

# COMPLIANCE WEEK

---

## **Taking A Holistic View Of Risk And Privacy By Christine Dunn – January 17, 2007**

Companies looking to purchase technology to assist in compliance efforts increasingly are turning to systems that allow them to implement controls for both governance and privacy regulations. "Customers are more mature," says Ron Ben-Natan, chief technology officer of Guardium, a database monitoring and security company. Customers know not to treat each regulation with standalone initiatives, he contends; instead, they bundle them into two groups, governance (think Sarbanes-Oxley) and privacy (HIPPA or SB-1386), and then put systems into place to manage all changes and access to the data.

Their ability to do this reflects, in part, a growing use of risk management techniques to evaluate their corporate processes. Risk management helps organizations accept the truth that an entity can't be completely protected, and teaches them to accept some residual risk, says Paul Proctor, a security and risk analyst at Gartner Research.

"We used to rely on security tools and technology exclusively to protect the organization, and what we ended up with was protecting the organization as much as possible with the available budget," Proctor says. Now companies are purchasing technology and implementing processes that allow them to meet the accepted level of risk, he says.

"Measuring how much risk to accept becomes more important than asking the question, 'Which tools should we buy?'" Proctor says.

A risk management approach encourages business unit managers to work together with their IT counterparts in deciding which technology to purchase. Companies now have compliance teams comprised of people from both the business and IT sides of an organization, Proctor says. Risk management also encourages companies to buy technology with good measurability and transparency features that give companies visibility into how data is being protected and allow managers to evaluate their effectiveness.

### **Making Selections**

In choosing technology, companies must know where their information is located. Executives should conduct an inventory of data assets, assessing where they are and what they're worth. "Understanding the criticality of the data and its contribution to revenue is an important first step," says Steve Adler, of IBM.

Then conduct a quantitative risk assessment. Ask the question: What's the probability, based on past behavior, that this data might be compromised? This will allow the business to forecast potential losses in the future, Adler says. Companies also need a classification system to identify where their sensitive data is located. Ben-Natan warns: "Not all data is created equal."

Next, develop a system to monitor access to the database. Companies are finding that identity and access management (IAM) systems are not sufficient on their own to control access to sensitive data, especially access by privileged insiders such as database administrators and outsourced developers.

For compliance reasons, companies need to have a detailed and secure audit trail of who is monitoring and accessing the data, Ben-Natan says. "People start out doing this for risk management and compliance reasons, but the side effect is [finding out] which applications people are using, which data they're touching, how often, and which users are doing what."

This also helps companies create rules about what constitutes "normal" business processes versus suspicious or unauthorized access to data. For example, a call center representative should be able to use the company's standard CRM application to access a single customer account at a time, but if someone uses a non-standard application, such as Microsoft Excel, to download thousands of records at a time, that should be flagged as suspicious activity.

Companies can use that new information to improve the overall quality of their data, which in and of itself has become a valuable asset—and a potential liability, Adler warns. "It's like currency in the digital economy," Adler says. "When you aggregate data, it becomes more valuable to you and to other organizations that would like to access it."

### **Leveraging Your Efforts**

Once the data is organized, the next step is safeguarding the sensitive data. Companies must first decide who has the right to do things to the data, and whether managers want immediate alerts whenever critical tables are modified. "It's one thing to have data in a database, but if you're making important business decisions with data whose integrity is questionable, it can do more damage than not having any data at all," Ben-Natan says.

Companies must also make someone accountable for the system. "In my experience, it's not enough to have a data governance counselor," Adler says. "Companies need a real leader who can make things happen, build consensus and lead a team."

Adler also says that person should not be a middle manager, but should be an executive who briefs the CEO. And the board of directors needs to understand that given current regulatory conditions, it has a fiduciary responsibility to govern data effectively both from an asset enhancement perspective and a liability perspective. "The onus is on organizations to take a more mature approach" to managing their data, Adler says.

On the privacy side, companies need to look at what kinds of data need monitoring and whether they should report on who accesses and examines the data.

"You can be compliant and still not have good security practices," Ben-Natan says. "On the other hand, if you have good security practices, you will be in compliance."

Adler suggests that companies think at least three years forward when coming up with a technology strategy. He also recommends developing key performance indicators to measure the efficiency of the program. This will allow a company to evaluate the quality of its data and its effect on revenue, as well as analyze the probability and consequences of reducing costs and mitigating risk.

"The natural consequence of governing data effectively is the ability to demonstrate the value of data to the bottom line," he says. "Increasingly, technology is the engine of growth. IT's no longer just a repository of information and human activity. It's the way we interact with customers, employees, the world. IT really is the innovation and growth engine of 21st century business, and data is the gasoline—which is why it is so important to govern its uses correctly."