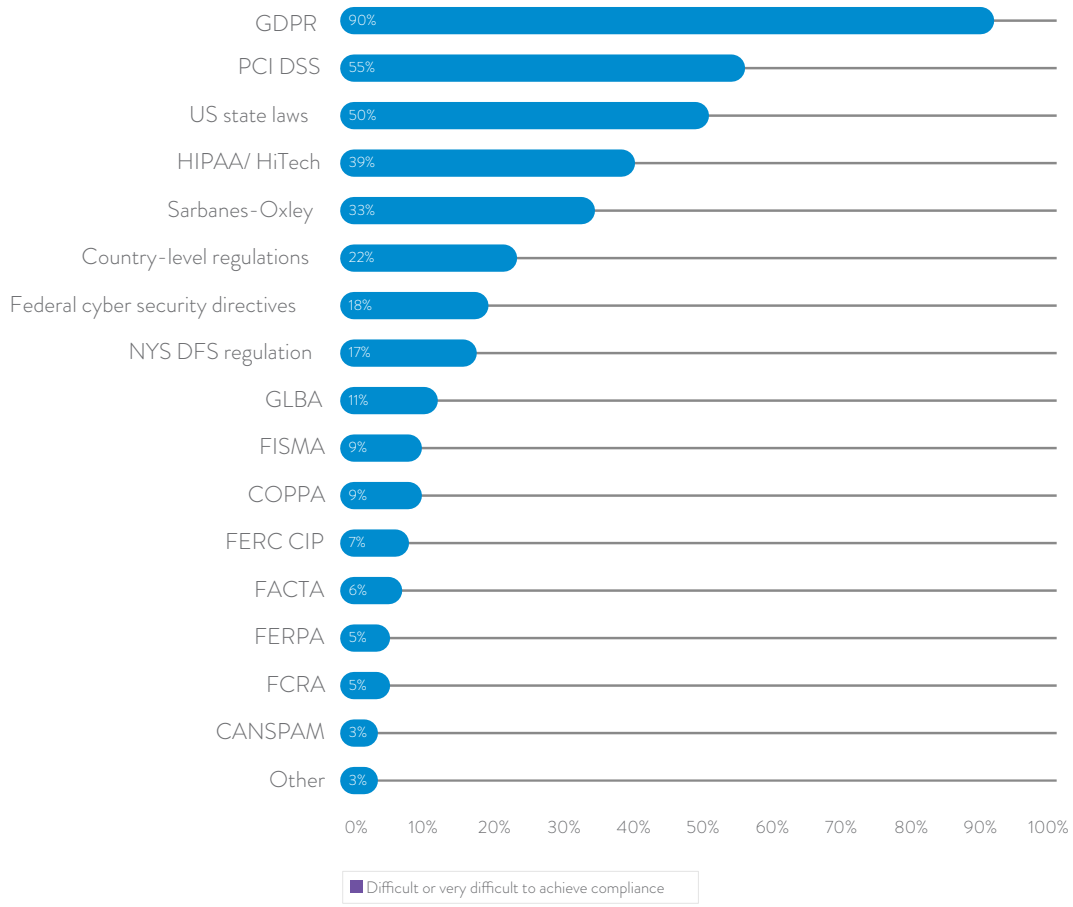


Compliance with GDPR is considered difficult to achieve. This analysis concerns how 237 respondents in our sample of 53 benchmarked organizations view different data compliance regulations in terms of importance and difficulty. Clearly, certain regulations are specified by industry (such as HIPAA, GLBA, FISMA).

PCI DSS, various US state data breach or privacy laws, Sarbanes-Oxley and country-level regulations are also viewed as difficult or very difficult to meet compliance requirements.

Figure 12 shows that 90 percent of respondents view GDPR compliance as the most difficult to achieve.

