

July 2007

Why Compliance Pays: Reputations and Revenues at Risk

Benchmark Research Report

Contents

Executive summary	1
Key findings	1
Implications and analysis	2
Recommendation: Follow the leaders	3
Findings	4
Most firms continue to struggle with compliance	4
Compliance deficiencies, business disruptions, and data losses	5
Firms that do well on compliance have the fewest business disruptions	5
Firms that do well on compliance have the fewest data losses and thefts	6
Publicly exposed and reported data loss/theft: When, not if	8
Financial losses from publicly exposed data loss and theft	10
Share price declines for publicly traded companies	11
Customer and revenue losses	12
Expenses and costs	14
Financial returns for compliance and data protection	15
Leaders cracked the code: Operational excellence in IT	18
More and appropriate IT controls	19
Fewer control objectives	20
High standards and key performance indicators	21
More frequent monitoring and measurement	22
Allocation of spending to automate controls monitoring	23
Why compliance pays	23
Appendix A: Probability of publicly reported data losses	25
Appendix B: Financial risks and IT policy compliance	26
About the benchmarks	27
About IT Policy Compliance Group	30

Executive summary

Key findings

Most organizations are exposed to financial risk from data loss and theft

Nine out of ten firms are not leveraging compliance and IT governance procedures that could help mitigate financial risk from lost or stolen data. Benchmark results include:

- Lagging organizations—2 out of 10—have the most to gain.
- Normative organizations—7 out of 10—can reduce substantial financial risk.
- Leading organizations—only 1 out of 10—are well positioned.

Compliance leaders have the fewest business disruptions

Firms with the best IT compliance results have the least business downtime from IT security events. Findings show:

- Compliance leaders have only two or fewer disruptions annually from IT security events.
- Compliance laggards experience 17 or more disruptions a year from IT security events.

Compliance leaders have the least data loss and theft

Firms with the best IT compliance report the fewest data losses. Results include:

- Compliance leaders have two or fewer data losses or thefts of sensitive data annually.
- Compliance laggards have 22 or more data losses per year.

Probability of a financial loss: Not if, but when

Financial loss will occur with data loss and theft. The question is when and by how much. The probability of making the front page of the paper for a data loss or theft is:

- Once every three years or sooner for compliance laggards
- One every 42 years or later for compliance leaders

Financial risk and loss are significant enough to manage

The expected financial risk for publicly disclosed data loss and theft is matched by limited actual experience. Financial risks include:

- An 8 percent decline in the market value of a share of stock for publicly traded firms
- An 8 percent loss of customers
- A temporary decline in revenue of 8 percent
- Additional costs for litigation, notification, settlements, cleanup, restoration, and improvements averaging \$100 per lost customer record

Returns are high

Due to high financial risk and relatively low spending on compliance and data protection, returns on spending for compliance and data protection are high:

- Start at about 100 percent on the low end
- Easily exceed 1,000 percent for higher returns

Key findings *(continued)*

Best practices to improve results: Follow the leaders

The benchmarks identify practices being implemented by leaders that dramatically improve IT compliance results, markedly reduce business downtime from IT security events, substantially reduce incidents of data loss and theft, and reposition these firms for lower financial risk. Such practices include:

- **Implementing more of the appropriate IT controls**
- **Reducing control objectives, making it easier to communicate, measure, and report**
- **Establishing higher standards for performance objectives**
- **Encouraging a culture of operational excellence in IT**
- **Monitoring, measuring, and reporting controls against objectives at least once every two weeks**
- **Allocating more funds to control automation**

Implications and analysis

The probability of an undisclosed data loss being turned into an exposed publicity event is relatively high for most organizations. It is directly related to how well an organization complies with its own policies as well as regulatory and industry governance requirements regarding the handling and custody of sensitive data. Financial returns for improving compliance and data protection are a measure of the expense of the financial risk divided by the total cost to avoid the risk.

On a constant dollar basis, total spending on compliance activities ranges from \$200,000 or less for small businesses to more than \$30 million annually for the largest of enterprises. This total spending falls roughly between 0.2 percent and less than 0.03 percent of revenue, for firms with revenue ranging from \$100 million, to \$100 billion, respectively. The majority of this spending is on compliance, not data protection.

Return on spending: Positive for almost all organizations

Based on financial losses sustained after a publicly exposed data loss—including lost customers and revenues, stock price declines, and additional costs and total cumulative spending on compliance and data protection activities over the “number of years to disclosure”—the returns on compliance and data protection spending are positive for almost all organizations.

Firms that excel at compliance are those with the fewest data losses and thefts.

Operational excellence in IT

The benchmarks show that firms excelling at compliance are those with the fewest data losses and thefts. The benchmarks also show that to avoid, mitigate, or delay the financial consequences of publicly reported data loss and theft, it is essential to drive operational excellence in IT by monitoring and measuring controls against objectives consistently, at least once every two weeks.

Delaying the financial risk

Among larger enterprises, the probability of a data loss is likely once every three years if the firm is currently operating as a laggard. Improving the performance profile of the organization to the norm decreases the odds of a data loss—and its financial consequences—to once every 15 years. Further improvement—to the leadership category—improves the odds even more, to once every 42 years.

Better compliance pays for itself through the avoidance of predictable financial risk.

Perhaps most important, the amount spent on improving compliance and data protection is a very small percentage of the financial value that is at risk. With returns on compliance spending for larger enterprises starting at 1,000 percent and climbing to 100,000 percent, it is obvious that compliance is good for business. Not only is good governance the right thing to do, but better compliance pays for itself through the avoidance of predictable financial risk.

Recommendation: Follow the leaders

To avoid the fallout from publicly reported data losses or thefts, firms can take guidance from the practices that work: those being implemented by organizations with the fewest IT compliance deficiencies, business disruptions from IT security events, and data losses or thefts.

To avoid the fallout from publicly reported data loss or theft, firms can take guidance from the practices that work.

1) More and appropriate IT controls

There is a large gap between the laggards and leaders regarding the number of different IT controls being implemented by organizations. Selecting the appropriate IT controls, and more of them, is shown to drive superior performance results among leading companies, with the fewest IT compliance deficiencies and the fewest latent data losses or thefts.

2) Fewer control objectives

Control objectives are the policies and objectives that organizations establish for compliance and data protection. While the leading organizations—those with the fewest IT compliance deficiencies and the lowest rates of unreported data losses—are employing more appropriate IT controls, they also have the fewest number of control objectives compared with other firms. A clearly articulated set of objectives leads to more effective training, certifications, reporting, and measurements that are conducted by internal and external auditors.

3) High standards and key performance indicators

The leading organizations establish high standards for key performance indicators (KPIs). Although not always successful, the leaders target 5 percent of control objectives for all three KPIs: IT compliance control deficiencies, business disruptions from IT security events, and latent unreported data losses. To improve results, firms operating as compliance laggards should reduce the number of control objectives while also taking actions that will help achieve 5 percent or less for each KPI.

4) More frequent monitoring and measurement

From one benchmark to the next, and across all of the benchmarks conducted by the IT PCG, the frequency of monitoring procedural (nontechnical) and technical controls against control objectives is aligned with performance results. Organizations with the fewest latent data losses and compliance deficiencies are monitoring and measuring compliance controls once every one to three weeks, and controls for data losses and thefts once each week, averaging at least once every two weeks.

5) Allocation of spending to automate controls monitoring

The frequent monitoring and measurement of controls among firms that lead in compliance are being supported by significant differences in how funds for IT security are spent. In addition to spending larger percentages of the IT budget for IT security controls, the firms with the fewest undisclosed latent data losses and least number of compliance deficiencies are reallocating funds from external contract spending towards additional funding for equipment and software specifically targeted at automating the monitoring and measurement of controls and procedures.

