



The State of Privacy & Data Security Compliance

Sponsored by Sophos

Independently conducted by Ponemon Institute LLC

Publication Date: November 30, 2009

The State of Privacy and Data Security Compliance

Prepared by Larry Ponemon, November 30, 2009

I. Executive Summary

We are pleased to present *The State of Privacy and Data Security Compliance* study conducted by Ponemon Institute and sponsored by Sophos. The purpose of the study is to determine if various international, federal and state data security laws improve an organization's security posture. What is the value of compliance and does it correlate with the value of the compliance effort?

With the plethora of new privacy and data security regulations, we believe it is time to ask whether regulations help or hinder an organization's ability not only to protect sensitive and confidential information assets, but to be competitive in the global marketplace. Further, how difficult is it to be in compliance, who is the typical person or functional leader accountable for compliance? What is the value to the organization? Finally, what differences (if any) exist in security practices between compliant and non-compliant organizations?

We surveyed 528 IT and security practitioners (referred to as respondents) who are involved in their organization's data security efforts, which can include responsibility for the technologies that support compliance efforts and managing and/or auditing legal and regulatory requirements.

Sixty-seven percent of all respondents say they have at least an adequate knowledge about the many U.S. states, federal and international privacy and data security laws that their organizations are required to comply with today. More than 52 percent of respondents are at or above the manager levels with an average of almost 10 years experience in the IT or security fields.

Our sample of respondents was bifurcated into two groups – namely, 52 percent who reported their organizations have achieved substantial compliance with privacy and data security laws and 48 percent who admit their organizations have not achieved substantial compliance with all applicable laws.

Respondents in both the compliant and non-compliant groups represent various vertical industries, including financial services, retail, technology, healthcare and many others. Based on the results of our study, compliance with privacy and data security regulations appears to have a very favorable impact on an organization's security posture.

Specifically, the probability of a data breach occurrence that required notification to breach victims decreased by almost one-half as a result of better compliance efforts. Furthermore, organizations achieving a higher level of compliance reap a financial gain as measured by the reduction in cost associated with data breach.¹ Respondents in the compliant group believe the top two technologies that give them an advantage in managing risks are data loss protection and encryption of laptops and desktops.

Compliance also makes a difference in the attitudes and beliefs of respondents about their organization's security compliance efforts. Accordingly, respondents in the compliance group believe they are more likely to achieve the following benefits:

- Improves their organization's relationship with key business partners.
- Helps secure more funding for IT security.
- Improves their organization's security posture.²

¹ The average data breach cost of \$6.65 million is used to determine cost savings resulting from compliance. This is taken from the [Fourth Annual Cost of Data Breach Study](#) published by Ponemon Institute (01/2009).

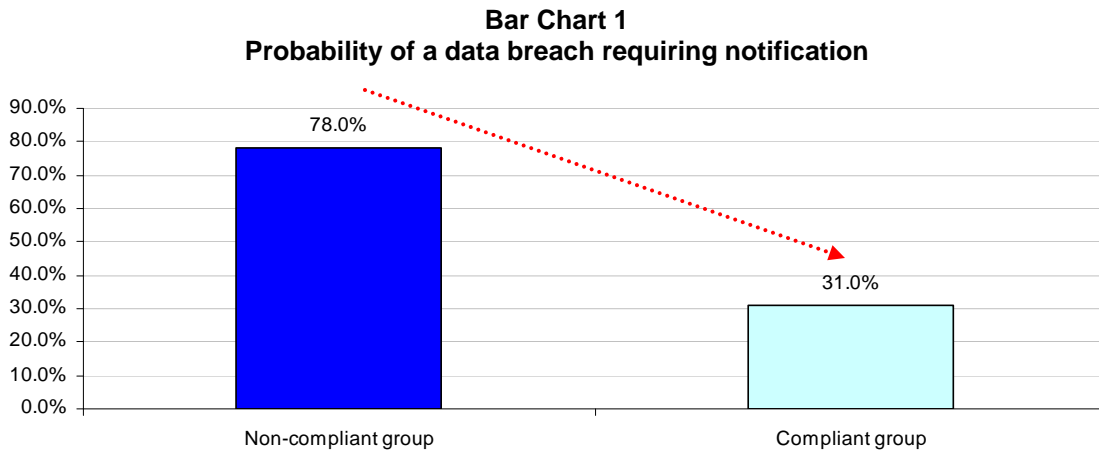
² Security posture is defined as an organization's ability to defend itself against insider and external threats. Such threats include the theft of information assets and attacks on an organization's critical infrastructure.

II. Key Findings

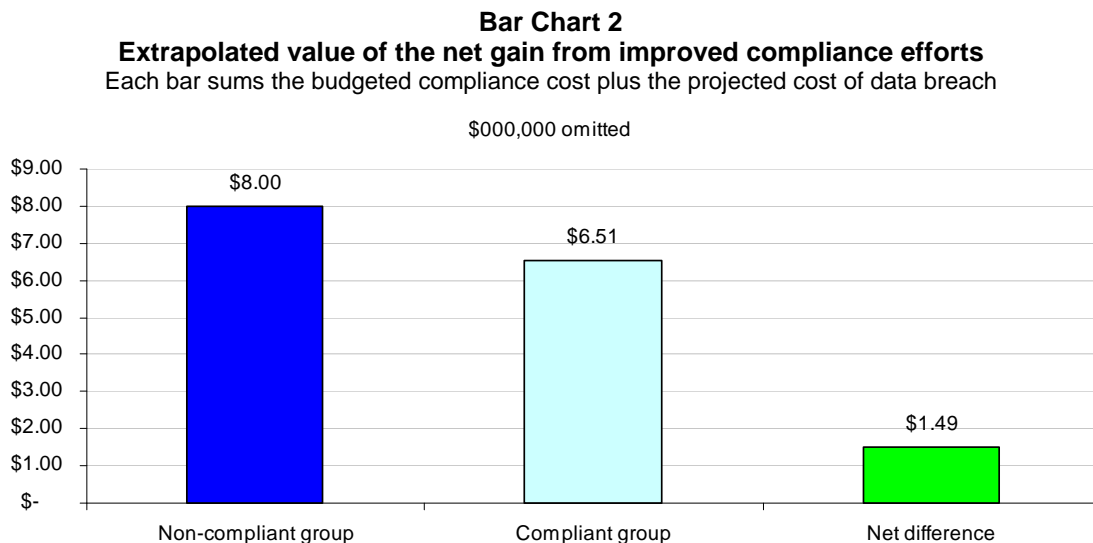
Following are the most salient findings of this survey research. The actual data utilized in each figure and referenced in this paper can be found in Appendix 1.

Investment in compliance reduces the occurrence and cost impact of a data breach.

Compliance is not cheap but it does significantly reduce the probability of a data breach as shown in Bar Chart 1. The computed probability of a data breach occurrence that requires notification for the non-compliant group in a one-year time frame is 78 percent.³ For the compliant group, the computed probability is only 31 percent. Clearly, this 47 percent difference suggests better compliance efforts reduce the incidence of serious data breaches in participating organizations.



Using the probabilities of occurrence and the average organizational cost of a data breach at \$6.65 million from previous research (see footnote 1), we calculate the net gain resulting from improved compliance efforts as a \$1.49 million difference between the two groups.

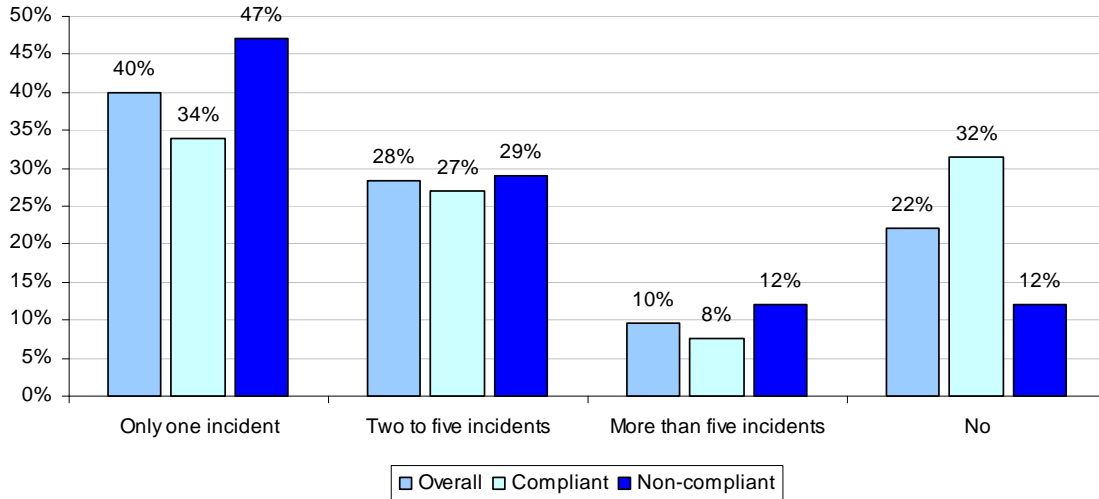


³ The probability of occurrence is computed from two survey questions about the frequency of data breach and the frequency of those incidents requiring notification. In total, 54 percent of respondents say their organizations experienced one or more data breaches requiring notification to breach victims.