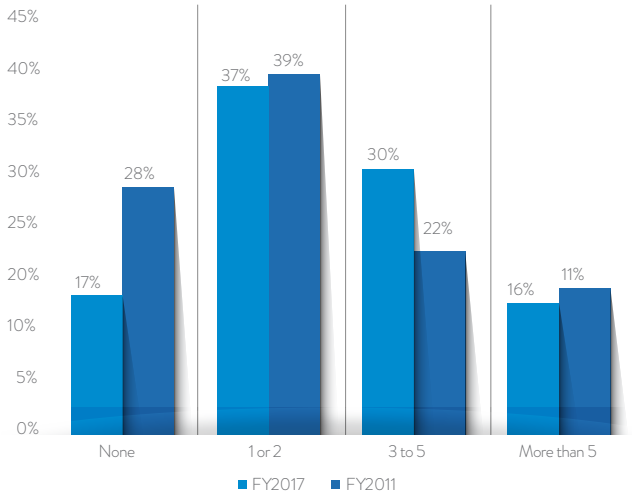
Figure 12. Regulatory compliance requirements difficult to achieve
Computed from 53 benchmarked organizations



MOST COMPANIES CONDUCT ONE OR MORE COMPLIANCE AUDITS ANNUALLY

Figure 13 reports the annual internal compliance audit frequency of participating benchmark companies.[3] The pattern of response for 2011 and 2017 is generally consistent. In 2011, a total of 72 percent (100%-28%) of companies said they conduct data compliance audits one or more times each year (or an average of 2.2 audits). In 2017, a total of 83 percent (100%-17%) of companies said they perform data compliance audits each year (or an average of 2.9 audits).

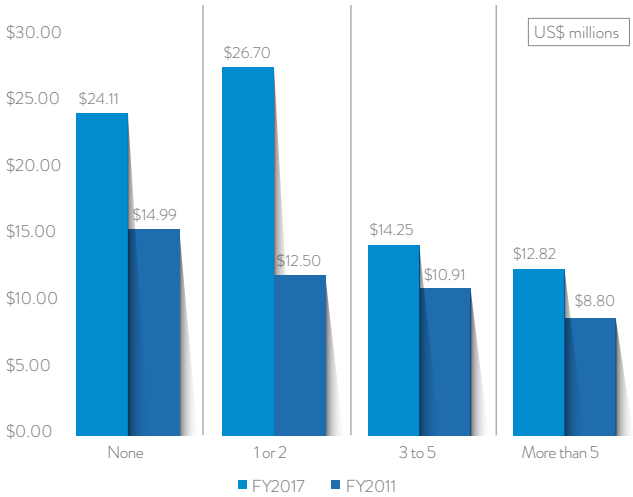
Figure 13. Internal audit frequency
Computed from 53 benchmarked organizations



MORE COMPLIANCE AUDITS REDUCE THE COST OF COMPLIANCE

Figure 14 shows the inverse relationship between total compliance cost and internal audit frequency. As can be seen, organizations that conduct five or more internal compliance audits per year have the lowest total compliance cost in both 2011 and 2017. The highest total compliance cost in the current study ($26.7 million) pertains to organizations that conduct one or two internal compliance audits per year.

Figure 14. Total compliance cost by audit frequency
Computed from 53 benchmarked organizations