Findings

Most firms continue to struggle with compliance

Eighty-seven percent of organizations—about 9 out of 10 firms—are not leveraging the appropriate compliance and IT governance procedures, which would reduce costs, business disruptions, and lost or stolen data. Instead, a majority of businesses and public institutions are still struggling with high rates of annual compliance deficiencies, business disruptions, and data losses and thefts that could be prevented with better implemented IT policy compliance, risk, and governance programs (Table 1).

Performance spectrum	Percentage of organizations	Number of IT compliance deficiencies to pass audit	Number of security events resulting in business disruptions	Number of unreported losses or thefts of sensitive data
Lagging firms	20%	26	17	22
Normative firms	67%	6	6	5
Leading firms	13%	2	2	2
Sample		1,779	1,269	694

Table 1. Compliance deficiencies, business disruptions, data losses, and thefts

Source: IT Policy Compliance Group, 2007

Compliance deficiencies, business disruptions, and data losses

There is a close alignment of results across thousands of organizations that have participated in the IT PCG benchmarks. The alignment includes:

- *Lagging organizations*—Two in every 10 organizations—20 percent of all firms—are correcting an average of 26 IT compliance deficiencies each year to pass audit by external auditors, are experiencing 17 business disruptions from IT security events, and are suffering from 22 losses or thefts of sensitive data each year, most of which are never publicly reported.
- *Normative organizations*—The vast majority of organizations—almost 7 out of 10, or 67 percent—are correcting six compliance deficiencies to pass audit, are experiencing six business disruptions, and have five losses or thefts of sensitive business data annually.
- *Leading organizations*—Slightly more than one in every 10 organizations—13 percent—are only having to correct two compliance deficiencies, are experiencing two business disruptions annually, and have two losses or thefts of sensitive data each year.

The alignment of performance results, across seemingly unrelated areas—IT compliance deficiencies, business disruptions from IT security events, and data losses and thefts—is consistent in every benchmark conducted by the IT PCG.

Firms that do well on compliance have the fewest business disruptions

Organizations with the best IT compliance results are those with the smallest amount of business downtime from IT security events. In contrast, firms with the most business downtime have the worst compliance results (Figure 1).

Compliance leaders have the least business downtime from IT security events

The majority—82 percent—of the firms with the fewest IT compliance deficiencies also have the fewest business disruptions from IT security events annually. Moreover, actual downtime for these firms averages six hours each year.

Compliance laggards have the most business downtime from IT security events

Most—62 percent—of the firms with the largest number of IT compliance deficiencies are also those with the largest number of IT security events resulting in business downtime each year. Among these firms, the average business downtime from IT security events is 272 hours—about 7 weeks—each year.

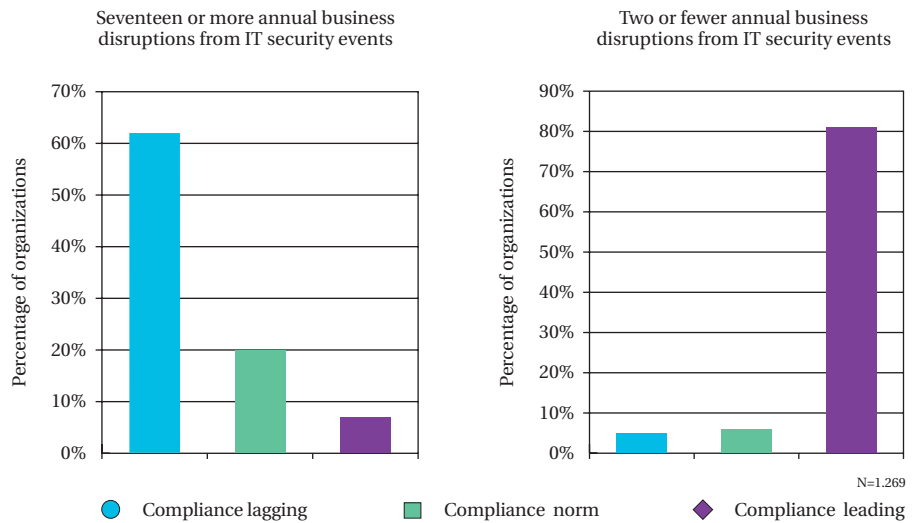


Figure 1. Business disruptions and compliance profiles

Source: IT Policy Compliance Group, 2007

Depending on the severity of the events, the result of business downtime could range from little or no impact to more severe financial consequences. While severity plays a role in determining how organizations react to IT security events, the benchmarks also show that firms have different financial risk appetites when it comes to sustaining financial losses before taking action to mitigate losses (Table 2).

Size of organization	Losses that will be sustained before spending additional funds on IT security
Small business (less than \$50 million)	\$100,000 per year
Midsize organizations (\$50 million to \$999 million)	\$330,000 per year
Large enterprises (\$1 billion or more)	\$600,000 per year

Table 2. Financial risk appetites by size of organization

Source: It Policy Compliance Group, 2007

Not restricted to business downtime, these self-insurance thresholds apply to any event resulting in financial loss as it applies to IT security, including the loss of sensitive business data.

Firms that do well on compliance have the fewest data losses and thefts

Firms with the best IT compliance results are those with the fewest losses or thefts of sensitive data each year. In contrast, the firms with the largest number of annual losses or thefts of sensitive data are those with the worst IT compliance results (Figure 2).

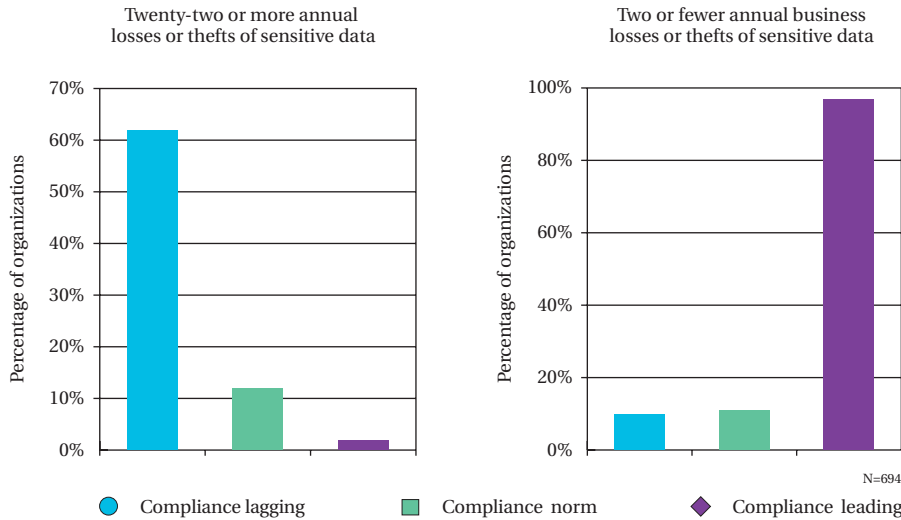


Figure 2. Unreported Data losses, thefts, and compliance profiles

Source: IT Policy Compliance Group, 2007

Compliance leaders have the fewest data losses and thefts

Firms that do well on IT compliance have fewer data losses and thefts. The majority—96 percent—of firms with the fewest compliance deficiencies are those with the fewest latent losses or thefts of data annually, averaging two or fewer losses or thefts of sensitive data each year.

Firms that do well on IT compliance have fewer data losses and thefts.

Compliance laggards have the most data losses and thefts

In contrast, most—63 percent—of the firms with the largest number of compliance deficiencies are also those with the largest number of latent data losses or thefts each year. Among them, the number of unreported, latent data losses or thefts averages 22 annually.

