

COMPLIANCE WEEK

Still A Disconnect Between Compliance, IT

By Christine Dunn

ComplianceWeek

November 14, 2006

It's the disappointing truth about much of Corporate America's IT efforts: Despite years of overhauls, tweaks, and projects, many companies still remain unprepared for lawsuits, audits, or regulatory probes because they lack the IT infrastructure to manage their data effectively and apply it to compliance efforts. So say two recent studies trying to gauge the general unpreparedness of corporate IT departments.

PricewaterhouseCoopers, in a survey of almost 7,800 senior executives at companies in more than 50 countries, found that U.S. and international organizations still struggle with applicable information-security laws and regulations that govern their industries. For example, about 35 percent of U.S. respondents admit that they remain out of compliance with Sarbanes-Oxley—down only slightly from the 38 percent who responded similarly in 2005.

A study by the Business Performance Management Forum and AXS-One found that while most chief executives say their attention on compliance issues has increased in the past six years, less than half of IT executives consider compliance to be a “critical initiative with full management support.” Almost 40 percent of respondents said their company's IT executives don't understand current regulations well enough to implement compliance technologies and policies effectively.

“In our world today we don't get the chance to stop and reflect and think through our approaches,” says Mark Lobel, a partner in PwC's advisory services practice who focuses on IT and information-security issues. “Companies have quarterly numbers to meet, they've got customers pushing for their specific needs, and then all of a sudden the government comes up with SOX. It's easier to comply with the top priorities and deal with what's on your plate first, but that may not be the smart way to approach it.”

Many organizations consciously aren't in compliance because the initiatives they would need to implement can be expensive and time consuming, Lobel says. In any technology purchase, for instance, companies must undergo at least four steps to help find the right product: Identify their business requirements; identify and compare a list of management product vendors; select a solution; and implement the new program.

“Depending on the project, if you're a mid-size organization, that's not a two-month project; that can be a two-year project,” Lobel says. “So it's not surprising that certain organizations are not compliant with certain laws and regulations.”

The legal and regulatory risks of not being compliant include the public embarrassment of being found out and the possibility of losing business, Lobel adds.

Understanding Your Priorities

“There is no question that Sarbanes-Oxley compliance is a high priority for corporate executives,” says Phil Neray, a vice president at database-security company Guardium. “They are committed to it and they are serious about it. And one of the reasons for that is that there are serious consequences to not being SOX-compliant in terms of their companies and their careers.”

But historically, the multi-faceted nature of compliance has left companies’ IT groups in a reactive mode, as they waited to hear instructions from senior management on how to proceed.

That’s starting to change, says Thomas Bookwalter, an adviser to AXS-One and president and chief executive officer of FMDC, a compliance-consulting company. IT executives are learning that they need to take a lead responsibility in a company’s compliance efforts. They have started to ask what’s needed, and take part in decision-making discussions.

“That’s a watershed,” Bookwalter says. “Companies tend to want to focus on one compliance issue at a time, which can cause the holistic view to be missed. Each thing dealt with individually can have great cost. Dealt with collectively, it can have tremendous economy.”

To build a technology infrastructure that responds to compliance efforts, and changes as those efforts emerge, companies must first get their data under control, Bookwalter says. Companies need to know what kind of information they have available in their systems, where it can be found, and how it relates to regulatory obligations. They should establish a corporate policy about how data is handled.

Managing access to critical information has increasingly become a challenge for companies because of changing business models. Practices such as outsourcing or allowing employees remote access to their jobs change the security paradigm of companies, says Wain Kellum, chief executive of Trusted Network Technologies.

“The biggest problem is that IT guys have spent all this money on perimeter systems—firewalls to keep the bad guys out,” Kellum says. “But the business models are changing, and who is in and out crumbled. The whole concept of who is in the network and outside of the network is problematic.”

Kellum suggests that companies physically partition their networks, meaning that employees only have access to those applications and data on the network that they need to do their job. That way, if a company experiences a security breach, the affected section of a network can be closed off, isolated from the rest.

Cracking Down On Good Policies

Companies also should have the ability to keep analytics on a network. While being able to track who went where, and when, on a network is important, being able to figure out who tried to gain access to part of a network, and was denied entry, is crucial, Kellum says

Kellum also expects companies to increasingly encrypt data, not only at rest but in transit, as in the use of email. (Data “at rest” means the information is stored in a hard drive.)