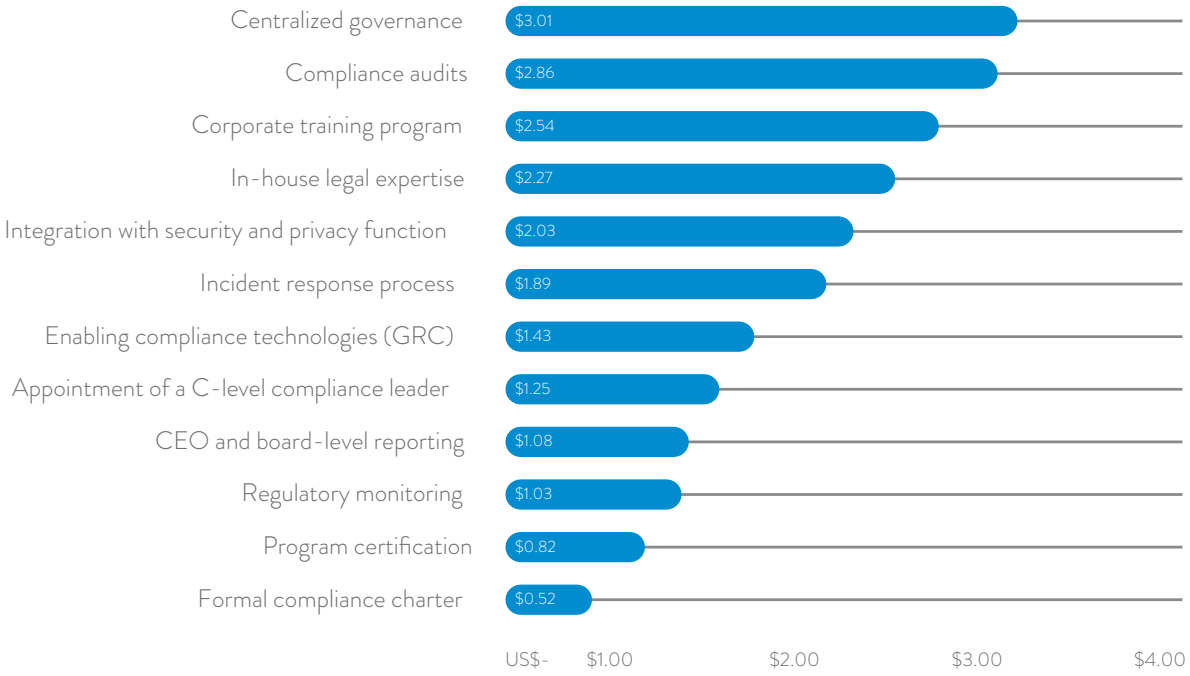
CENTRALIZED GOVERNANCE AND AUDITS REDUCE TOTAL COMPLIANCE COSTS

Figure 15 summarizes the incremental cost savings resulting from the implementation of 12 best practices.

For example, the deployment of a centralized data governance program reduces total compliance cost by $3.01 million. Similarly, conducting compliance audits reduces total compliance costs by $2.86 million. Other best practices that are cost saving include corporate training programs, in-house legal experts, integration of security and privacy functions and a fully functional incident response process.

Figure 15. Twelve best practices that reduce total compliance costs

Computed from 53 benchmarked organizations



THE IMPACT OF SECURITY POSTURE ON THE COST OF COMPLIANCE

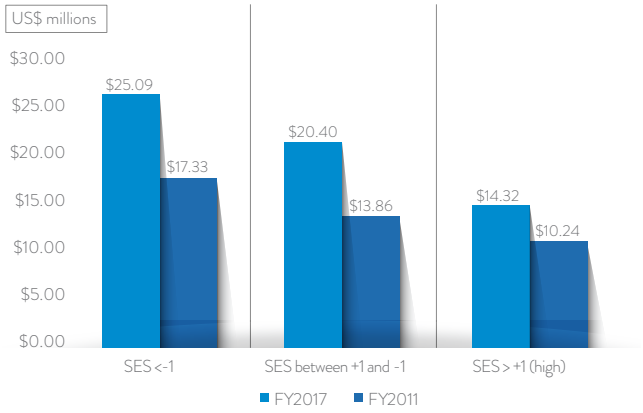
In this benchmark study, we utilize an indexing methodology known as the Security Effectiveness Score (SES) to measure an organization's ability to meet reasonable security objectives.[4] Recent research shows that the higher the SES index, the more effective the organization is in protecting information assets and critical infrastructure.

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 -1.60 to a high of +1.73, with a mean value at +.21. In the 2011 study, the lowest score was -1.67, the highest score was +1.69 and the mean SES was +.18.

As with prior Ponemon Institute research, we measured the security posture of participating organizations as part of the benchmarking process for this study. Figure 16 reports the total compliance cost in ascending order by SES. This graph clearly shows an inverse relationship between effectiveness score and compliance cost. Specifically, companies with an SES above +1 have the lowest total compliance cost. Companies with an SES below -1 have the highest total compliance cost.