Publicly exposed versus latent unreported data losses

There is an important difference between latent unreported data losses and the losses or thefts of data that are publicly exposed and reported. The benchmarks are a measure of the latent, unreported data losses and thefts. The number of publicly exposed data losses and thefts is much smaller than the benchmark findings.

Publicly exposed and reported data losses/thefts: When, not if

When undisclosed data loss and theft rates are factored in, the probability of a public exposure—primarily among U.S.-based firms—of data losses or thefts occurring is not if but when the event occurs for any organization.

Based on the Attrition database (see www.attrition.org), the number of publicly disclosed and reported data thefts and reports since the Choice Point incident in the United States in March 2005 averages 278 publicly exposed incidents of data theft or loss each year.

The probability of a public exposure—primarily among U.S.-based firms—of data losses or thefts occurring is not “if” but “when” the event will occur for any organization.

This average does not predict the probability of a data theft or loss occurring for any one organization. The probability of a publicly exposed data loss or theft is a measure of the number of outcomes of publicly exposed data losses by the total number of possible outcomes in a sample space. In this case, the sample space includes the number of firms, as well as their predisposition to data losses and thefts based on existing loss rates that are not reported publicly. See Appendix A, “Probability of Publicly Reported Data Losses.”

Size and latent data losses influence likelihood of public exposure

Although the size of an organization does not materially influence outcomes for compliance or data losses, the number of firms does influence the probability that any one firm, by size, will experience a publicly disclosed loss or theft of sensitive data. For example, the population of small businesses in the United States is more than 6,000 times larger than that of large enterprises and more than 400 times larger than that of midsize firms. This difference decreases the likelihood of any one small business experiencing a publicly reported data loss or theft, while increasing the odds of a data loss or theft being publicly reported among larger enterprises.

Small businesses: Most “years to disclosure”

For a small business with 250 employees, the range of “years to disclosure” is between 36 and 108 years if the firm is performing as a compliance laggard and suffering from large numbers of annual undisclosed data losses and thefts of data. If the same small business improves its latent data loss and compliance results, the “years to disclosure” jump to between 786 and 1,191 years (Table 3).

Compliance Performance Profiles	Small business (250 employees)	Midsize organization (1,500 employees)	Large enterprise (9,000 employees)
Lagging firms	36 to 108 years	6 to 18 years	1.5 to 5 years
Normative firms	288 to 476 years	39 to 77 years	10 to 20 years
Leading firms	785 to 1,190 years	127 to 193 years	34 to 51 years

Table 3. Years to disclosure for publicly exposed data thefts and losses

Source: IT Policy Compliance Group, 2007

Midsize organizations: Public exposure could occur on your watch

The smaller number of midsize firms, compared with the larger population of small businesses, increases the probability of a public exposure from undisclosed data loss rates for any one midsize firm. Based on a firm with 1,500 employees, the “years to disclosure” is once every 6 to 18 years for an organization with the highest rate of unreported data losses that is operating as an IT compliance laggard. If that same midsize firm improves its latent data loss and compliance posture, it could push the “years to disclosure” for a data theft or loss to between 127 and 193 years.

Large enterprises: Public exposure is more likely

For a 9,000-employee-sized large enterprise with high latent data losses and operating as a compliance laggard, the “years to disclosure” for a data loss or theft is between one and one-half and five years. When that same 9,000-person organization improves its latent data loss rates and compliance posture, the likelihood of a public exposure is delayed to once every 33 to 51 years.

Firms operating as compliance leaders are less likely to experience public exposure of latent data losses and thefts.

Average time to public exposure

While the ranges are probably a more accurate way of estimating the likelihood of a data loss becoming publicly reported, the average time to disclosure is easier to use than the ranges. As part of an analysis involving financial risk and risk mitigation measures that can be undertaken, including the actions needed to improve compliance and latent data loss results, the average time is most often employed.

For a large enterprise operating as a laggard for compliance and data protection, the average time before experiencing a publicly reported data loss or theft is once every three years. If the same large enterprise improves its compliance and data protection

loss rates to operate at the norm, it delays the likely occurrence of a publicly reported data loss or theft to once every 15 years. Further improvements to IT compliance and data protection, placing the organization in the category of a leader with two or fewer latent unreported data losses annually, delays the likelihood of a publicly reported data loss or theft to once every 42 years (Figure 3).

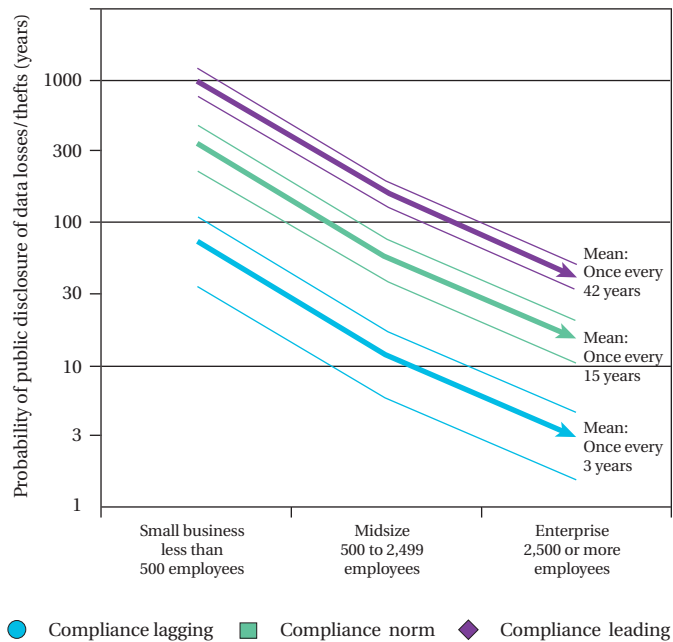


Figure 3. Average time to public exposure of data loss and theft

Source: IT Policy Compliance Group, 2007

Financial losses from publicly exposed data loss and theft

To determine the financial risks, the IT PCG conducted benchmarks focused on the expected financial losses associated with data losses and thefts that are publicly disclosed. Based on benchmarks conducted with 475 organizations, the expected financial consequences of publicly exposed data thefts and losses include:

- Changes in the price of stock for publicly traded firms
- Customer and revenue losses
- Additional expenses and costs

Share price declines for publicly traded companies

The benchmark findings show that publicly traded firms expect to see a decline of 8 percent in the price per share for their firm as a result of a data loss or theft being reported publicly.

The benchmarks conducted with these 475 organizations also show an inverse relationship in expected declines in the price of stock for publicly traded organizations, with increasing losses directly tied to company size and decreasing losses tied to an organization's compliance and data protection performance profile (Figure 4).

Declines in stock value increase with size of organization

As organizations become larger, the expected financial impact from a decline in stock price increases. The benchmarks show an expected financial decline in stock value per share increase from a 7.9 percent decline for organizations with 1,000 employees to a 13.6 percent decline for organizations with 100,000 employees.

Declines in stock value decrease with improvements in compliance

As a function of an organization's compliance and unreported latent data loss postures, per-share stock prices decline from 14.6 percent for organizations with 22 deficiencies to 7.3 percent for firms with two compliance deficiencies and latent data losses.