Compliant organizations have fewer data breaches.

Bar Chart 3 shows the data breach experience of both the compliant and non-compliant groups of respondents. Thirty-two percent of the compliant group versus 12 percent of the non-compliant group did not have any data breaches. This suggests the technologies and tasks used to achieve compliance can have the positive effect of mitigating the risk of data loss. According to the findings of the study, 88 percent of the non-compliant group had at least one data breach versus 69 percent in the compliant group.

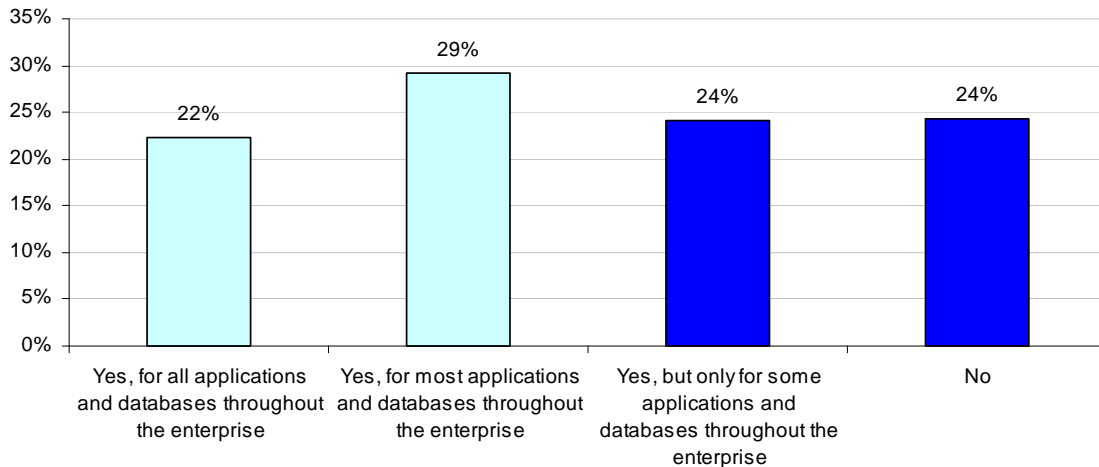
**Bar Chart 3
Data breach experience**



More than half of respondents (52 percent) self-reported their organizations are in substantial compliance with privacy and data security regulations.

We bi-furcated respondents into two groups: compliant and non-compliant based on the response pattern shown in Bar Chart 4. It shows that 52 percent believe their organizations are compliant for all or most applications throughout the enterprise. Forty-eight percent are compliant only for some applications or not at all.

**Bar Chart 4
Compliance profile**



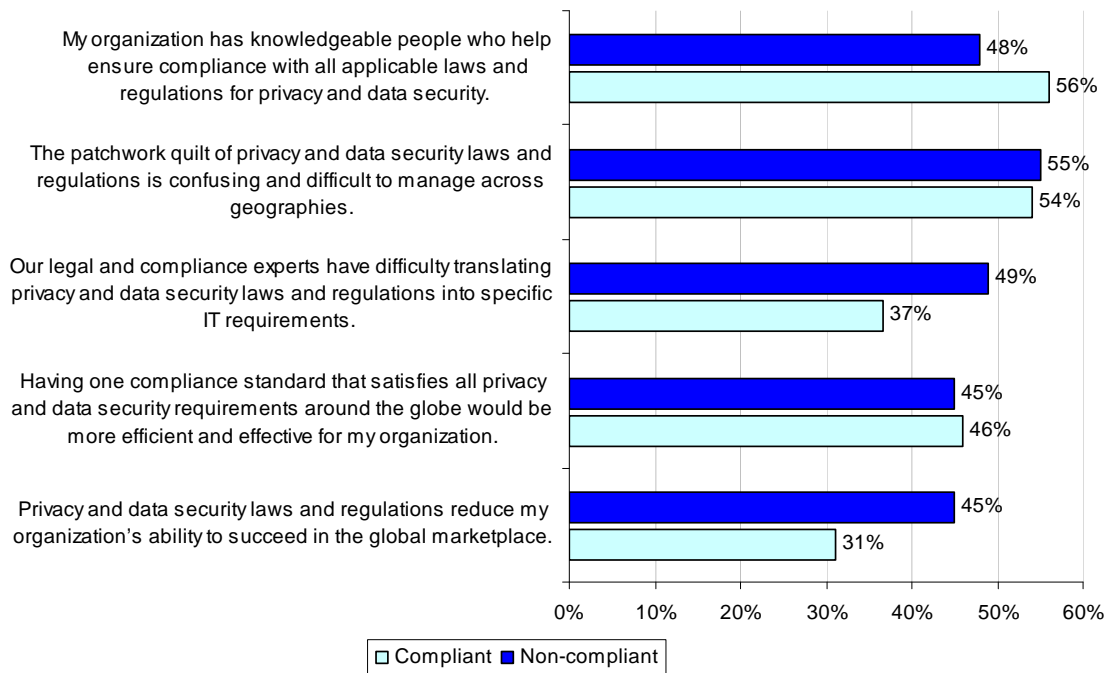
Respondents in the compliant group are more positive about their organization’s ability to deal with regulations and still maintain a competitive stance.

Bar Chart 5 reports the respondents’ perceptions about their organizations’ security compliance posture. In comparison to the non-compliant group, respondents in compliant organizations seem less likely to believe privacy and data security regulations reduce their company’s ability to succeed in the global marketplace.

Respondents in the compliant group also appear to be more confident about their organization’s ability to translate complex privacy and data security regulations into specific IT requirements. In addition, they believe their organizations have the requisite knowledge to achieve compliance with applicable laws and regulations.

It is important to note that both the compliant and non-compliant groups hold similar views about the difficulty in managing the requirements for privacy and data security laws across geographies. However, they do not agree that one global standard for their organization would make it easier to achieve compliance.

Bar Chart 5
Attributions about privacy and data security compliance



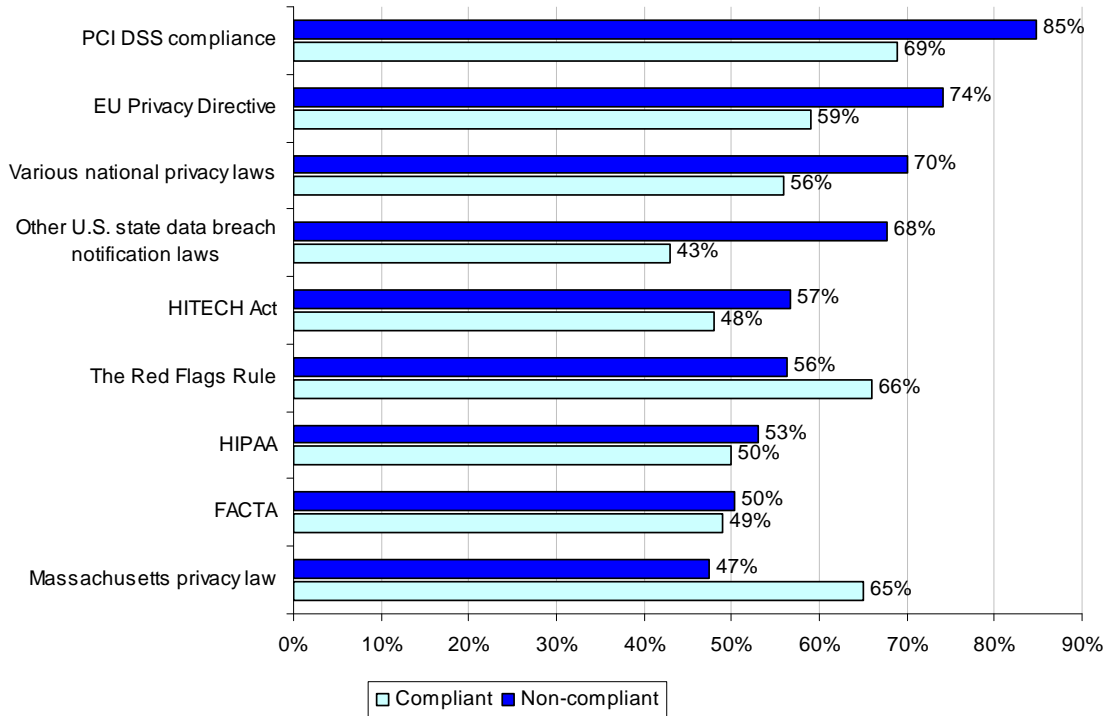
Respondents in the non-compliant group find it difficult to achieve compliance with various regulatory requirements for privacy and data security.