Figure 16. Benchmark sample in ascending order by SES

Computed from 53 benchmarked companies



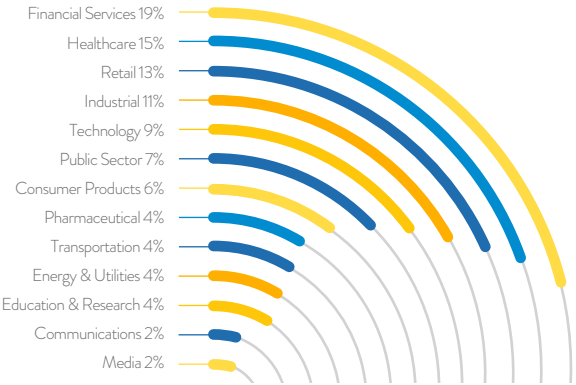
PART 3

SAMPLE OF PARTICIPATING ORGANIZATIONS

Pie Chart 1. Industry classification of the benchmark sample

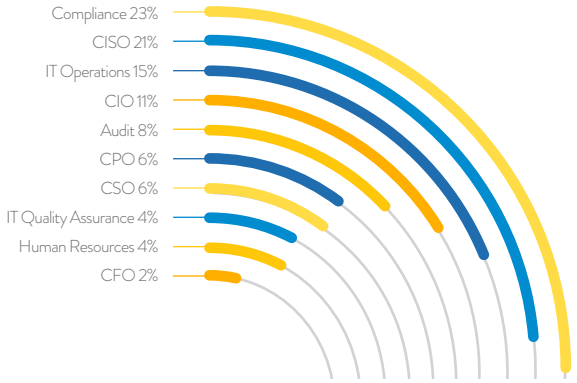
Computed from 53 benchmarked companies

Pie Chart 1 reports the percentage of companies by industry that participated in the benchmark study. Our final sample includes a total of 53 organizations, which serves as the unit of analysis. As previously mentioned, a total of two organizations were rejected from the final sample for incomplete responses to interview questions or survey responses. As shown, financial services, healthcare and retail organizations represent the three largest segments.



Pie Chart 2. Participating respondents by their approximate job function or title

Computed from 237 separate interviews



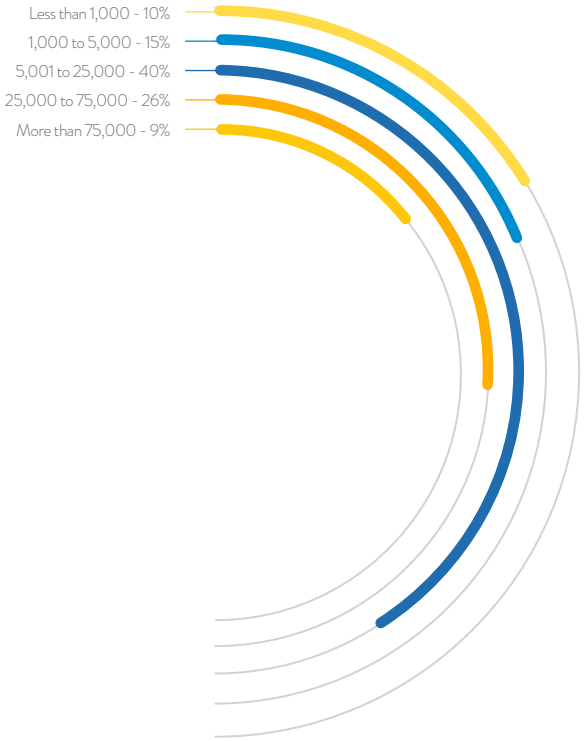
Pie Chart 2 reports the approximate job functions or titles of participants who completed the diagnostic interview. In total, 237 individuals with responsibility for data protection compliance activities were engaged in the benchmark research process.

Pie Chart 3. Distribution of participating organizations by global headcount

Computed from 53 benchmarked companies

On average, benchmark methods required four or five interviews to capture enough information to extrapolate compliance and non-compliance costs. As seen in Pie Chart 1, respondents in information security, compliance, and IT operations represent the top three functional areas participating in these diagnostic interviews.

Pie Chart 3 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 surrogate for organizational size in this research.



PART 4

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 16 attributes have the strongest correlation to creating an effective security posture while meeting data compliance goals of an organization. These attributions from the security effectiveness score (SES) instrument have the highest negative correlation to non-compliance cost as compiled from 53 benchmark companies. This means that these attributes are most supportive of a strong compliance culture.

