New Report Chronicles the Cost of Data Leaks

April 25 2007

A McAfee-commissioned report by the research firm Datamonitor says that 60 percent of respondents experienced a data leak last year.

Researchers at Datamonitor can give corporations 1.8 million reasons to protect themselves against data breaches.

According to the research group's new report, "Datagate: The Next Inevitable Corporate Disaster?", the average cost of a data leak incident is $1.82 million. That figure is based on accounts of 23 percent of respondents - the others were unable to track and audit losses after a breach.

The report surveyed 1,400 IT decision makers across the globe. All totaled, 60 percent of those surveyed said they experienced a data leak last year, and only six percent could state with certainty that they had no data leakage problems in the past two years.

Kevin LeBlanc, group product marketing manager at McAfee, noted that in the physical world, if a piece of merchandise is stolen, it's actually missing.

"In the electronic world, the copy is all the perpetrator needs," he said.

McAfee commissioned the Datamonitor report and is including it in its pitch for McAfee Data Loss Prevention Gateway, a new tool that company officials said will be generally available in late May. McAfee

DLP Gateway prevents data loss from guest laptops, non-Windows systems such as Mac and Linux, servers, mobile devices and all other agentless devices by blocking the transfer of confidential information at the gateway.

One-third of participants in the survey said they felt a data leak could put them out of business, a statistic McAfee vice president and chief technology evangelist Carl Banzhof called alarming. Respondents estimated that it costs an average of $268,000 to inform customers of a data leak, even if the lost data is never used. In addition, 61 percent believe data leaks are the work of insiders.

Phil Neray, vice president of marketing at Guardium, of Waltham, Mass., said enterprises need to monitor all database activity at the network layer and on the database server itself to protect themselves against the insider threat.

Guardium's product, Guardium DBLP, locates and classifies sensitive data and then monitors traffic to and from database servers in search of unauthorized or suspicious activity.

"Most sensitive data is stored in enterprise databases that are at the core of your Oracle Financials, SAP or PeopleSoft systems," Neray said.

"Privileged insiders such as administrators, developers, and outsourced personnel have virtually unfettered access to these data sources. So if you're only focused on preventing leaks as the information leaves your organization at the perimeter via e-mail or IM, you're only going to catch unauthorized or suspicious activities when it's almost too late."