Bar Chart 6 lists major privacy and data security regulatory requirements that apply to many organizations. This chart also shows differences between the compliant and non-compliant group in terms of the relative difficulty in achieving compliance. As shown, PCI DSS, EU Privacy Directive, various national privacy laws, and U.S. state data breach notification laws are viewed as the most difficult to comply with.

The non-compliant group considers compliance as more onerous than those in the compliant group. Especially compliance with U.S. state data breach notification laws, PCI DSS self-

regulatory compliance standards and the European Union Privacy Directive. However, the exception is the Red Flags Rule and the new Massachusetts privacy law. In the case of these two regulations, the compliant group finds it more difficult or very difficult to comply with.

Bar Chart 6
Level of difficulty in achieving compliance
 Each bar reports the combined percentage difficult and very difficult response

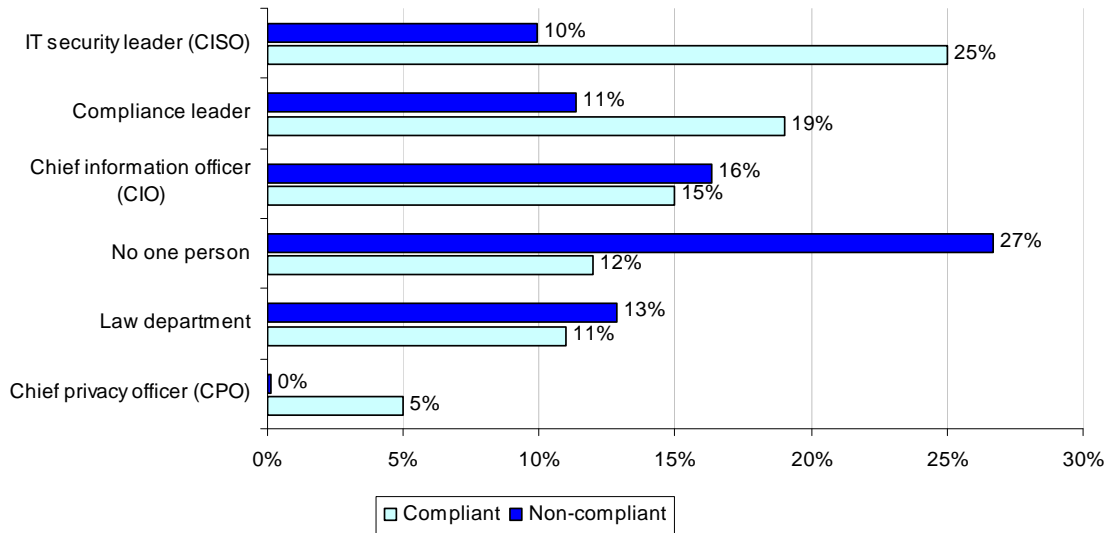


The compliant group is more likely to see the IT security leader (CISO) as the one person responsible for privacy and data security compliance.

Bar Chart 7 below summarizes the functional leaders most responsible for privacy and data security compliance. As can be seen, respondents in the compliant group believe their company’s IT security leader (CISO) is most responsible for overseeing privacy and data security compliance. Others responsible include the organization’s compliance leader and chief information officer (CIO). It is surprising that only a small percentage of respondents see their organization’s privacy officer (CPO) as having overall responsibility for privacy and data security compliance. This finding, however, may be due to the fact that the sample of respondents consists of IT and security practitioners.

The non-compliant group is less likely to recognize one person in their organization as responsible for privacy and data security compliance. This uncertainty could explain why compliance is more difficult to achieve and why this group is less confident that they have the expertise to translate privacy and data security laws and regulations into specific IT requirements.

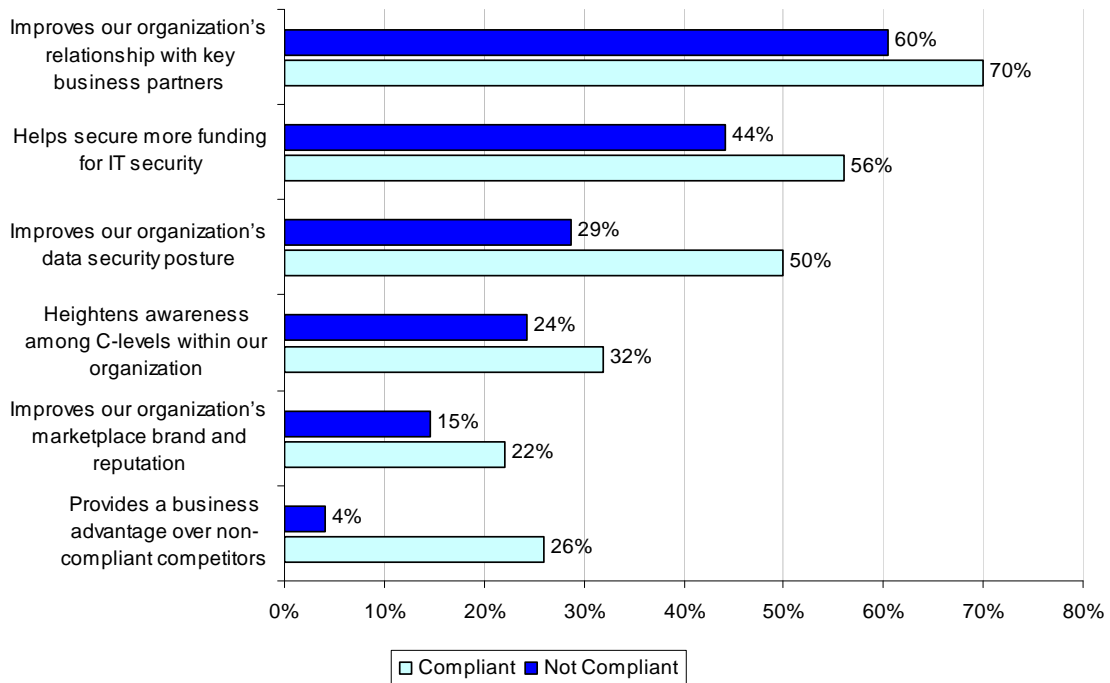
Bar Chart 7
Responsibility for privacy and data security compliance



Privacy and data security regulations are essential to achieving an effective security posture, according to the compliant group.

Bar Chart 8 shows how respondents perceive the value of privacy and data security compliance requirements. Accordingly, the compliant group sees more value in compliance requirements than the non-compliant group.

Bar Chart 8
Value propositions for compliance



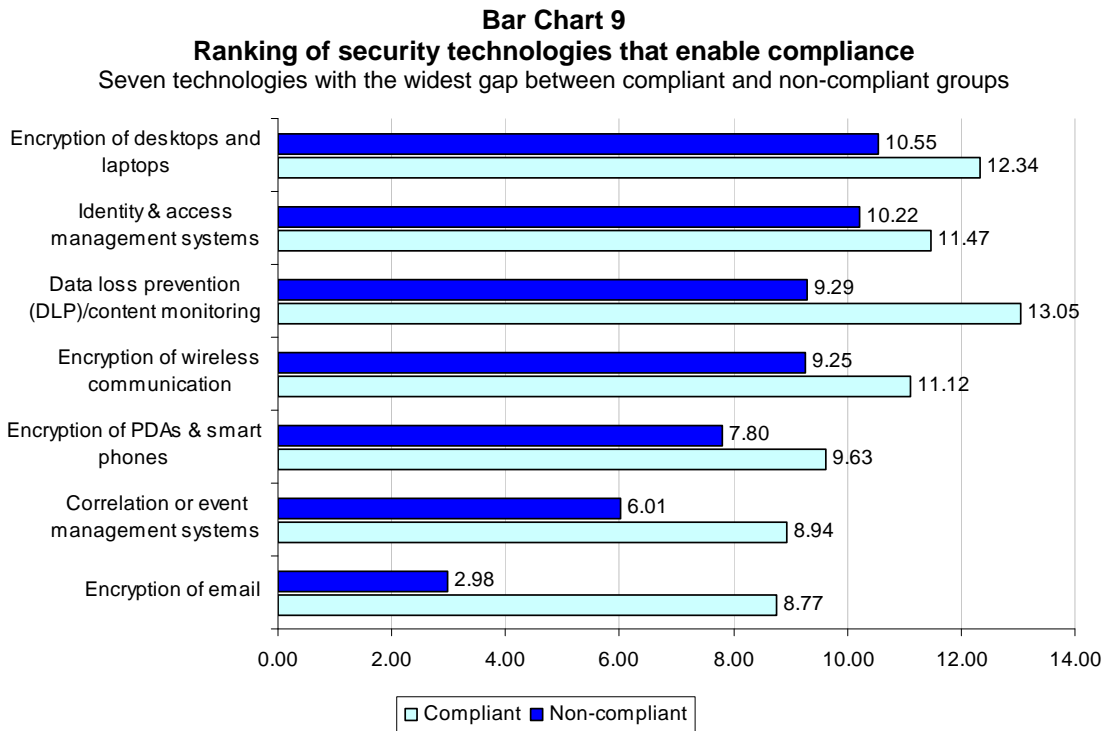
Specifically, respondents in the compliant group believe regulations improve their organization’s relationships with key business partners and data security posture. In addition, respondents see that compliance mandates help to secure more funding for IT security solutions.

