

Microsoft®
SQL Server 2005**Report: Some Companies Lose Data Six Times a Year**

March 7, 2007

By Lisa Vaas

TJX's massive data loss is just the tip of the iceberg.

Almost seven out of 10 companies—68 percent—are losing sensitive data or having it stolen out from under them six times a year, according to new research from the [IT Policy Compliance Group](#). An additional 20 percent are losing sensitive data a whopping 22 times or more per year.

ADVERTISEMENT

HP Smart Buy nc6320Provides an ideal balance
to maximize productivity.**\$1099***

*After \$300 Instant Savings

Learn More ▶



The ITPCG is a security and compliance policy industry group that counts among its members the Institute of Internal Auditors, the Computer Security Institute and Symantec.

RELATED LINKS[Verizon Service
Combats Web
Threats](#)[New McAfee Head:
We Ain't Just AV](#)[Apple Patches
QuickTime Flaw](#)[What's Bugging
eBay?](#)[Microsoft's OneCare
Finishes Last in
Anti-virus Tests](#)

Between August and October 2006, the group conducted a benchmark of 201 organizations.

About a third of the organizations surveyed have revenues, assets or budgets of less than \$50 million,

with another third worth \$50 million and \$499 million, and 30 percent of the surveyed organizations were worth \$500 million or more. Ninety percent of the organizations were located in the United States.

The good news to come out of the group's survey is that 12 percent of surveyed organizations are losing sensitive data less than twice each year.

Such organizations, those with the least amount of data fumbling, are also those that consider [IT security](#) data and IT-related regulatory data as among the most sensitive data within their domains, according to James Hurley, who directs research at the group and is also a senior research manager with Symantec.

"In the high-90 percent of these organizations that have very few losses consider the IT security-side data as their most important and sensitive data," he said in an interview with eWEEK. "The rest of the universe doesn't value IT and audit information as highly."

As a matter of fact, the respondents that rated financial data as their most important and sensitive data turn out to have high data losses, Hurley said.

"Seven in 10 organizations out there, being most of them, rank things like customer data and other things highly, but few regard nonregulatory auditing data as being of high importance," he said.

The takeaway is that those organizations that focus in on protecting the keys to the kingdom—i.e., those that track who has access to data and also protect the knowledge of how to get access to data—are doing "very well," comparatively, Hurley said.

The most sensitive losses are around customer data, financial data, corporate data, employee data and IT security data, according to the report, titled "Taking Action to Protect Sensitive Data." The report is due to be released March 8.

Another potentially surprising finding is that the leading cause for data loss is user error. Policy violations are the second leading cause, but Internet threats, attacks and hacks only comes in at No. 3.

When it comes to how data vanished, lost devices topped the chart, including loss of PCs, laptops and mobile field devices. The second most common channel of data loss was through e-mail, IM and other electronic means. Software applications, including [databases](#) and the systems they work on, came in as the third most frequent channel through which data is being lost.

Hurley said that one of the most interesting findings of the survey concerns controlled monitoring. What the group found is that organizations doing well in compliance and IT security—which are also those suffering the fewest occurrences of data loss—are monitoring with a variety of controls at least monthly.

"Frequency of monitoring appears to have been stepped up by organizations doing well with lack of high data losses," he said. Those organizations doing poorly aren't paying attention to IT security controls and evidence logs of what happened during a data loss incident, he said.

Another finding: Losing data is expensive. Companies that publicly reported a data loss or breach had to shell out, on average, 8 percent per customer to report the loss, notify the customers and restore the data. The average loss of revenue was 8 percent as well. The cost on average to notify customers and to clean up and restore data was \$100 per record.

There's no silver bullet to stem the loss, Hurley said. Although there's been talk in Washington recently about strengthening reporting laws around breaches and having it tied to a particular technology such as data encryption, the ITPCG found that such steps would only touch the surface of the problem.

Those companies that are doing well, with minimal data loss, reported a host of technologies that have helped them to improve their results.

They're using everything but the kitchen sink to protect data, including Internet threat controls, network access controls, database access controls, IT asset management tracking and configuration management.

"Organizations that did well are using almost all of these things," Hurley said.