- Monitor and strictly enforce security policies
- Conduct audits or assessments on an ongoing basis
- Attract and retain highly skilled security personnel
- Provide company-wide training and awareness activities
- Minimize downtime or disruptions to business processes
- Prevent or curtail malware or non-malware attacks
- Measure the effectiveness of the data security program
- Ensure security program is consistently managed
- Know where sensitive or confidential information resides
- Secure all endpoints to the network (including IoT devices)
- Implement strong identity and authentication processes
- Reduce data clutter, especially unstructured data assets
- Develop a data compliance governance strategy
- Develop a communication channel to the CEO and board
- Obtain C-level support for data compliance and privacy
- Create and test an incident response process

Essential to achieving substantial compliance goals requires holistic and integrated security solutions that ensure every aspect of the organization is covered and protection works seamlessly. 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 challenges 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 challenges that affect all organizations. They are: 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 will help organizations succeed in aligning their core practices and technologies across the enterprise in ways that minimize the risk of compliance failure. Following are security challenges and how to respond to them:

- External and internal security threats
  Changing threats requires an organization to do the following: make security an integral part of its culture; keep pace with technological advances; "design-in" security in business processes to "design-out" compliance risks; understand the latest threats and actively assess the insider threat.
- The changing workforce
  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 whether remote workers are securely accessing the network.
- Changing business models and processes
  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.
- Change the world
  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.

What are the implications for an organization that does not have the right integrated and holistic response to data security and related compliance challenges? The consequence of not managing compliance risks include a loss of trust that will jeopardize customer loyalty, and the inability to deliver services and products causing revenues to decline.

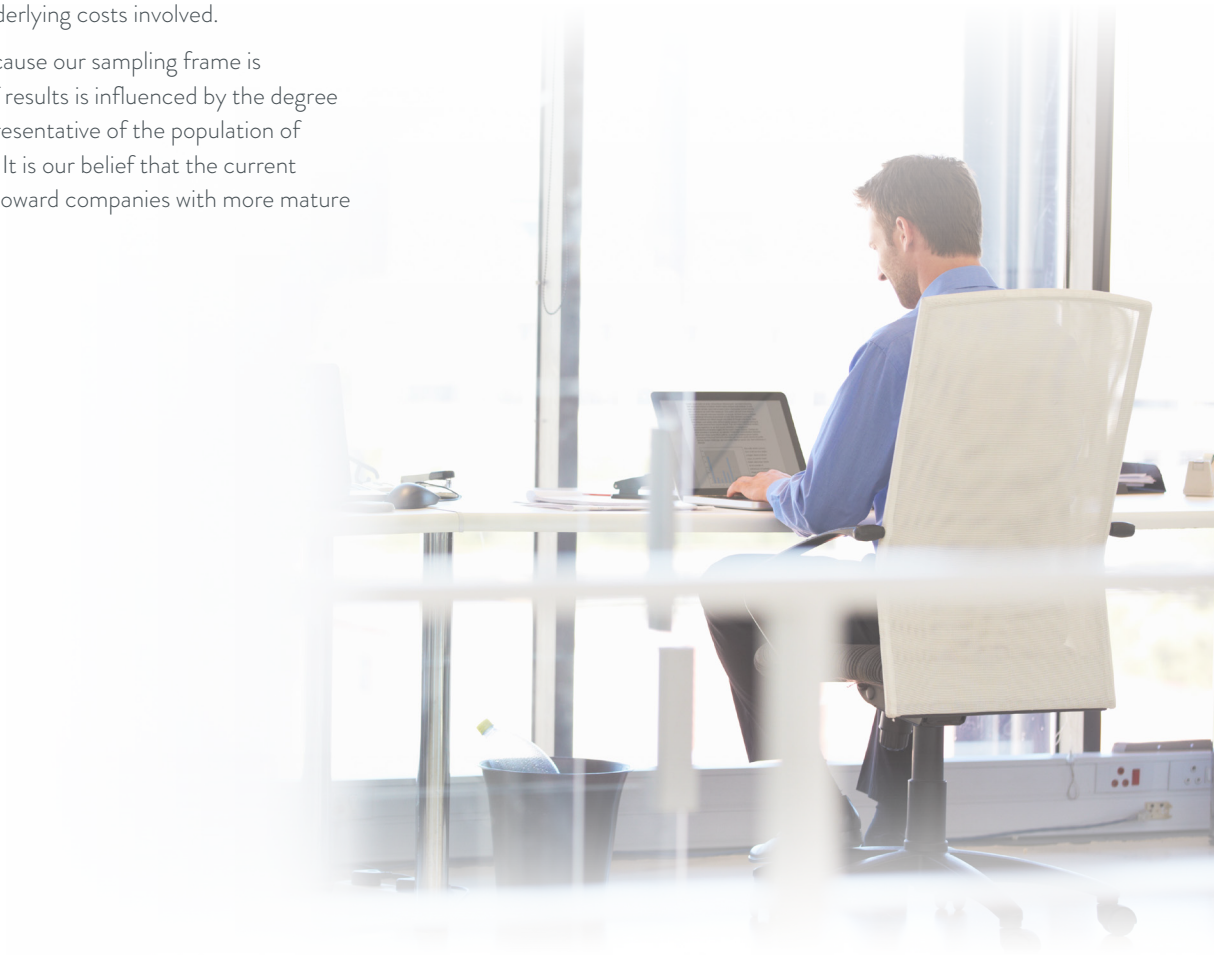
Beyond the economic impact, non-compliance increases the risk of losing valuable information assets such as intellectual property, physical property and customer data. Further, non-compliant organizations risk becoming victims of cyber fraud, business disruption, and many other dangers that might cause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