The greatest difference between the compliant and non-compliant groups is the belief that compliance provides a business advantage over non-compliant competitors (22 percent difference), followed by the belief that compliance improves the organization’s data security posture (21 percent difference).

DLP technologies and encryption of laptops and desktops are considered by the compliant group to be the most important solutions for achieving compliance.

Bar Chart 9 reports the ranking of different technologies considered important to achieve compliance with privacy and data security regulations. The chart shows seven technologies with the greatest gap between the compliant and non-compliant groups. Please note the higher the percentage the more important the respondents consider the technology to be.⁴

Respondents in the compliant group see data loss prevention and whole disk encryption for desktops and laptops as the most important technologies for achieving compliance with privacy and data security regulations (13.95 and 12.34, respectively). Least important technologies for the compliant group are email encryption and correlation management systems (8.77 and 8.94, respectively).

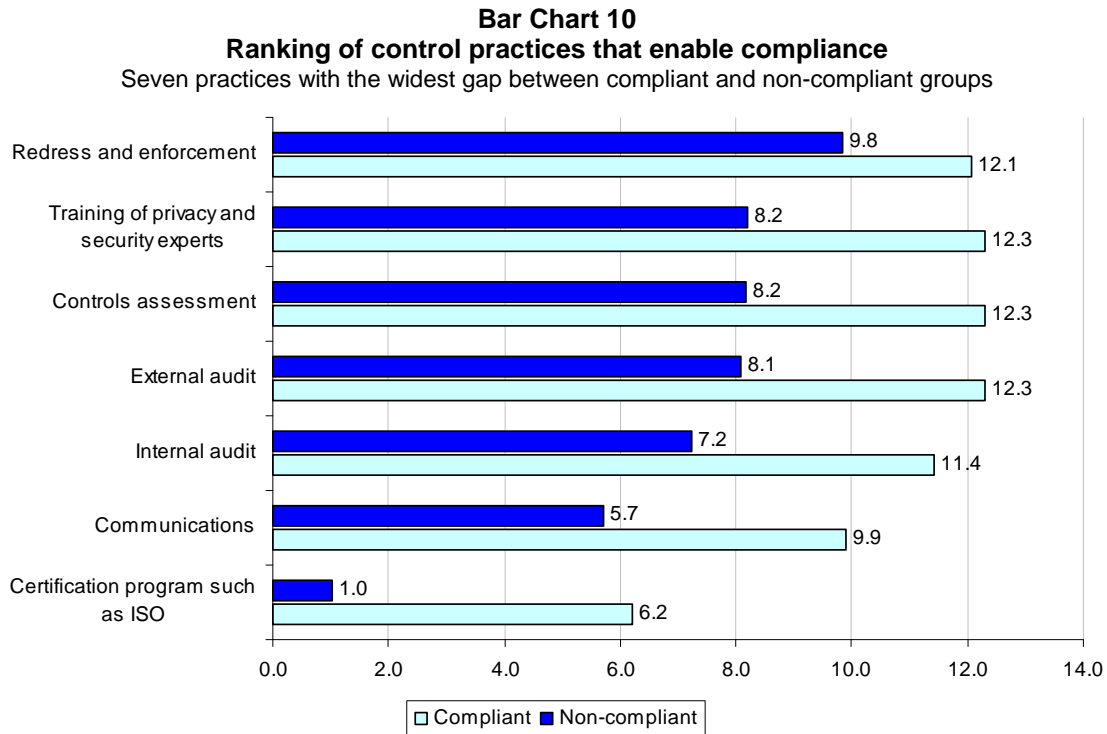


It is important to note that the compliant group ranks all seven technologies as more important to achieving compliance than the non-compliant group. The widest gaps in ranking between the two groups are email encryptions, event management systems, data loss prevention, encryption of wireless communications, and encryption of PDAs and smart phones.

⁴The rank order was reversed from 1 to 15 = most important. This transformation allows longer bars to reflect a higher level of importance.

The higher ranking for encryption and DLP suggests that the compliant group may be more concerned than the non-compliant group about the risk of lost laptops and other mobile data-bearing devices. In the Ponemon Institute *Cost of Lost Laptop* study, the average value of a lost laptop is more than \$49,000. However, there is almost a \$20,000 difference between lost laptops that had encryption installed versus those that did not have encryption.

Bar Chart 10 reports the ranking of different control practices considered important to achieve compliance with privacy and data security regulations. This chart shows seven generally accepted control practices with the widest gap between the compliant and non-compliant groups. Similar to the above analysis, a high rank reflects a higher rating (i.e., is more important).



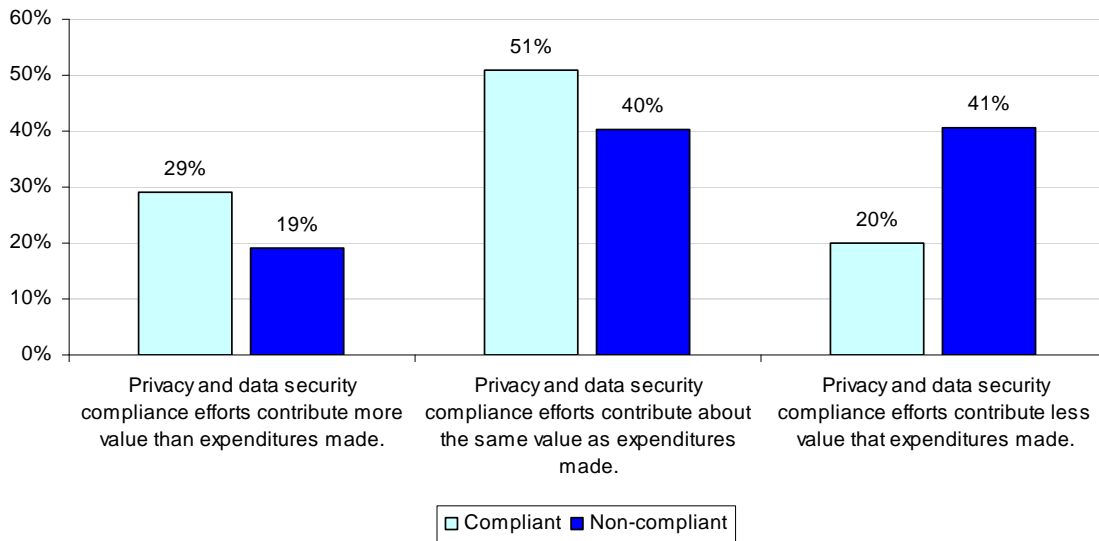
To achieve compliance, the most important control practices include specialized training for privacy and security practitioners, external (independent) audits, and controls assessment. Least important are certification programs, downstream communications and internal audit.

Once again, the compliant group ranks all seven control practices listed above as more important than the non-compliant group. The widest gaps in ranking between the two groups concern certification programs, internal audit and communications.

Respondents in the compliant group believe their organizations gain value from allocating resources to privacy and data security compliance efforts.

Bar Chart 11 shows how respondents in the compliant and non-compliant group respond to three attributions about the value of privacy and data security compliance expenditures to their organizations. According to the survey findings, 29 percent of the compliant group believes compliance efforts contribute more value than expenditures made, and 51 percent believe it receives an equal value. In contrast, 19 percent of the non-compliant group believes there is more value received than expenditures made. Forty percent believes the organization receives equal value for the expenditures made.