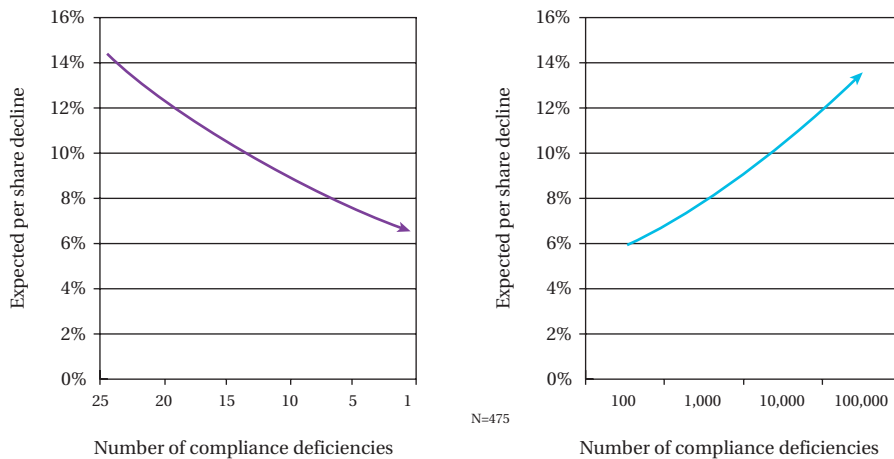


Figure 4. Stock price declines for publicly exposed data loss/theft

Source: IT Policy Compliance Group, 2007

Recent experience: Thirty publicly traded companies

Expectations of loss can sometimes be worse than actual experience. For this reason, the actual stock prices of 30 firms were checked. The 30 firms are listed in the Attrition database and are publicly traded, and all experienced a data loss or theft sometime between January 2004 and March 2007. The organizations that were selected are from different industries, but all share a common trait: They experienced a large number of lost or stolen customer accounts, or records.

The average price-per-share decline among the 30 firms was 7 percent: very close to the benchmark expectation. The declines experienced by the 30 firms ranged from no decline for a one-year period after the data loss to a high of 23.1 percent.

Although many factors beyond a data loss or theft are responsible for the price of stock, only 2 of the 30 firms experienced no decline over the one-year period after the data loss or theft, while the other 28 firms experienced declines in the price per share of their publicly traded stock. This occurred during a time (January 2004 through March 2007) when the indexes for the U.S. markets rose, including an 18.6 percent increase in the value of the New York Stock Exchange, a 28 percent increase in the Standard and Poor's 500, and a 23 percent increase in the NASDAQ index.

The expected average decline in the price of publicly traded stock is higher for the benchmark (8 percent) conducted with 475 companies than the actual experience of the 30 companies (7 percent). The smaller sample base of the 30 companies indicate the benchmark results for expected declines in stock value are reliable indicators of declines in capitalization and market value.

Customer and revenue losses

The expected loss of customers and revenue after public disclosure of a data loss or theft is another financial consequence measured by the benchmarks conducted with 475 organizations. Expected customer and revenue losses for a publicly disclosed data loss or theft demonstrate an inverse relationship based on the size of a firm and its compliance posture (Figure 5).

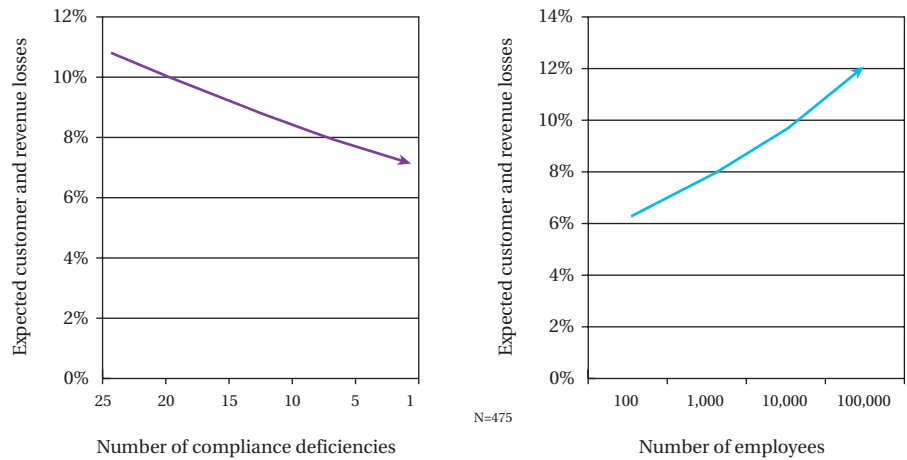


Figure 5. Customer and revenue losses for publicly exposed data loss/theft

Source: IT Policy Compliance Group, 2007

Across the 475 organizations participating in the benchmarks, the average expected loss of customers was 8.1 percent, while the average expected revenue loss was a concomitant 8 percent. The expected losses vary by the size of the organizations and their compliance and data protection profiles.

Customer and revenue losses increase with organization size

The expected loss of customers and revenues track each another and increase with organization size. The benchmark results show an increase in the expected customer and revenue losses from 7.8 percent for organizations with 1,000 employees to 12 percent for organizations with 100,000 employees.

Customer and revenue losses decline with improvements to compliance

As a function of compliance posture, which is nearly identical to latent data losses and thefts, the expected loss of customers and revenue declines from 10.3 percent for organizations with 22 deficiencies to 6.8 percent for firms with two compliance deficiencies and unreported data losses.

Recent experience: Ten of the 30 companies listed in the Attrition database

Based on a more limited sample of actual results that have occurred in the market, it would appear the benchmark data are reliable: There is a temporary—one to two calendar quarter—drop in customers and revenue that hovers around 8 percent.

The revenue for the sample of 10 public companies was compared with historical changes in revenue over four quarters after the publicly reported data loss or theft. These results were compared with historical revenue dating back two years prior to the reported data loss.

All of the 10 firms experienced short-term declines in revenue, relative to historical norms for the same quarters, after the announcement of the data loss or theft. Averaging an 8 percent loss in revenue, none of the firms showed declines in revenue year over year.

Averaging an 8 percent loss in revenue, none of the firms showed declines in revenue year over year.

Instances of data losses and thefts involving smaller numbers of lost records or customers may or may not influence results, but such an analysis could not be included in time for this report.

Expenses and costs

Other expenses and costs resulting from data loss and theft that were measured by the benchmarks with 475 organizations are associated with litigation, class action lawsuits, settlements, legal fees, customer notifications, data reconstruction, investigations, improvements in IT security and compliance, and labor expenses needed to manage and triage events after a publicly exposed data loss or theft.

The average additional expected cost is \$100 per lost or stolen customer record to pay for litigation, cleanup, settlements, investigations, fines, improvements, customer notifications, and ancillary costs.

The benchmarks also show a difference in expected additional costs by size of organization and by compliance and data protection profiles.

Costs increase with the size of an organization

The benchmark findings show expected costs increase as the size of organization increases: from \$66 per lost customer record for an organization with 1,000 employees to \$144 for an organization with 100,000 employees (Figure 6).

Costs decrease with improved compliance results

Expected costs decrease from an exposed data loss or theft as compliance results—and latent data losses—decrease: from \$137 per lost customer record for organizations with 22 deficiencies to \$84 per lost customer record for organizations with two compliance deficiencies.

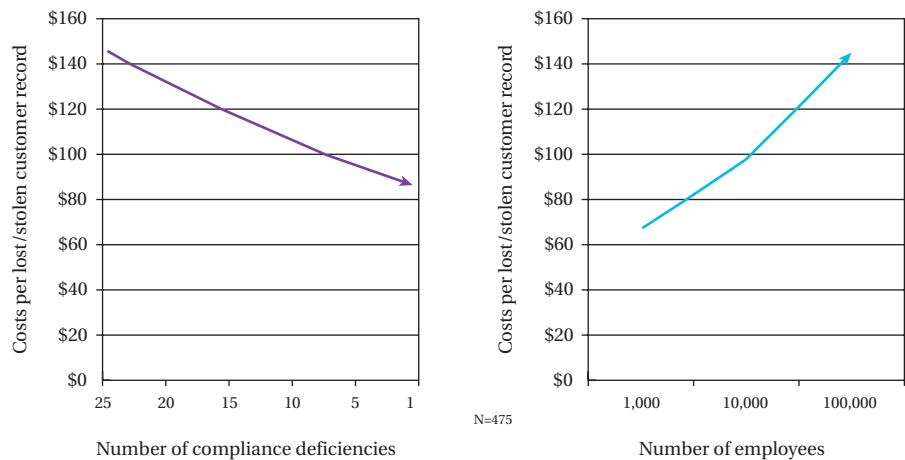


Figure 6. Costs per lost customer record

Source: IT Policy Compliance Group, 2007

Recent experience

The IT PCG has been unable to reliably verify whether actual experience differs from or mirrors the predicted benchmark results. When enough substantive experience exists, a comparison between actual and expected additional costs will be provided.