We believe our study demonstrates that an investment in both external and internal compliance activities is beneficial not only to the security but also to the overall operations of an organization. By investing in compliance activities, we have shown that organizations reduce the risk created by non-compliance. By considering the above practices, organizations can enjoy better compliance 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. Fifty-three 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.



PART 5

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 allocate detailed cost data into discernible activity centers that explain the entire data protection and compliance mandate within benchmarked companies.[5] We determined that the following six cost activity centers explain the full economic impact of compliance costs associated with data protection. Within each center, we compile the direct and indirect costs associated with each activity.

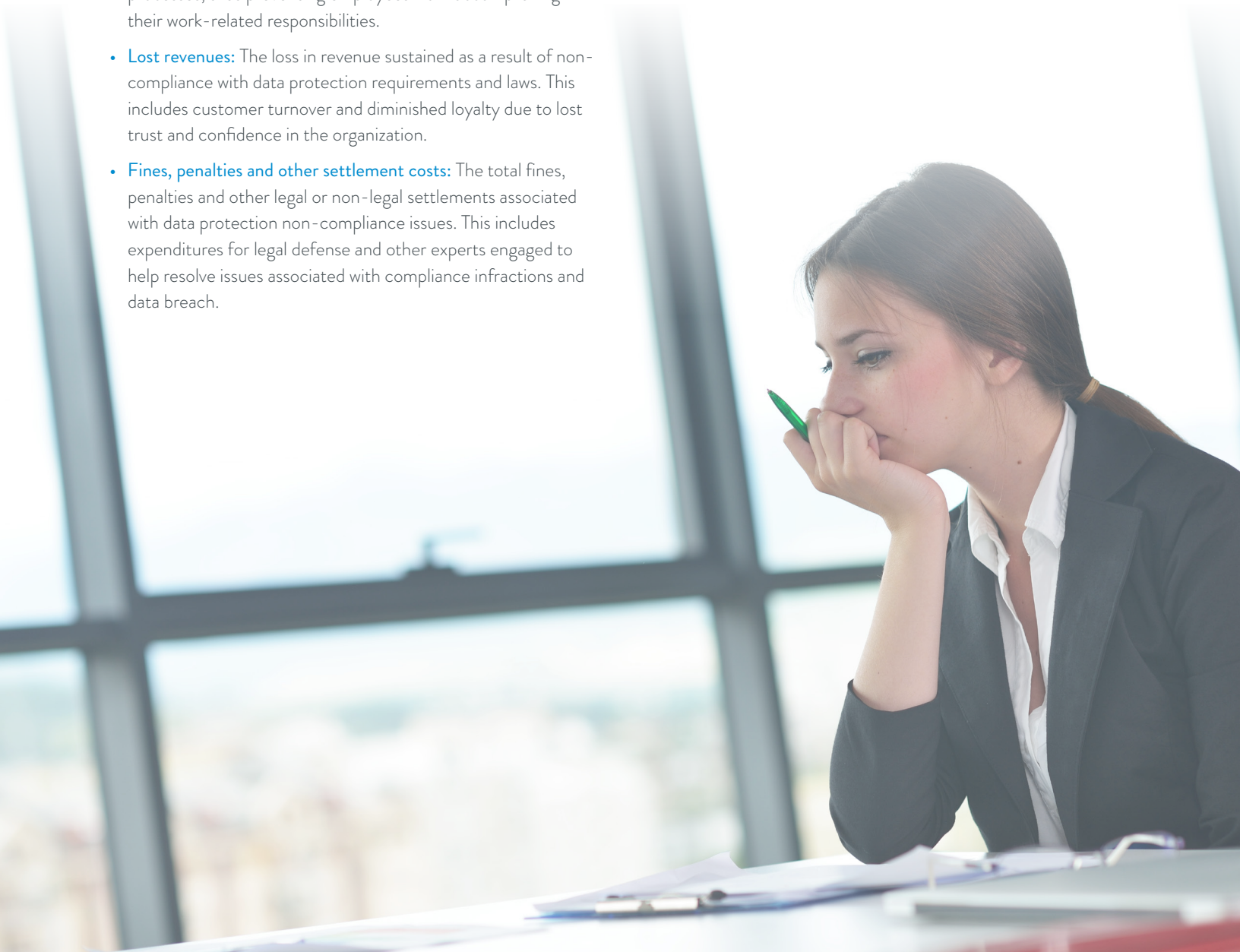
- Data compliance policies: Activities associated with the creation and dissemination of policies that pertain to the protection of confidential or sensitive information such as customer data, employee records, financial information, intellectual properties and others.
- Communications: Activities and 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 that relate to the coordination and governance of all program activities within the enterprise, including direct and indirect costs relating 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, verification programs, professional audit staffing, audit technologies and others.
- Enforcement: Activities that relate to the detection of non-compliance, including incident response. It also includes 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 lost time and related expenses associated with the downtime of systems and other critical processes, thus preventing employees from accomplishing their work-related responsibilities.
- 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 legal defense and other experts engaged to help resolve issues associated with compliance infractions and data breach.