Bar Chart 11
Attributions about the value of a compliance program

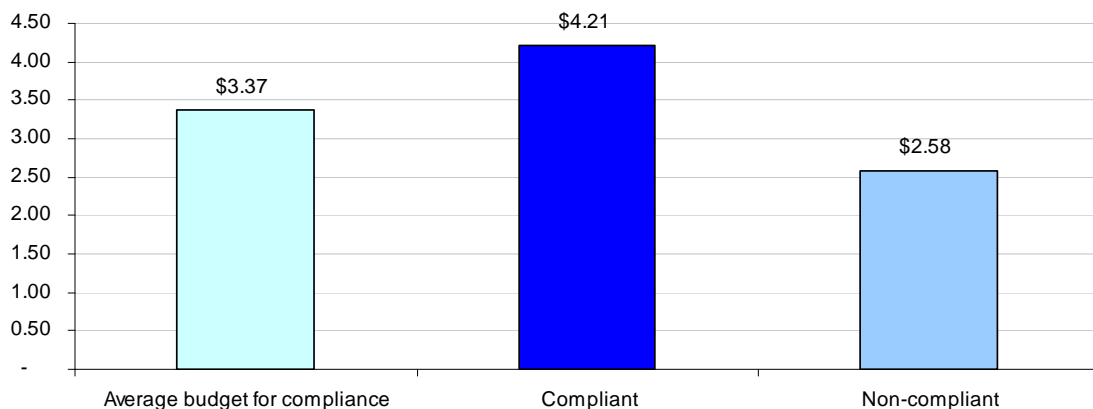


Based on extrapolation methods using survey results, we calculated the average compliance budget for the overall sample and the two groups. Bar Chart 12 shows the overall compliance budget is nearly \$3.4 million. The compliance budget for compliant organizations averages \$4.2 million versus \$2.6 million for non-compliant organizations.⁵

We believe the above analysis provides evidence that achieving a higher level of compliance is positively correlated to the amount of resources an organization is willing to expend. Hence, non-compliant organizations appear to under fund their privacy and data security initiatives.

Bar Chart 12
Extrapolated budget for compliance

\$000,000 omitted from the numbers shown below

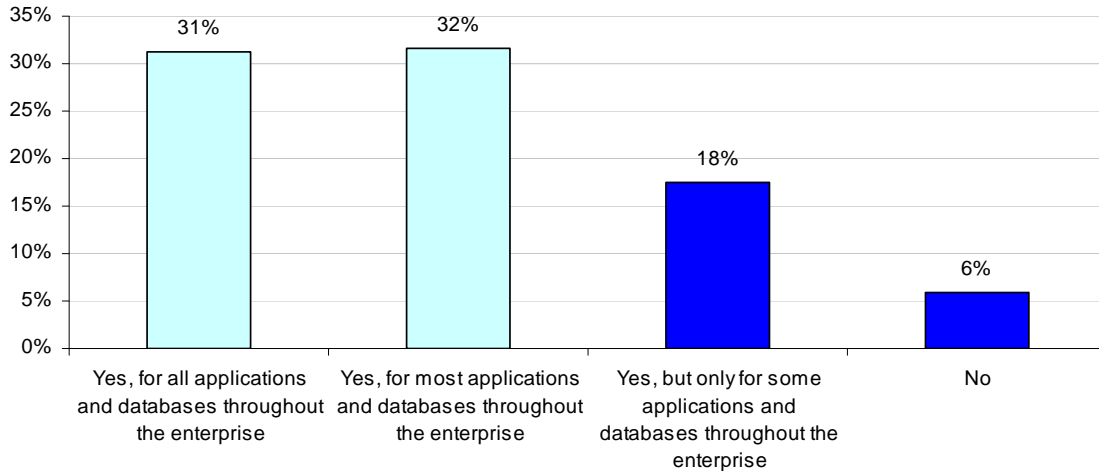


⁵ This finding is consistent with *The Business Case for Data Protection* conducted by Ponemon Institute. In that study of C-level executives, the average spending for data protection programs was \$3.7 million and they believe the average gain from that investment is \$16 million, which suggests a very healthy return on investment for privacy and data protection programs.

The Impact of compliance and budget on data breach

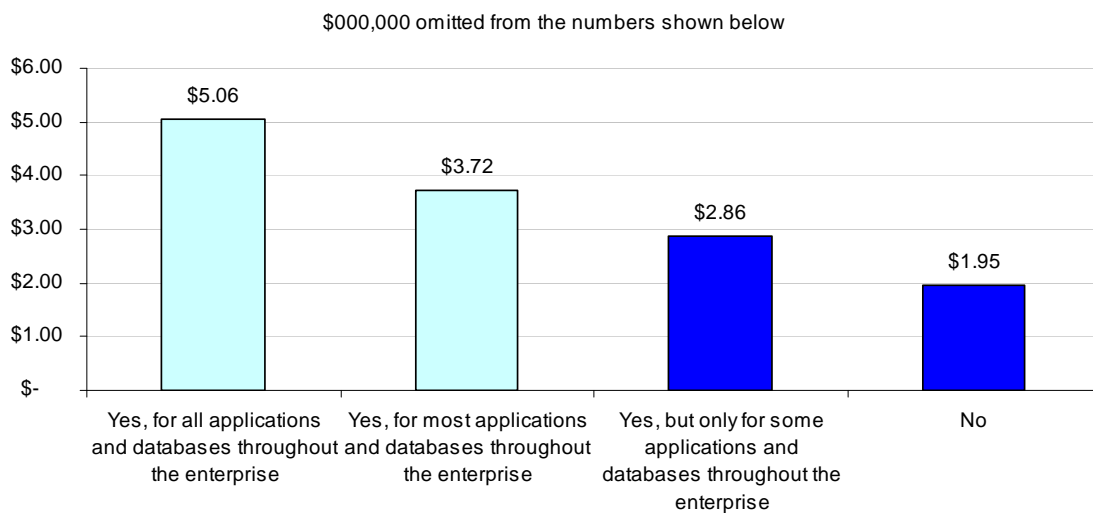
Bar Chart 13 reports the frequency of respondents who state their organizations did not experience a data breach over the past two years. It is clear from this cross-sectional analysis that organizations achieving a high level of enterprise compliance with privacy and data security requirements are much less likely to experience a data breach incident.

Bar Chart 13
Organizations without a data breach in the past two years
 Shown for four compliance levels



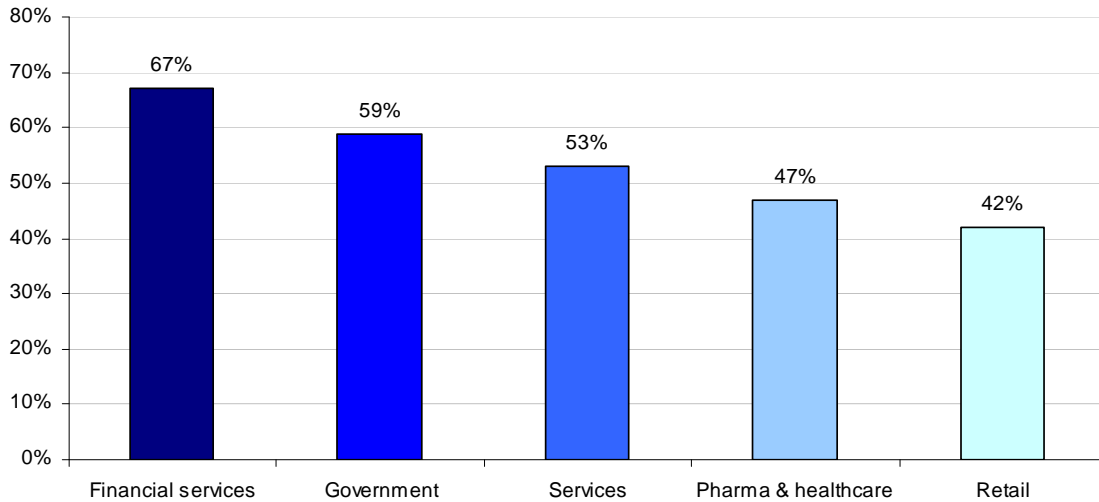
Bar Chart 14 reports the extrapolated average budget dollars according to four compliance levels. As shown, budget dollars assigned to implementing privacy and data security programs vary consistently with the level of compliance.

Bar Chart 14
Extrapolated budget by level of compliance
 Shown for four compliance levels



Bar Chart 15 reports the breakdown of the percentage of respondents in the compliant group for five industry sectors. Financial service has the highest percentage of compliant members (67 percent), while retail has the lowest proportion (42 percent).