For now, it is difficult to imagine that additional costs will reach \$100 per record, or more, and almost impossible to verify the reliability of the findings for these additional costs based on recent experience. Only time will tell what the additional costs will be for cases of publicly reported data losses that occurred in 2006 and early 2007.

Financial returns for compliance and data protection

No organization wants to find its good name displayed on the evening news, in Internet blogs, in the financial press, or in weeklies for an exposed data loss or theft. The probability of an unreported data loss being turned into a publicly exposed event is relatively high and, as the benchmarks show, is directly related to how well an organization complies with its own policies as well as regulatory and industry governance requirements regarding the handling and custody of sensitive data.

Financial returns for improving compliance and data protection are a measure of what the financial risk is divided by the total costs to avoid the risk.

Spending on compliance and data protection

On a constant dollar basis, total spending on compliance activities ranges from \$200,000 or less for small businesses to more than \$30 million annually for the largest enterprises. Based on findings with 867 organizations, total spending on compliance and data protection currently ranges from less than 0.2 percent to less than 0.03 percent of revenue by firms with revenue ranging from \$100 million to \$100 billion, respectively. Note that the majority of this spending is on compliance, not on data protection, which is a very small percentage of compliance spending.

Return on compliance and data protection spending

Based on financial losses sustained after a publicly exposed data loss, including one or more losses of customers and revenues, stock price declines, or additional costs, and the total cumulative spending on compliance and data protection activities over the “number of years to disclosure,” the returns on compliance and data protection spending are positive for almost all organizations (Table 4).

Performance profile	Revenue	Return on financial risk (4% of revenue)	Return on financial risk (8% of revenue)	Return on financial risk (12% of revenue)
Lagging firms	\$100 million	47%	95%	1,42%
	\$1 billion	502%	1,004%	1,505%
	\$10 billion	6,228%	12,455%	18,683%
Normative firms	\$100 million	10%	19%	29%
	\$1 billion	101%	202%	303%
	\$10 billion	1,255%	2,510%	3765
Leading firms	\$100 million	4%	7%	10%
	\$1 billion	37%	73%	110%
	\$10 billion	454%	907%	1361%

Table 4. Returns on spending for compliance and data protection

Source: IT Policy Compliance Group, 2007

Financial exposure for publicly reported data losses and thefts

The benchmarks—and experience—show average revenue and customer losses are at about 8 percent of revenue currently. This 8 percent of revenue represents a typical value for what is at risk, even if additional expenses and costs as well as market capitalization declines from share-price decreases are not included.

An optimistic assessment of the financial value at risk would probably be around 4 percent of revenue, while a pessimistic view might peg the financials at risk due to a publicly reported data loss at about 12 percent.

Large enterprises: At greater risk

Larger enterprises are more likely to be covered by trade journals, the media, and financial outlets. Moreover, 4 percent or 8 percent of larger revenue means that financial risk—and therefore the break-even point for spending on compliance and data protection—will occur faster. Actual returns will vary based on current compliance performance profiles and the level of improvement organizations are able to achieve (Figure 7).

Midsized firms: In the middle

Compared with larger enterprises, any one midsized firm is less likely to suffer from a data loss or theft, and the total financial value at risk is lower. Although they may be subject to the same press coverage as larger competitors, the break-even point—for spending on compliance and data protection—while positive, may not occur as rapidly as it does for larger enterprises.

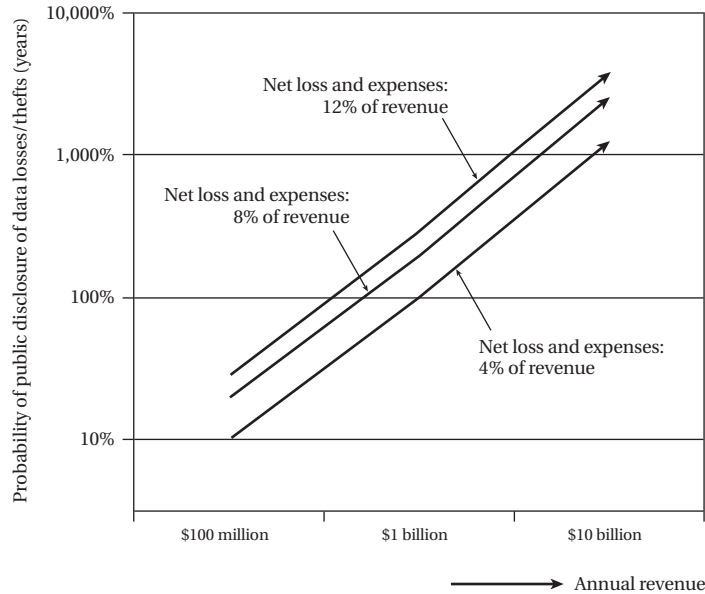


Figure 7. Return on compliance spending: Normative performers

Source: IT Policy Compliance Group, 2007

Small businesses: Compliance and data protection are still required, but at what cost?

Small businesses performing as laggards will enjoy positive returns on spending for compliance and data protection. Although returns on spending for small businesses, based solely on data losses and thefts, are probably not sufficient to justify performing as leaders, specific industry requirements and company policies may 1) dictate the need to improve results to this level or 2) result in faster returns on spending. See Appendix B, “Financial Returns and IT Policy Compliance.”

Financial returns for noncompliance and data risk are real

The IT PCG benchmarks show that the financial risks of noncompliance with organizational policies and objectives are real and are accompanied by tangible—and predictable—financial consequences. Given the predictable occurrence rate of data losses and thefts, the almost one-to-one correlation between good compliance results—with fewer unreported data losses and thefts—and the magnitude of financial value that is at risk from data theft and loss, managing the risk should be of concern to senior management, the board, and shareholders.

Contrary to popular wisdom that funding for compliance can and should be used for more productive pursuits, the benchmark results show that firms excelling at compliance are in a much better position to mitigate, delay, and reduce financial risk.

Leaders cracked the code: Operational excellence in IT

Why do organizations operating as compliance leaders have the fewest latent data losses and thefts, and what can others learn from companies with stellar compliance and data protection records? Part of the answer lies in the primary causes of compliance deficiencies uncovered by the IT PCG benchmarks (Figure 8).

