IT PCG Research Reveals Significant Savings Potential for Information Security and Audit

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[[](http://itmanagersinbox.com/wp-content/uploads/2009/02/4.jpg)](http://itmanagersinbox.com/wp-content/uploads/2009/02/4.jpg)The IT Policy Compliance Group (IT PCG), of which ISACA is a sponsor, today announced the availability of its latest benchmark research report titled, “[Managing Spend on Information Security and Audit to Improve Results](http://www.itpolicycompliance.com/research_reports/spend_management/read.asp?ID=14).”

Based on research conducted with more than 2,600 firms, the study reveals that 68 percent of firms are under-spending on information security relative to the financial risks and losses they are experiencing. Yet incremental increases toward the funding of best practices are responsible for financial returns that can exceed more than 200 percent for most organizations.

The new research, sponsored by the Computer Security Institute, The Institute of Internal Auditors, Protiviti, ISACA, IT Governance Institute, and Symantec Corp. (NASDAQ: SYMC) outlines a risk-based approach to budgeting for information security that rewards results; the practices responsible for managing business and financial risks from the use of IT; and the substantial reductions in spending on audit in IT.

“Like an insurance deductible, all organizations are willing to sustain some level of financial risk and loss from theft of customer data or some level of business downtime from IT disruptions,” said Jim Hurley, managing director of IT PCG and principal research manager at Symantec. “However, the research findings show that an organization’s loss-tolerance is exceedingly low, and the financial returns for small improvements are extraordinarily high.”

Top Business Risks

Firms ranked three business risks from IT well ahead of other possible risks: Confidentiality of sensitive information; Integrity of information, assets and controls in IT; and Availability of IT services. The IT PCG report leverages ongoing benchmarks to measure the performance of firms against these three risk areas. The results of the benchmark surveys can be broken up as follows:

* **Worst Outcomes:** 19 percent of all firms are experiencing more than 15 losses or thefts of data each year, 80 or more hours of business downtime from IT failures, and more than 15 audit-failing deficiencies.
* **Normative Outcomes:** 68 percent of all firms are operating at ‘normal’ levels experiencing between 3-15 losses or thefts of data each year, between 7-79 hours of business downtime from IT failures, and between 3-15 audit-failing deficiencies.
* **Best Outcomes:** 13 percent of all firms are achieving the best results, experiencing fewer than 3 losses or thefts of sensitive information each year, less than 7 hours of business downtime, and fewer than 3 audit-failing deficiencies. The financial returns among these organizations range from 22 percent to more than 3,000 percent annually.

Surprisingly, the difference in outcome between the worst performers and the best performers was not as a result of the size of security budgets. In fact, the differences in size of security budgets were negligible. What mattered was how those budgets were used.

The new report details the following five practices being leveraged by those with the best outcomes and the least financial losses:

* Leveraging a senior management team to manage risk
* Prioritizing risks, improving controls, and automating procedures
* Continuously assessing controls and risks
* Leveraging technical controls, policies, and IT change management
* Comprehensive reporting

Financial Implications

The financial ramifications of these risks were found to correspond almost entirely with the practices implemented by IT to manage the exposure to them. Not surprisingly, firms leveraging the best practices experience the least expensive and most infrequent financial losses. Firms operating at the worst levels paid the price, literally, with data loss and theft equaling 9.6 percent of annual revenue and business downtime costs equaling nearly 3 percent of annual revenue.

Among organizations with $5 billion in revenue, the combined costs from data loss or theft and business downtime ranged from $329 million for firms with the worst practices to $2.25 million for firms who had implemented the best practices – 149 times less.

“Firms can either wait until an emergency pushes them to reprioritize, or they can decide that it is in their best interests to institute these industry proven practices,” said Hurley.

The research found that firms with the best outcomes were actually spending between 35 and 52 percent less on audit fees and expenses. For these firms, adjusting the amount of money spent on practices that reduce risk, loss and audit spending can produce financial returns ranging from 1,000 to 500,000 percent more than the loss which the organizations are willing to sustain.

Quotes from ITPCG Member Organizations

“This report is a clear demonstration of the benefits that organizations can achieve from effective management of security, availability and other IT-related business risks,” said Brian Barnier, member of the IT Governance Institute’s Risk IT Task Force. “Good practices such as the freely downloadable COBIT framework can help organizations take specific actions to mitigate risk and maximize value.”

“As the IT Policy Compliance Group’s research demonstrates, companies that make improvements in managing their IT security risk will realize numerous benefits, including lower financial exposure and losses as well as savings on regulatory audit fees and expenses,” said Rocco Grillo, a managing director in Protiviti’s Information Security & Data Privacy practice. “The group’s findings quantify what has been assumed to be a best practice: organizations with a top-down approach and a clear owner who has line of authority and visibility to the business lines maintain the most cost-effective and comprehensive information security programs.”

About the Research

Topics researched by the IT Policy Compliance Group benchmarks are part of an ongoing research calendar established by input from supporting members, advisory members, and findings compiled recent research. The most recent benchmarks included in this report were conducted between September and December 2008 with 734 separate, qualifying organizations. All of the 734 participating organizations in the most recent benchmarks are from North America, with a majority of these (95 percent) from the United States. A majority of the 2,600+ participating organizations (90 percent) are from the United States. The other 10 percent come from countries in Europe, Latin America, the Middle East, Asia and the Pacific Rim.

About IT Policy Compliance Group

The IT Policy Compliance Group is dedicated to promoting the development of research and information that will help organizations to meet their policy and regulatory compliance goals. The IT Policy Compliance Group focuses on assisting member organizations to improve business, governance, risk management and compliance results based on fact-based benchmarks. It is supported by several leading organizations including: the Computer Security Institute, The Institute of Internal Auditors, Protiviti, ISACA, IT Governance Institute, and Symantec Corporation (NASDAQ: SYMC). More information is available at [www.ITPolicyCompliance.com](http://www.itpolicycompliance.com/).