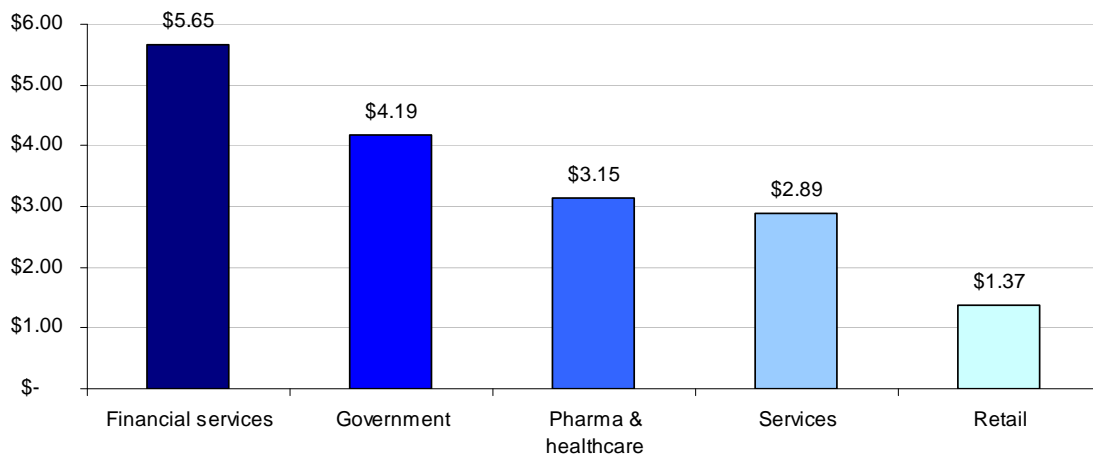
Bar Chart 15
Percentage of compliant group by industry sector
 Shown for five industry sectors



Bar Chart 16 reports the extrapolated average compliance budget according to five industry sectors. Budget dollars for privacy and data security compliance programs vary considerably by industry with financial service organizations having the highest (\$5.65 million) and retail companies having the lowest (\$1.37 million) assigned budget values.

Bar Chart 16
Extrapolated budget by industry
 Shown for five industry sectors

\$000,000 omitted from the numbers shown below



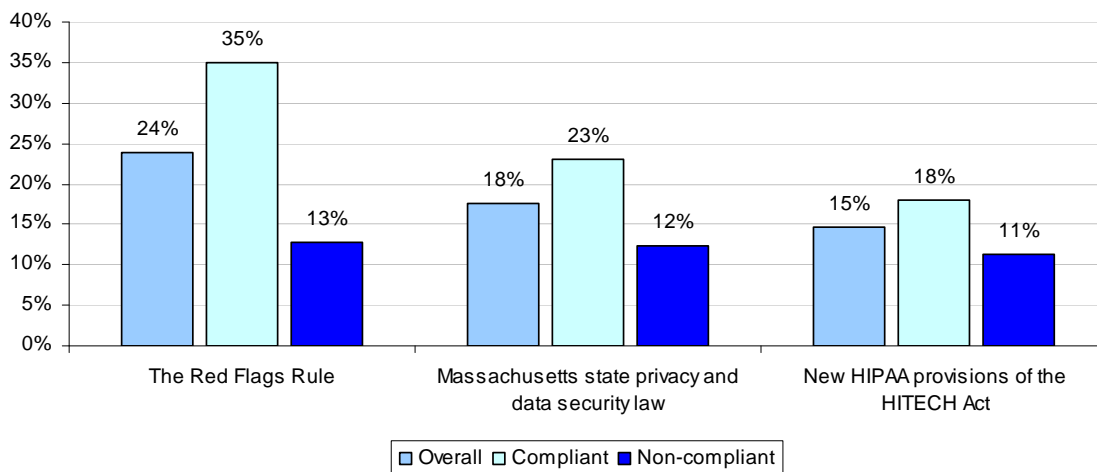
According to respondents, U.S. state data breach notification laws are the most frequently cited regulations for compliance.

Table 1 reports regulations that many U.S. organizations are required to comply with today or in the very near future. Following data breach notification laws, 63 percent must comply with PCI DSS followed by Sarbanes-Oxley (40 percent). Least required to comply with are the Children’s Online Protection Act (COPPA) (13 percent) and FTC’s Do Not Call Registry (12 percent).

Table 1 The privacy and data security regulations organizations are required to comply with.	Applicability
U.S. state data breach notification laws	91%
PCI DSS compliance	63%
Sarbanes-Oxley compliance	41%
CANSPAM Act	39%
European Union Privacy Directive (including Safe Harbor compliance)	39%
Gramm-Leach-Bliley Act	38%
Various national privacy laws (different countries around the world)	33%
Fair Credit Reporting Act (FCRA)	31%
The Red Flags Rule	24%
Health Insurance Portability & Accountability Act (HIPAA)	22%
Fair & Accurate Credit Transactions Act (FACTA)	22%
Massachusetts state privacy and data security law	18%
Federal Privacy Act	16%
New HIPAA provisions of the HITECH Act	15%
Nevada state privacy and data security law	14%
Children’s Online Protection Act (COPPA)	13%
FTC’s Do Not Call Registry	12%

Bar Chart 17 reports the applicability of three new laws for the overall sample and two groups. As can be seen, respondents in the compliant group are more likely to see these regulations as required for their organizations than the non-compliant group. This suggests a higher readiness orientation among respondents in the compliant group.

Bar Chart 17
Applicability of three new laws



Compliance with regulations is believed to reduce some common threats to data security.

According to Table 2, 59 percent of respondents believe compliance decreases the threat of data loss or theft. Fifty-seven percent of respondents believe that compliance reduces the threat of policies and procedures that are not monitored or strictly enforced. More than 50 percent believe that compliance reduces the threat of external penetration by hackers and malicious targeting.

Table 2 How compliance affects nine common threats to the data security environment.	Compliance decreases threat	Compliance has no affect on threat
Data loss or theft	59%	41%
Policies and procedures are not monitored or enforced	57%	43%
External penetration by hackers and malicious targeting (i.e., botnets)	50%	50%
Insecure endpoints connect to the network or enterprise system	49%	51%
Negligent or incompetent employees	39%	61%
Malicious employee attacks	32%	68%
Surreptitious downloads of malware, virus, worm or Trojan that penetrates your company's network or enterprise system	31%	69%
Use of insecure cloud computing applications or platform	20%	80%
Economic espionage	12%	88%

According to most respondents, compliance with privacy and data security requirements does not affect such incidents as economic espionage (88 percent), the use of unsecured cloud computing applications or platforms (80 percent), or surreptitious downloads of malware, virus, worm or Trojan that penetrates your company's network or enterprise system (69 percent).

III. Implications

The purpose of this study is to understand how privacy and data security regulations affect an organization's ability to defend itself against internal and external threats to sensitive and confidential information. We determined that compliance does improve a security posture. The benefit is not only a decrease in data breaches that require notification, but if such an incident occurs the cost is significantly lower.

Other benefits include better relationships with key business partners, receive necessary funding for leading-edge security solutions and have the in-house expertise to understand how to meet regulatory and legal requirements as a result of their compliance efforts.

Compliance is not free. Our study reveals organizations that have minimized the risk of data breach and have achieved compliance spend more money on privacy and data protection. In addition, spending varies by industry. Specifically, heavily regulated industries such as financial services and healthcare allocate more resources to compliance goals than less regulated industries such as retail and services.

IV. Method

Table 3 reports the sample response statistics. A random sampling frame of 11,980 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of experienced IT and security practitioners.

Table 3 Sample response statistics	Freq.
Total sampling frame	11,980
Bounce-back	2,683
Total returns	674
Rejected surveys	58
Final sample	616
Response rate	5.1%

In total, 674 respondents completed the survey. Of the returned instruments, 58 surveys failed reliability checks. A total of 616 surveys were used as our final sample, which represents a 5.1 percent net response rate. Two screening questions were used to ensure respondents had requisite experience in data security or IT compliance, resulting in a reduced sample size of 528 individuals. Ninety-five percent of respondents completed all survey items within 23 minutes.

Table 4 reports the respondent's self-reported position level. As can be seen, more than half of these individuals are at or above the manager level. The average experience in IT, security or both fields is 9.68 years.

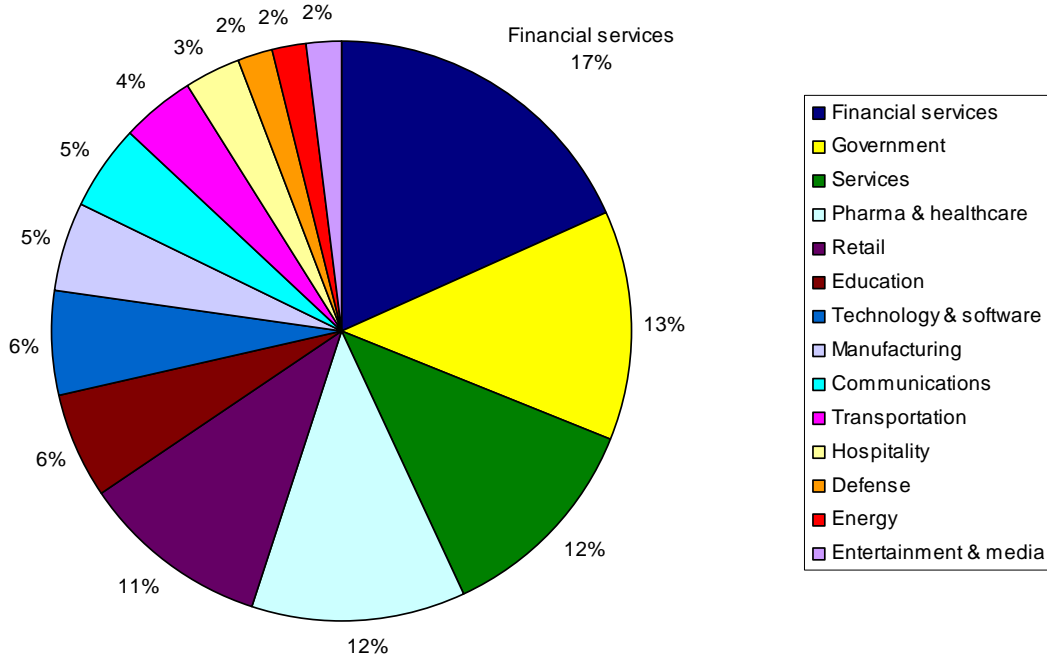
Table 4 What organizational level best describes your current position?	Pct%
Senior Executive/Vice President	1%
Director	17%
Manager	34%
Associate/Staff	20%
Technical Staff	16%
Contractor	12%
Total	100%

Table 5 reports the respondent organization's global headcount. As shown, a majority of respondents work within companies with more than 1,000 employees.