Leading causes of compliance deficiencies for all organizations		Problem areas of lagging and normative—87% of all—organizations																			
<ol style="list-style-type: none"> 1. User and application access controls 2. Documentation 3. PC and laptop access controls 4. Configuration and change management 5. IT security policies and standards 6. Auditing and reporting 7. Database access controls 8. Information access controls 9. Email, Web, and Internet access controls 10. Asset classification <p>IT Security—7 of the Top 10</p>		<table border="1"> <thead> <tr> <th>Rank</th> <th>Cause of deficiencies among lagging and normative firms</th> <th>Percentage of lagging and normative firms</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>User and application access controls</td> <td>63%</td> </tr> <tr> <td>2</td> <td>IT security policies and standards</td> <td>63%</td> </tr> <tr> <td>3</td> <td>IT configuration change management</td> <td>60%</td> </tr> <tr> <td>4</td> <td>IT auditing and reporting</td> <td>54%</td> </tr> <tr> <td>5</td> <td>Application development and maintenance</td> <td>50%</td> </tr> </tbody> </table>	Rank	Cause of deficiencies among lagging and normative firms	Percentage of lagging and normative firms	1	User and application access controls	63%	2	IT security policies and standards	63%	3	IT configuration change management	60%	4	IT auditing and reporting	54%	5	Application development and maintenance	50%	
Rank	Cause of deficiencies among lagging and normative firms	Percentage of lagging and normative firms																			
1	User and application access controls	63%																			
2	IT security policies and standards	63%																			
3	IT configuration change management	60%																			
4	IT auditing and reporting	54%																			
5	Application development and maintenance	50%																			

Figure 8. Primary causes of compliance deficiencies: IT general controls

Source: IT Policy Compliance Group, 2007

Majority of deficiencies are in IT general controls

The major contributors to compliance deficiencies—where 8 of the top 10 deficiencies must be corrected to pass audit—are found in IT general controls. The primary culprit of compliance deficiencies is technical and nontechnical controls associated with IT security, which are responsible for 7 of the top 10 compliance deficiencies for the majority of organizations.

The top five causes of deficiencies among the majority of the population—the 87 percent of the population not performing as leaders for compliance and data protection—include the following:

- User and application access controls
- IT security policies and standards
- IT configuration and change management
- IT auditing and reporting
- Application development and maintenance

More and appropriate IT controls

There is a huge gap between the laggards and the leaders in the number of different IT controls being implemented (Figure 9).

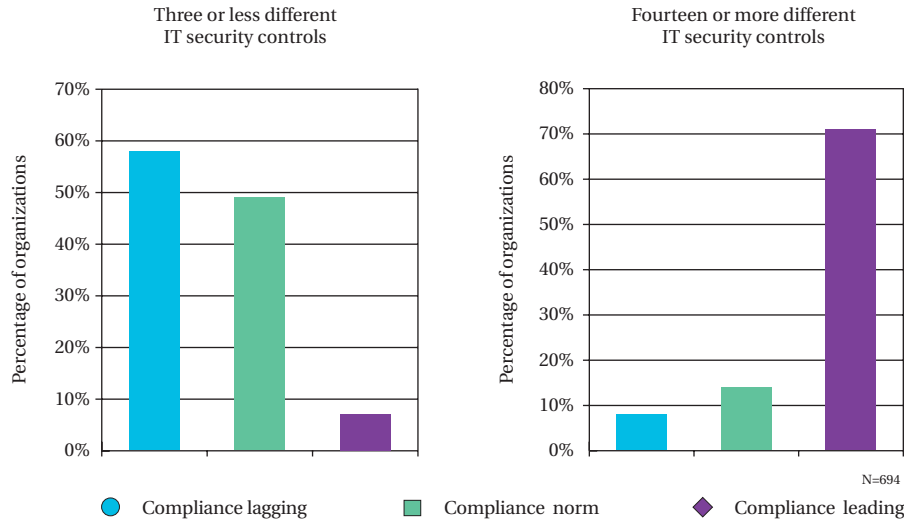


Figure 9. Appropriate number of IT controls: Laggards to leaders

Source: IT Policy Compliance Group. July 2007

Usage of IT controls among the leaders

Seventy-one percent of the leading organizations—the firms with two or fewer IT compliance deficiencies and two or fewer latent data losses annually—are employing 14 or more different kinds of IT security controls. On the other hand, fewer than 7 percent of leaders are employing three or fewer IT security controls.

Usage of IT controls among the laggards

Whereas the majority of leaders are employing many different types of IT security controls, 58 percent of the firms operating as laggards—the firms with 26 compliance deficiencies and 22 unreported data losses annually—are employing three or fewer IT security controls. In comparison, fewer than 7 percent of the laggards are employing 14 or more different IT security controls.

Technical and nontechnical controls

Based on the evidence, it is apparent that the appropriate selection of IT controls and the use of more of them, have been important to performance results among leading companies with the fewest IT compliance deficiencies and latent data losses or thefts. The use of more IT controls has not been the only reason for the success enjoyed by leaders. To learn more about the relationship between the actions taken to improve data protection and results as well as procedural and technical controls employed by leading organizations, see “Taking Action to Protect Sensitive Data,” IT Policy Compliance Group, February 2007.

Fewer control objectives

Control objectives are the policies that organizations establish for compliance and data protection. An example of a control objective might be, “We will not land on the front page or the 11 o’clock news for having a publicly exposed data loss or theft.” Another example might be, “We will adhere to financial reporting requirements mandated by Sarbanes-Oxley.”

Controls, on the other hand, are the procedures, nontechnical and technical, that are put in place to carry out the control objectives. These might include such procedures as separation of duties for transactions requiring authorization or IT technical controls and procedures limiting access to, and protecting, customer and sensitive data.

While the leading organizations—those with the fewest IT compliance deficiencies and the lowest rates of latent data losses—are employing more appropriate IT controls, they also have the fewest number of control objectives compared with all other firms (Table 5).

	Lagging firms	Normative firms	Leading firms
Number of control objectives	82	38	32

Table 5. Number of control objectives

Source: IT Policy Compliance Group, 2007

This apparent contradiction—fewer policies reinforced by more controls—works to the advantage of leaders by focusing on clearly articulated and limited set of objectives that can be more easily communicated to employees and measured and reported across more controls. Although firms in the norm share a similar number of compliance objectives with the leaders, they suffer from higher rates of compliance deficiencies, business disruptions, and latent data losses.

High standards and key performance indicators

The KPIs being measured by leading organizations include:

- Number and severity of compliance deficiencies
- Number and severity of IT security events resulting in business disruptions
- Number and severity of undisclosed data losses and thefts

High standards: Number of events as a percentage of control objectives

The leading organizations establish high standards for key performance indicators. Although not always successful, they target 5 percent of compliance objectives for IT compliance deficiencies, security events, and latent data losses (Figure 10).

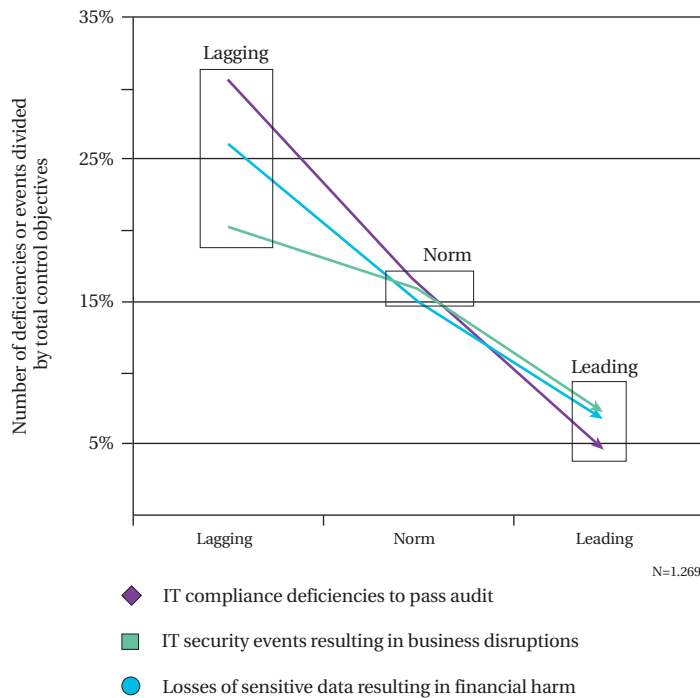


Figure 10: KPI results: Laggards to leaders

Source: IT Policy Compliance Group, 2007

Normative organizations—those with six compliance deficiencies and business disruptions and five latent data losses—are having more difficulty achieving a 5 percent target and are typically operating in the 15 to 17 percent range for the three primary KPIs. The challenge for firms operating in the norm is not the absolute number of control objectives; rather, it is reducing deficiencies and losses to the 5 percent KPI targets.