We used an activity-based costing framework, which consists of six discernible cost center activities termed "compliance costs" and four discernible cost consequences termed "non-compliance costs." As shown, the six compliance costs are policy, communications, program management, data security, compliance monitoring and enforcement.

Each one of these activities generates direct, indirect and opportunity costs. The consequences for failing to comply with data compliance requirements include business disruption, productivity losses, revenue losses and fines, penalties and other cash outlays. Both sets of costs comprise the total cost of compliance, which is compiled for each benchmarked organization.



APPENDIX

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 160 functional leaders in benchmarked organizations participating 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 descriptive cost for each one of the six cost activity centers. Within each activity center, the survey requires respondents to estimate the cost range to signify direct cost, indirect cost and opportunity cost, 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 and auditing
- 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, we extrapolated the costs incurred by each organization either directly or indirectly 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 as defined in the above.

The benchmark framework presents the two separate cost streams used to measure the total cost of data compliance for each participating organization. These two cost streams pertain to cost center activities and after-the-fact 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 rather than a point estimate to preserve confidentiality (in order to ensure a higher response rate). Second, the survey requires participants to provide a second estimate for both indirect cost and opportunity cost, separately. These estimates are calculated based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we conduct a follow-up interview to validate the reasonableness of cost estimates provided by respondents (and 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 focusing on process yields a higher response rate and better quality of 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 compliance costs rather than all IT compliance costs. Based on discussions with learned experts, the final set of items focus on a finite set of direct or 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 April 2017 and fieldwork concluded in September 2017. The recruitment started with a personalized letter and a follow-up phone call to 209 organizations for possible participation in our study. While 71 organizations initially agreed to participate, 53 organizations permitted researchers to complete the benchmark analysis.

The time horizon used in the analysis of data compliance costs is a 12-month period. We collected information over approximately the same time frame; hence, this limits our ability to gauge seasonal variation on specific cost categories.

SOURCES

1. See: Cost of Compliance: Benchmark Study of Multinational Organizations (sponsored by Tripwire), Ponemon Institute January 2011.
2. The percentage net change calculation is defined as follows: (FY2017–FY2011) ÷ [(FY2017+FY2011)×½].)
3. Please note that all audits examined in this analysis were all internally conducted either by in-house or contract (outsourced) staff.
4. Ponemon Institute initially developed the Security Effectiveness Score 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 leading information security and data protection practices. This indexing method has been validated from more than 50 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.
5. Ponemon Institute's cost of data breach studies conducted over the past 12 years utilizes activity-based cost to define the total economic impact of data loss or theft that requires notification. See, for example, 2017 Cost of Data Breach, (sponsored by IBM) Ponemon Institute May 2017.