Table 5 The worldwide headcount of your organization?	Pct%
Less than 500 people	11%
500 to 1,000 people	15%
1,001 to 5,000 people	26%
5,001 to 25,000 people	24%
25,001 to 75,000 people	15%
More than 75,000 people	10%
Average	100%

Pie Chart 1 reports the respondent organization’s primary industry classification. As can be seen, over 17 percent of respondents are in financial service companies (including banks, brokerage, credit cards, and insurances). Thirteen percent of respondents are located in government organizations (federal, state and local), and 12 percent are in service organizations (including professional services such as law, accounting and consulting firms).

Pie Chart 1
Industry distribution of respondents’ organizations



V. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix 1: Survey Results

Audited results presented on September 24, 2009

The following table summarizes the sample response for the presented study. As can be seen, the total sample size is 616 individuals, representing a 5.1% response rate.

Sample description	Freq.
Total sampling frame	11,980
Bounce-back	2683
Total returns	674
Rejected surveys	58
Final sample	616
Response rate	5.1%

1. Screening questions

The following two questions were used to refine the sample to those respondents who are involved in their company's privacy or data security compliance programs. The final usable sample is 528.

S1. Are you <u>involved</u> in your organization's privacy or data security compliance efforts?	Freq.
Yes	559
No (STOP)	57
Total	616

S2. Please explain the nature of your involvement in privacy or data security compliance?	Freq.
I am responsible for the technologies that support compliance efforts.	295
I am responsible for managing and/or auditing legal and regulatory requirements.	110
Both	123
None of the above (STOP)	31
Total	559
Useable sample	528

2. Attitudes about compliance

Question 1 provides the strongly agree or agree response combined to five attributions about security compliance.

Q1. Please rate the following five statements using the scale below each item.	Strongly agree and Agree response
Q1a. The patchwork quilt of privacy and data security laws and regulations is confusing and difficult to manage across geographies.	55%
Q1b. Having one compliance standard that satisfies all privacy and data security requirements around the globe would be more efficient and effective for my organization.	45%
Q1c. Privacy and data security laws and regulations reduce my organization's ability to succeed in the global marketplace.	38%
Q1d. Our legal and compliance experts have difficulty translating privacy and data security laws and regulations into specific IT requirements.	43%
Q1e. My organization has knowledgeable people who help ensure compliance with all applicable laws and regulations for privacy and data security.	52%
Average	47%

3. Experience

The following questions provide information how organizations are responding to privacy and data security compliance requirements.

Q2. Please rate your level of knowledge about various U.S. states, federal and international privacy and data security laws that your organization is required to comply with?	Pct%
Significant knowledge	22%
Adequate knowledge	45%
Inadequate knowledge	31%
No knowledge	2%
Total	100%

Q3a. Please check <u>all</u> the privacy and data security regulations that (to the best of your knowledge) your organization is required to comply with today.	Pct%
Massachusetts state privacy and data security law	18%
Nevada state privacy and data security law	14%
Other U.S. state data breach notification laws	91%
Health Insurance Portability & Accountability Act (HIPAA)	22%
New HIPAA provisions of the HITECH Act	15%
Children's Online Protection Act (COPPA)	13%
Gramm-Leach-Bliley Act	38%
Fair & Accurate Credit Transactions Act (FACTA)	22%
The Red Flags Rule	24%
Fair Credit Reporting Act (FCRA)	31%
Federal Privacy Act	16%
Various national privacy laws (different countries around the world)	33%
European Union Privacy Directive (including Safe Harbor compliance)	39%
PCI DSS compliance	63%
Sarbanes-Oxley compliance	40%
CANSPAM Act	39%
FTC's Do Not Call Registry	12%
Other	2%
Total	521%

Q3b. For each privacy and data security regulation checked above (in Q3a), please rate the level of difficulty that compliance creates for your organization using the following four-point scale: from 1 = not difficult to 4 = very difficult to achieve compliance.	Difficult & Very difficult response
Massachusetts state privacy and data security law	56%
Nevada state privacy and data security law	33%
Other U.S. state data breach notification laws	55%
Health Insurance Portability & Accountability Act (HIPAA)	52%
New HIPAA provisions of the HITECH Act	52%
Children's Online Protection Act (COPPA)	14%
Gramm-Leach-Bliley Act	18%
Fair & Accurate Credit Transactions Act (FACTA)	50%
The Red Flags Rule	61%
Fair Credit Reporting Act (FCRA)	39%
Federal Privacy Act	13%
Various national privacy laws (different countries around the world)	63%
European Union Privacy Directive (including Safe Harbor compliance)	67%
PCI DSS compliance	77%
Sarbanes-Oxley compliance	32%
CANSPAM Act	30%
FTC's Do Not Call Registry	4%
Total	42%

Q4. Who in your organization is <u>responsible</u> for ensuring compliance with all applicable privacy and data security laws and regulations? Please use the following code to record your response. 1= The individual or role is most responsible (only record once). 2 The individuals or roles are involved but not most responsible. Blank means the individual or role is not involved (or leave blank)	Pct%
No one person	19%
Chief information officer (CIO)	16%
Chief technology officer (CTO)	6%
IT security leader (CISO)	17%
Privacy officer or leader (CPO)	3%
General IT operations	5%
Chief Financial Officer	3%
Compliance leader	15%
Internal audit	3%
Law department	12%
Human resources	1%
Other	1%
Total	100%

Q5a. To the best of your knowledge, is your organization compliant with all applicable laws and regulatory requirements for privacy and data security today?	Pct%
Yes, for all applications and databases throughout the enterprise	22%
Yes, for most applications and databases throughout the enterprise	29%
Yes, but only for some applications and databases throughout the enterprise	24%
No	24%
Total	100%

Q5b. If you said No (Q5a), why is your organization not compliant with these requirements? Please check the top two reasons only.	Pct%
Lack of enforcement	21%
Lack of resources to sufficiently comply	44%
Lack of support from senior management	31%
Lack of accountability and leadership	55%
Unclear on how to comply with the law or regulation	40%
Other	0%
Total	190%

Q6. Please choose one statement that best describes the value of compliance-related expenditures to your organization.	Pct%
Privacy and data security compliance efforts contribute more value than expenditures made.	19%
Privacy and data security compliance efforts contribute about the same value as expenditures made.	40%
Privacy and data security compliance efforts contribute less value that expenditures made.	41%
Total	100%

Q7. Please select the value privacy and data security compliance provides your organization. Check all that applies.	Pct%
Improves our organization's data security posture	39%
Improves our organization's marketplace brand and reputation	18%
Improves our organization's relationship with key business partners	65%
Heightens awareness among C-levels within our organization	28%
Helps secure more funding for IT security	10%
Provides a business advantage over non-compliant competitors	3%
Other	0%
Total	164%

Q8. What is the purpose of self-regulatory security compliance programs such as PCI, ISO, NIST and other related initiatives? Please choose the statements you believe to be true about compliance.	Pct%
Not necessary	39%
Only "CYA"	26%
Necessary to achieve consistent security practices across the enterprise	32%
Necessary to obtain buy-in from management	48%
Necessary to secure security budget and funding	53%
Necessary to prioritize security requirements	49%
Essential to achieving an effective security posture	42%
Total	287%

4. Budgets for compliance

The following items provide information about the respondent organization's IT security spending on privacy and data security compliance.