Firms operating as laggards have more compliance deficiencies, events resulting in business disruptions, and unreported losses of sensitive data. Moreover, they have too many control objectives. To improve results, firms operating as laggards should consider reducing the number of control objectives while also taking actions that will result in the achievement of the 5 percent KPI targets.

More frequent monitoring and measurement

The factor most associated with fewer IT compliance deficiencies, IT security business disruptions, and latent unreported data losses is frequency of monitoring and measurement (Figure 11).

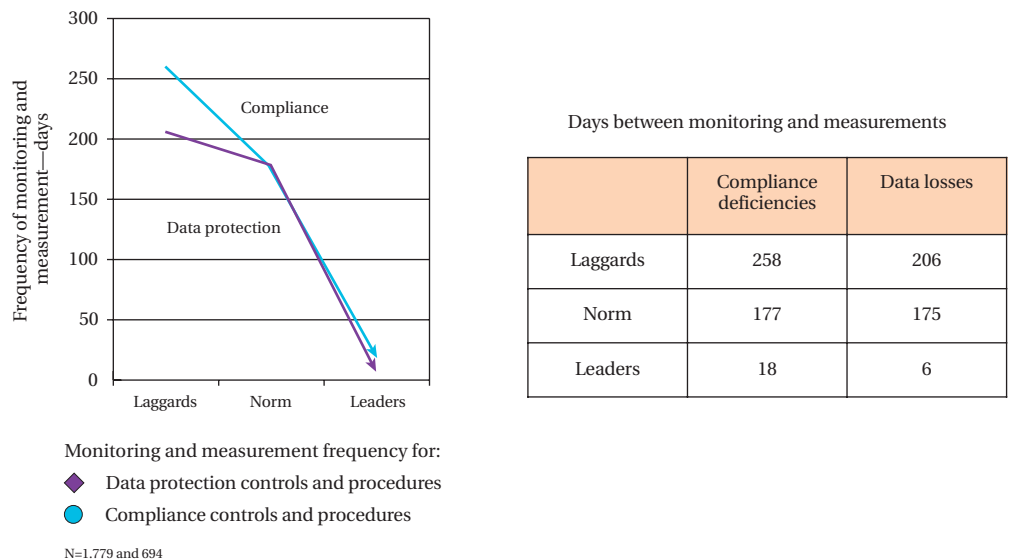


Figure 11. Frequency of monitoring and measurement

Source: IT Policy Compliance Group, 2007

From one benchmark to the next, and across all of the benchmarks, the frequency of monitoring procedural (nontechnical) and technical controls against control objectives is aligned with performance results.

Leaders: Weekly monitoring and measurements

Organizations with the fewest unreported latent data losses and compliance deficiencies are monitoring and measuring controls once every one to three weeks, and on average at least once every two weeks. The rate of monitoring for data losses and thefts averages once every six days among these firms, while the rate of monitoring for IT compliance deficiencies and the potential for business disruptions averages once every 18 days. The average for both is once every 13 days.

Norm: Twice a year

In comparison, firms operating in the norm are monitoring and measuring procedural and technical controls once every 5.7 months.

Laggards: Twice a year to once every nine months

Last, firms with the most IT compliance deficiencies and the highest latent data losses are monitoring and measuring controls once every 6.8 to 8.5 months.

Allocation of spending to automate controls monitoring

There are significant differences among firms in how funds for IT security are being spent to monitor and measure controls. In addition to spending a larger percentage of the IT budget for security, the firms with the fewest latent data losses and least number of compliance deficiencies are reallocating funds from external contractors to equipment and software targeted at automating the monitoring and measurement of controls and procedures.

In contrast, firms with the most undisclosed data losses and compliance deficiencies are spending less of the IT budget on security and are allocating more to external contractors and less to equipment and software. And they are monitoring and measuring controls too infrequently to improve results. For further references on how spending and fund allocation are related to IT compliance results, see “Managing Spending in IT to Improve Compliance Results,” IT Policy Compliance Group, October 2006.

Why compliance pays

Compliance is not only about regulatory audit, as the data loss and theft events at numerous companies have shown in the past four years. Rather, it is about conforming to organizational policies, including the organization’s risk appetite for data loss and theft, business disruptions from IT security events, broad regulatory mandates, and specific industry regulations and audits.

There is perhaps no more urgent compliance objective than to avoid damage to the organization’s brand, especially when such damage results in avoidable negative financial consequences, as it does with the loss and theft of sensitive business data.

The benchmarks show the firms excelling at IT compliance are those with the fewest data losses and thefts. The findings are clear: To avoid, mitigate, or delay negative financial consequences from publicly reported data losses and thefts, it is essential to drive operational excellence in IT by improving compliance results, especially in IT controls and procedures. Further, the benchmarks show that operational excellence for compliance and data protection is improved for those organizations that monitor and measure controls against objectives consistently, at least once every two weeks.

Firms excelling at IT compliance are the same organizations with the fewest data losses and thefts.

The probability of a data loss is once every three years for a large enterprise currently operating as a compliance and data protection laggard. Firms can improve the odds, limiting financial and brand damage to once every 15 years, by improving their compliance posture to keep even with the norm in the industry. Improving the compliance posture of the organization even further, delays the likelihood of financial risk from a publicly reported data loss to once every 42 years—or more—among larger enterprises.

The best news of all is that the amount spent on improving compliance and data protection is a very small percentage of the financial value that is at risk. With returns for larger enterprises starting at 1,000 percent and improving up to 100,000 percent, it is obvious that good compliance pays for itself.

Better compliance—along with data protection—pays for itself through the avoidance of predictable financial risk.

In summary, compliance is good for business. Not only is good governance the right thing to do, better compliance—along with data protection—pays for itself through the avoidance of predictable financial risk.

Appendix A: Probability of publicly reported data losses

The IT PCG benchmarks are a measure of actual latent, unreported data losses and thefts occurring in organizations today. The number of unreported data losses is much higher than the number of publicly reported losses and thefts.

This report uses the Attrition database, available at www.attrition.org, as the basis for determining the probability of an unreported data loss becoming one that is publicly reported. Although the Attrition database contains a few duplicates, the majority of the incidents contained in the database are documented cases that have occurred.

At the time the database was employed to determine the probability of an unreported latent data loss being reported publicly, the demographics of the data set included:

- Nearly 97 percent of the losses occurring in the United States
- Fifty-three percent of the losses are among commercial businesses
- Twenty-seven percent of the losses are for educational institutions
- Seventeen percent of the losses are among government institutions

Based on the public report contained in the Attrition data set, the data losses and thefts are attributed to the following:

- About 35 percent are due to external attacks and thefts.
- About 42 percent are due to theft and fraud, with half due to the theft of laptops.
- About 21 percent are due to accidents.

The method employed to determine the probability of a publicly reported data loss involves the number of reported incidents divided by the number of firms in the sample set. In this instance, the sample set consists of organizations of a given size—based on U.S. Census data for firms of a given size—and the propensity for loss based on latent unreported data losses from the IT PCG benchmarks. U.S. Census data was used because the primary reported data losses contained in the Attrition data set are almost wholly U.S. based. The propensity for data loss, based on unreported data losses from the IT PCG benchmarks, was used to modify the sample space because firms with higher rates of unreported data losses are more likely to experience a publicly reported data loss than firms with fewer unreported data losses.

