



KPMG ANALYSIS

Data Protection Gets Policy, Tech Backing

July 11, 2007

By Dave Pelland, Managing Editor, Digital Insider

Data breaches that generate unexpected costs and negative publicity are shifting the focus of enterprise security to data protection and stronger policies for accessing and storing that information.

Technology designed to regulate network access and restrict people's activities to their corporate function are expected to improve security, but only if they're installed in conjunction with stronger information policies.

"The future of security is data-centric," said Stephen R. Katz, president of consulting firm Security Risk Solutions, at the June 26 Enterprise Data Protection Forum organized by technology publisher Infoworld.

"Companies have to protect data wherever it is, independently of the infrastructure components that store or transmit the data," Katz said. "Companies will use centrally enforced policies to specify who can see, who can move, and who can modify data."

Pressure to avoid data breaches has been increasing since the enactment of a 2003 California law requiring companies to notify consumers about security incidents. Over the past four years, 37 other states have passed similar laws, said Thomas J. Smedinghoff, a partner in the privacy, data security and information law practice of law firm Wildman Harrold.

The states have differing requirements and mechanisms for triggering the need to disclose a breach, but as a whole have made enterprises more willing to embrace data-centric security.

"These laws have done a lot in general to force the issue," Smedinghoff said. "Before we heard nothing [about data breaches] and we thought nothing was happening."

Smedinghoff also said state disclosure laws have also prompted a shift in consumer attitudes about information protection. In the past, banks or retailers that experienced physical robberies were considered victims, but with data breaches leading to potential identity theft, customers are considered the victims -- and banks and retailers are likely to be blamed.

"There's been a shift in focus," Smedinghoff said. "You have to have appropriate security, and if you don't, you're going to be held liable."

To avoid the costs and publicity associated with data breaches, companies are paying closer attention to how employees, guest workers and business partners access, use and store network data.

"Companies are relatively good at detecting threats that come from the outside, but most aren't as good at detecting inside threats," said C. Warren Axelrod, chief privacy officer of

MORE...

Attachment Spam May Emerge as Malware Vector

AUGUST 8 PDF attachments are the latest effort to evade corporate spam filters, and may foreshadow the use of e-mail attachments as a way to deliver malware.

Selected Technology Company Earnings

JULY 31 Technology and media companies generally reported earnings growth in the second quarter.

Transfer Pricing Risk Hitting Boardroom Agendas

JULY 25 Technology companies face a major challenge in transfer pricing risk as national governments seek new sources of tax revenue.

Product Placement Takes Its Role on the Global Stage

JULY 18 The head of a television studio talks about how product placements are expanding across the globe.

IT Governance Is a Matter of Information Over Technology

JULY 5 A language barrier between audit committee members and technology officers can severely complicate IT risk oversight.

For Better Security, Web Browsers Go Green

JUNE 26 The latest generation of Web browser certificates could help reduce phishing attacks against banks, retailers and other companies.

Growth, Profit and Expansion in the Global Semiconductor Industry

JUNE 18 Gary Matuszak, global line of business chair in KPMG's Information, Communications & Entertainment practice, and Ron Steger, a KPMG partner in the same practice, discuss KPMG's annual Semiconductor Survey.

U.S. Trust. "We're often too free with the availability of data, and don't give those issues enough thought."

Gerit Nel, data security solutions manager for IBM's Global Technology Services, said common causes of breaches range from employees exploring network files out of curiosity to avenging perceived slights. In many instances, workers reveal sensitive corporate information inadvertently.

"We need to invert our security thinking," Nel said. "The traditional view is that we feared outsiders and set up restrictive policies to prevent access. Now we need to understand the value of business data to an organization, and apply policies to protect the value of that information."

According to the Ponemon Institute's research among companies that have reported data breaches, the direct costs of a security incident (which includes the price of notification letters, legal costs and call center expenses) average \$54 per lost record.

Companies are turning to network tools to scan and monitor traffic patterns to identify how business units and partners generate and access data, and instituting policies to ensure there's a business need to employees to access specific data.

Along with improving their security technologies, companies are developing information access and use policies to help them identify what types of data are the most important and carry the highest risk of exposure.

"We're hearing many companies saying they don't know what information they have and who can access it," said Smedinghoff. "Even if third parties are processing your information, it's still your data and obligations to protect it apply [to that information]."

To better protect data, companies are using technologies such as network access control and role-based identity management to give employees the information they need to do their jobs while still blocking them from access to data unrelated to their duties.

"Just because data isn't leaving your firm doesn't mean it isn't being abused," said Stephen Scharf, head of security for financial data publisher Bloomberg LP. "If you only use tools that look at outbound traffic, you're only getting half of the picture. You want to look at file access [patterns] and if data is being copied to flash drives."

Scharf said companies are borrowing techniques from financial management and physical security, such as separation of duties and principles of least privilege, as well implementing training programs on safeguarding information.

"All of these things can be used in effective enterprise data protection," Scharf said. "We're not starting from scratch -- we have common toolsets and methodologies that we can leverage."

U.S. Trust's Axelrod said companies are also reviewing their data retention policies to ensure data isn't kept longer than business purposes or regulations require.

"Different types of information have different retention needs," Axelrod said. "We want to get rid of information as soon as it becomes obsolete, because that reduces the risk of [older] information getting leaked."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

[Submit](#)