“Those are really the things that if companies make a lot of progress on, they’ve gone a long way to giving people access, but at the same time prevented breaches and a negative material effect on their company,” Kellum says.

Once a company has its data management under control, IT executives should make sure their group knows their regulatory obligations and not leave these requirements in the hands of a compliance officer or records manager, Bookwalter says.

Any technology decisions should be integrated with the business objectives and risk assessment of any company, Lobel says. That way, organizations can identify the gaps between the systems they have in place and the processes they need, and create a plan to mitigate them.

“Our perspective is that security is a risk-based exercise because if you don’t know what risks your organization has, how do you know what controls you should use for compliance?” Lobel contends. “If you just comply to comply, you may be spending too much.”

To increase the likelihood of getting approval for the purchase of new technology, speak to the business concerns of your company in the proposal. Remember, it’s not just about being compliant; it’s about finding efficient ways to implement compliance and reduce the cost and effort of compliance, Neray said.

Look for technology that leverages automation to minimize manual processes, scales across your enterprise, and can grow as new compliance mandates are introduced. Look for technology that can address today’s Sarbanes-Oxley issues and tomorrow’s data governance and privacy issues, Neray says.

“It’s all about monitoring access to sensitive data, especially by privileged users, ensuring that unauthorized access and changes don’t occur, and establishing accountability for those controls,” he says. “That’s common across all regulations and mandates.”

FINDINGS [Sidebar]

An excerpt follows from the study that BPF and AXS-One conducted on the general preparedness of corporate IT departments.

It is estimated that over the next seven years, a company with 20,000 employees will have to save approximately 4.5 billion emails, and have the ability to search through all of them on a timely basis when required to for compliance and/or litigation support. Why then, if the failure to produce electronic communications can be so damaging, is there a lack of urgency in putting mechanisms in place to mitigate e-discovery risk?

For one, Sarbanes-Oxley looms large. Companies are spending millions on technologies and human resources on SOX. One CEE task force member with a large information services company says a dozen staffers do nothing but SOX and internal audits. As for management of

electronic content, he says, “We don’t have any specific regulations around it, and so far we’ve been able to locate and produce communications we’ve needed. But given the frequency of litigation, it’s definitely something we need to think about.” Clearly, SOX can’t be used as an excuse to ignore other compliance issues. A second distraction is the recent focus on the protection of the privacy of sensitive personal information. Already, 26 states have passed laws relating to the protection of personal data about their residents. As a result, many companies are focusing their compliance dollars on this problem. Interestingly, archiving enhances the abilities of companies to apply identity management and encryption to its sensitive data.

Another reason why electronic content management is not top of mind is many executives believe that existing computer back-up systems are effective enough for storage and retrieval of emails and other documents. There are, however, key operational and compliance advantages featured in email archiving applications that are missing in traditional backup systems. To name a few:

- Substantial reduction in storage costs
- Easier establishment of audit trail and chain of custody
- Control over inappropriate or illegal content
- Quicker response times to discovery orders
- Increased data and privacy protection
- Optimal system performance
- Improved employee productivity

Specifically, archiving saves up to 90 percent in storage, and can significantly reduce the conservative estimate of 15 minutes per day per employee that’s lost just in mailbox management—the equivalent of 625,000 hours of lost productivity per year in an organization with 10,000 employees. All of these drivers help minimize legal risk and negative publicity that invariably follows an investigation.

Compliance-savvy companies are putting such systems in place. But as this study shows, the majority has yet to do so. To get started, companies must first identify and quantify the risk of not having a planned approach to the archiving of electronic communications. Then, specific corporate messaging policies must be crafted as part of an overall risk management plan. A practical strategy needs to be set to store large volumes of historical communication— with the ability to easily search for and retrieve specific e-mails and documents.

Is there a financial upside to such implementation? The General Counsel Roundtable finds that each additional dollar of compliance spending saves an organization, on average, \$5.21 in heightened avoidance of legal liabilities, harm to the organization’s reputation and lost productivity. Furthermore, ask Morgan Stanley executives if a robust electronic document archiving system would have paid for itself given the \$1.45 billion judgement against them.

The notion that companies are ill-prepared for such compliance issues in and of itself is not surprising. But the low level of preparedness is a cause for concern. There will be litigation and there will be legal discovery issues. Companies would serve themselves well to take stock in their current e-discovery policies and technologies, before a nightmare scenario strikes them.

Source

CEE: The Future: Building the Compliance-Enabled Enterprise (Business Performance Management Forum; 2006)