Appendix B: Financial risks and IT policy compliance

This benchmark quantifies the financial risk for public reporting of the loss or theft of sensitive data. It does not quantify financial risks for noncompliance with other regulatory compliance mandates and organizational policies other than those pertaining to data protection and privacy.

There may be, and in some situations are likely to be, negative financial consequences for noncompliance with an array of other regulatory mandates, including Gramm-Leach-Bliley; laws governing healthcare delivery services, the pharmaceutical industry, the banking and financial services industry, hazardous waste, and workplace employment; Sarbanes-Oxley; Payment Card Industry requirements; risk management practices governed by Basel; and data custody and legal hold requirements governing information.

Based on the IT PCG benchmarks, 43 percent of organizations are subject to only one principal regulatory audit each year. Another 25 percent are subject to two regulatory audits annually, while 32 percent of organizations are subject to three or more. Most organizations (57 percent) are subject to two or more regulatory mandates involving external audit and reporting requirements, including those governing the protection of sensitive data. As a result, the total financial risk involving noncompliance with policy and law is probably understated by the findings presented in this benchmark report.

The financial risks quantified by this report are specific to the public reporting of losses and thefts of sensitive data. Firms should also consider and weigh the financial risks involving noncompliance with specific regulatory audits in evaluating financial returns—as these relate to financial risk—for spending on compliance, business disruptions, data protection, and data custody.

About the benchmarks

The IT Policy Compliance Group findings cited in this report contain data from different benchmarks, as follows:

Financial impact of publicly reported data losses and thefts

The findings covering the expected financial impact of publicly reported data losses are from two benchmarks conducted between November 2006 and March 2007. In total, the sample for these benchmarks consisted of qualified participants from 475 organizations. The expected financial impact findings represent the anticipated financial impact rather than a direct measure of actual impact on these organizations.

Differences between expected and actual experience are documented in this report based on publicly available data for publicly traded firms. Privately held organizations, educational institutions, government institutions, and nonprofit organizations were not included in determining the reliability of the benchmark findings based on the actual experience of firms listed in the Attrition database.

Compliance deficiencies

The findings covering the number of compliance deficiencies that must be corrected in IT to pass regulatory audit are for 1,779 qualified participating organizations and have been averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Business disruptions from IT security events

The findings covering the number of business disruptions caused by IT security incidents are for 1,269 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Risk appetites

The findings covering risk appetite—the financial value firms are willing to sustain in loss before spending additional funds on IT security—are for 475 qualified participating organizations and are averaged across benchmarks conducted between November 2006 and March 2007. The results from the two benchmarks are consistent, which is why the data has been aggregated for this report.

Unreported but confirmed latent losses of sensitive data

The findings covering the number of unreported data losses caused by IT security incidents are for 694 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Number of IT controls

The findings covering the number of IT controls and key performance indicators are for 694 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Number of control objectives

The findings covering the number of IT controls and key performance indicators are for 694 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Frequency of monitoring and measurement

The findings for the frequency of monitoring and measurement for compliance results are for 1,578 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

The findings for the frequency of monitoring and measurement for latent unreported data losses and thefts are for 694 qualified participating organizations and are averaged across benchmarks for the past year. The results from the earliest individual benchmarks are consistent with those of succeeding benchmarks, which is why the data has been aggregated for this report.

Countries of participating organizations

The organizations participating in the benchmarks are primarily from the United States, with 92 percent of the entire sample being drawn from this area. Outside the United States, the other 8 percent come from such countries as Australia, Brazil, Canada, Germany, Japan, the United Arab Emirates, and the United Kingdom among others.

Participants

Twenty-eight percent of the participants in the benchmarks are senior managers (CEO, CFO, CIO, etc.), 12 percent are vice presidents, 37 percent are managers or directors, 20 percent are staff, and 3 percent are internal consultants. Thirty-two percent of the participants work in finance and internal controls, another 29 percent work in IT, 9 percent are employed in customer service, 8 percent are employed in legal and compliance, and the remaining 22 percent are distributed across a wide range of job functions, including sales, marketing, design, development, manufacturing, procurement, and logistics.

Size of organizations

Thirty-three percent of the organizations participating in the benchmarks have annual revenues, assets under management, or budgets of less than \$50 million. Another 35 percent have annual revenues, assets under management, or budgets between \$50 million and \$1 billion. The remaining 32 percent have annual revenues, assets under management, or budgets of \$1 billion or more.

Industries represented

A wide range of industries participated in the benchmarks, including advertising; aerospace; agriculture; apparel; automotive; banking; chemicals; computer equipment and peripherals; computer software and services; construction, architecture, and engineering services; consumer durables, electronics, and packaged goods; distribution, education, financial, and accounting services; general business and repair services; government public administration, defense, and intelligence; health, medical, and dental services; insurance, law enforcement, and legal services; management, scientific, and consulting services; manufacturing; medical devices; metals and metal products; mining, oil, and gas; paper, timber, and lumber; pharmaceuticals; publishing, media, and entertainment; real estate, rental, and leasing services; retail trade; transportation and warehousing; telecommunication equipment and services; travel, accommodation, and hospitality services; and utilities and wholesale trade.

The largest industry segments represented in the benchmarks consist of health, medical, and dental services (10 percent), manufacturing (10 percent), government (10 percent), financial and accounting services (6 percent), education (6 percent), banking (7 percent), retail trade (6 percent), and consumer goods (6 percent). All other segments make up 5 percent or less of the total sample.

About IT Policy Compliance Group sponsors

The IT Policy Compliance Group is dedicated to promoting the development of research and information that will help compliance and IT security professionals meet the policy and regulatory compliance goals of their organizations. The IT Policy Compliance Group focuses on assisting member organizations to improve compliance results based on fact-based benchmarks.

The IT Policy Compliance Group Web site at www.itpolicycompliance.com features content by leading experts in the world of compliance and published reports containing primary research. Research and benchmarks sponsored by the Group produce fact-based insight and recommendations about what is working and why.

The results of Group-sponsored research are designed to help compliance and IT professionals to:

- Benchmark IT policy compliance efforts against peers and best-in-class performers
- Identify key drivers, challenges, and responses to implement successful IT policy and security compliance initiatives
- Determine the applicability and use of automation tools to assist, streamline, and improve results
- Identify best practices for IT policy and compliance programs



Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
+1 (408) 517 8000
www.symantec.com
info@symantec.com



The Institute of Internal Auditors
247 Maitland Ave.
Altamonte Springs, FL, 3270-4201, USA
+1 (407) 937 1100
iia@theiia.org
www.theiia.org



Information Systems Audit and Control Association
3701 Algonquin Road,
Suite 1010
Rolling Meadows, IL 60008
+1 (847) 253 1545
info@isaca.org
www.isaca.org



Computer Security Institute
600 Harrison St.
San Francisco, CA 94107
+1 (415) 947 6320
csi@cmp.com
www.gocsi.com



Protiviti
1290 Avenue of the Americas,
5th Floor
New York, NY 10104
+1 (212) 603 8300
info@protiviti.com
www.protiviti.com



IT Governance Institute
3701 Algonquin Road,
Suite 1010
Rolling Meadows, IL 60008
+1 (847) 590 7491
info@itgi.org
www.itgi.org

Founded in 2005, the IT Policy Compliance Group conducts benchmarks that are focused on the interrelationships between compliance and IT with the aim of delivering fact-based guidance to organizations on the steps that can be taken that will improve compliance results. Benchmark results are reported through www.itpolicycompliance.com for the benefit of members.

IT Policy Compliance Group

Managing Director, Jim Hurley
Telephone: +1 (216) 321 7864
jhurley@itpolicycompliance.com

www.itpolicycompliance.com

July 2007