Q9a. Approximately, what dollar range best describes your organization's IT security budget in the present fiscal year?	Pct%
Less than \$1 million	9%
Between \$1 to 5 million	13%
Between \$6 to \$10 million	15%
Between \$11 to \$15 million	17%
Between \$16 to \$20 million	15%
Between \$21 to \$30 million	18%
Between \$31 to \$40 million	9%
Between \$41 to \$50 million	5%
Between \$51 to \$60 million	0%
Between \$61 to \$70 million	0%
Between \$71 to \$80 million	0%
Between \$81 to \$90 million	0%
Between \$91 to \$100 million	0%
Over \$100 million	0%
Total	100%
Extrapolated value (\$000,000 omitted)	\$ 16.25

Q9b. Approximately, what percentage of the current IT security budget will be spent on achieving compliance with all applicable privacy and data security legal and regulatory requirements?	Pct%
Less than 5%	10%
Between 5% to 10%	21%
Between 10% to 20%	28%
Between 20% to 30%	17%
Between 30% to 40%	17%
Between 40% to 50%	5%
Between 50% to 60%	2%
Between 60% to 70%	0%
Between 70% to 80%	0%
Between 80% to 90%	0%
Between 90% to 100%	0%
Total	100%
Extrapolated value	19.6%

Q9c. Approximately, what percentage of the current IT security budget is dedicated to compliance with all applicable privacy and data security legal and regulatory requirements will be spent on professional services ?	Pct%
Less than 5%	6%
Between 5% to 10%	6%
Between 10% to 20%	13%
Between 20% to 30%	36%
Between 30% to 40%	18%
Between 40% to 50%	11%
Between 50% to 60%	9%
Between 60% to 70%	3%
Between 70% to 80%	0%
Between 80% to 90%	0%
Between 90% to 100%	0%
Total	100%
Extrapolated value	29.3%

Q9d. What is the nature of these professional services indicated in Q9c? Please check all that apply.	Pct%
Audit & assessments	10%
Certification such as ISO, NIST, PCI and others	11%
Integration of new technologies (such as DLP)	44%
Change management	8%
Management or strategic consulting	10%
Legal services	13%
Other	3%
Total	100%

Q10a. Approximately, what dollar range best describes your organization's corporate compliance budget in the present fiscal year?	Pct%
Less than \$1 million	4%
Between \$1 to 5 million	14%
Between \$6 to \$10 million	20%
Between \$11 to \$15 million	16%
Between \$16 to \$20 million	21%
Between \$21 to \$30 million	6%
Between \$31 to \$40 million	8%
Between \$41 to \$50 million	7%
Between \$51 to \$60 million	4%
Between \$61 to \$70 million	0%
Between \$71 to \$80 million	0%
Between \$81 to \$90 million	0%
Between \$91 to \$100 million	0%
Over \$100 million	0%
Total	100%
Extrapolated value (\$000,000 omitted)	\$ 17.45

Q10b. Approximately, what percentage of the current corporate compliance budget will be spent on achieving compliance with all applicable privacy and data security legal and regulatory requirements?	Pct%
Less than 5%	10%
Between 5% to 10%	21%
Between 10% to 20%	28%
Between 20% to 30%	11%
Between 30% to 40%	19%
Between 40% to 50%	9%
Between 50% to 60%	1%
Between 60% to 70%	0%
Between 70% to 80%	0%
Between 80% to 90%	0%
Between 90% to 100%	0%
Total	100%
Extrapolated value	20.4%

Q10c. Approximately, what percentage of the current corporate compliance budget is dedicated to compliance with all applicable privacy and data security legal and regulatory requirements will be spent on professional services ?	Pct%
Less than 5%	9%
Between 5% to 10%	6%
Between 10% to 20%	16%
Between 20% to 30%	33%
Between 30% to 40%	17%
Between 40% to 50%	10%
Between 50% to 60%	5%
Between 60% to 70%	4%
Between 70% to 80%	0%
Between 80% to 90%	0%
Between 90% to 100%	0%
Total	100%
Extrapolated value	27.0%

Q10d. What is the nature of these professional services indicated in Q6c? Please check all that apply.	Pct%
Audit & assessments	15%
Certification such as ISO, NIST, PCI and others	9%
Integration of new technologies (such as DLP)	15%
Change management	16%
Management or strategic consulting	21%
Legal services	23%
Other	1%
Total	100%

5. Technology, controls and threats

The following table summarizes the results concerning compliance enabling security technologies and threats to information security. Please note that Bar Charts 7 and 8 transformed each rank shown for Q11a and Q11b by subtracting the average rank from 15 (total number of technology choices).

Q11a. Please rank the following 15 technologies that enable your organization to achieve compliance with the various legal and regulatory requirements for privacy and data security. 1 = the most important technology for achieving compliance and 15 = the least important technology for achieving compliance. If possible, please avoid tie scores.	Average Rank	Order
Network access control	11.25	14
Anti-virus & anti-malware solution	5.83	8
Application control	4.82	7
Correlation or event management systems	8.00	10
Data loss prevention (DLP)/content monitoring	3.92	3
Database scanning & monitoring	12.84	15
Encryption of email	10.05	13
Encryption of wireless communication	4.79	6
Encryption of desktops and laptops	3.65	2
Encryption of portable media (e.g., USB memory sticks)	4.04	4
Encryption of PDAs & smart phones	6.30	9
Device/port control solutions	8.85	11
Firewalls	3.10	1
Identity & access management systems	4.20	5
Intrusion detection or prevention systems	9.98	12
Average rank	6.78	

Q11b. Please rank the following 15 operational tasks that enable your organization to achieve compliance with the various legal and regulatory requirements for privacy and data security. 1 = the most important operational tasks for achieving compliance and X = the least important operational tasks for achieving compliance. If possible, please avoid tie scores.	Average Rank	Order
Training of end users	2.9	2
Training of data handlers (i.e., call center employees)	2.1	1
Training of privacy and security experts	4.9	7
Policies and procedures	7.8	12
Communications	7.3	11
Controls assessment	4.9	6
Quality assurance	11.0	14
Certifications (such as ISO, NIST, PCI and others)	11.9	15
Internal audit	5.7	8
External audit	4.8	5
Monitoring of third-party vendors and outsourcing partners	3.9	3
Monitoring changes in laws and regulations	9.3	13
Helpdesk activities	11.9	16
Surveillance	5.7	9
Redress and enforcement	4.1	4
Total	6.5	

Q12. The following matrix lists 9 common threats to the data security environment. Does compliance with privacy and data security laws and regulations decrease=1 or have no impact=2 on each security threat listed below?	Decrease	No Impact
Data loss or theft	59%	41%
Economic espionage	12%	88%
Negligent or incompetent employees	39%	61%
Malicious employee attacks	32%	68%
External penetration by hackers and malicious targeting (i.e., botnets)	50%	50%
Surreptitious downloads of malware, virus, worm or Trojan that penetrates your company's network or enterprise system	31%	69%
Use of insecure cloud computing applications or platform	20%	80%
Policies and procedures are not monitored or enforced	57%	43%
Insecure endpoints connect to the network or enterprise system	49%	51%

Q13a. Did your experience a data breach involving the lost or theft of personal information?	Pct%
Yes, only one incident	40%
Yes, two to five incidents	28%
Yes, more than five incidents	10%
No	22%
Total	100%

Q13b. If you said yes, did you publicly disclose the data breach?	Pct%
Yes, for all data breach incidents experienced	21%
Yes, for some data breach incidents experienced	48%
No, disclosure was not necessary	31%
Total	100%

6. Organizational characteristics & demographics

Following are the organizational characteristics of participating respondents in this study.

D1. What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	1%
Director	17%
Manager	34%
Associate/Staff	20%
Technical Staff	16%
Contractor	12%
Other	0%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	3%
Chief Information Officer	50%
Chief Technology Officer	9%
Compliance/Ethics Officer	9%
Human Resources Leader	0%
Chief Information Security Officer	16%
Chief Privacy Officer	3%
Chief Risk Officer	5%
Other	2%
Total	100%

D3. Total years of business experience	Average
Total years of IT or IT security experience	9.68
Total years in current position years	3.41

D4. What industry best describes your organization's industry focus?	Pct%
Airlines	0%
Automotive	2%
Brokerage & Investments	2%
Communications	4%
Chemicals	0%
Credit Cards	3%
Defense	2%
Education	6%
Energy	2%
Entertainment and Media	2%
Federal Government	9%
Food Service	3%
Healthcare	7%
Hospitality	3%
Manufacturing	5%
Insurance	2%
Internet & ISPs	1%
State or Local Government	4%
Pharmaceuticals	5%
Professional Services	6%
Research	1%
Retailing	8%
Retail Banking	12%
Services	5%
Technology & Software	6%
Transportation	2%
Total	100%

D5. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	11%
500 to 1,000 people	15%
1,001 to 5,000 people	26%
5,001 to 25,000 people	24%
25,001 to 75,000 people	15%
More than 75,000 people	10%
Total	100%

Thank you for your participation. All responses are completely confidential.
Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.