

March 15, 2004

## Dangerous disconnect

### Companies risk non-compliance with Sarbanes-Oxley by ignoring asset protection

*Aftershocks of the corporate ethics scandals of recent years continue to reverberate through American society. Several of the senior executives involved are only now facing trial and judgment, continuing to make headlines as their public upbraiding warns others against similar misconduct. Meanwhile, nearly two years after the passage of the Sarbanes-Oxley Act of 2002, public companies across the United States—as well as foreign corporations traded on the U.S. markets—are scrambling to comply with the final guidelines issued by the U.S. Securities and Exchange Commission (SEC) in June 2003. Just last month, the SEC extended the compliance date for the legislation's internal-control provisions in recognition of the monumental task public companies face.*

*The act has received acclaim for promoting sound corporate governance and helping to ensure ethical conduct in business transactions. Much of the recent publicity and discussion regarding Sarbanes-Oxley compliance has focused on Section 404—the provision that requires both management and the external auditors to report on the effectiveness of internal controls in annual reports. These provisions have an immediate impact on the security function: **Among the controls that the SEC guidelines explicitly include are controls over the safeguarding of company assets.** Not only do companies have a responsibility to employees, customers and shareholders to safeguard their assets, but implementation of the Sarbanes-Oxley Act will also require management to document, test, and certify in its annual report to the effectiveness of those programs. To be considered effective, the controls must be strong enough either to prevent losses that could have a material effect on the financial statements or to detect on a timely basis losses that have occurred. Identification of a single “material weakness” would be unacceptable because it would preclude finding the controls “effective.”*

*This report discusses the implications of Section 404 for the security function and the need for security officers to be involved in company 404 compliance measures.*

### Dangerous disconnect

In the nine months since the SEC released its final guidelines on implementing the legislation's provision on internal-control reporting, U.S. public companies have scrambled to document and test their accounting and control procedures, and for many

organizations, the bulk of the work lies in the months ahead. The SEC acknowledged the enormous scope of the initiative just last month, when it extended the compliance deadlines. The applicable deadlines for larger companies deemed “accelerated filers” was pushed back five months; the deadline for smaller companies and foreign private issuers was pushed back an additional three. These two groups must now report on the effectiveness of internal controls in the first annual reports for fiscal years ending on or after November 15, 2004, and July 15, 2005, respectively.

The need to extend the documentation and testing process to the protection of physical and information assets, however, may be overlooked—presenting potential control weaknesses. The adopting release issued by the SEC last June clearly includes safeguarding of assets as one element of “internal control over financial reporting.” Even so, a dangerous disconnect exists between the senior leaders responsible for Sarbanes-Oxley compliance and the managers who are executing the mission.

Asset protection may have received little attention in compliance efforts. “I can't imagine that anyone in management is not absolutely focused on Section 404, but physical security is not the first thing on their minds,” said one person with compliance experience as an audit committee chairman. “The biggest thing on their minds right now is not only whether their internal control is effective, but how do they document and test all of their processes in the time remaining?”

Further contributing to this possible oversight is the fact that many organizations do not involve the security department with asset protection until after a loss occurs. According to a security director with decades of leadership experience, companies often relegate inventory control and other forms of asset protection to the warehouse operation or production facility directly involved with storing or producing specific assets. “They don't ask for advice—they just set up accounting

(continued on next page)

---

## Dangerous disconnect

### Companies risk non-compliance with Sarbanes-Oxley by ignoring asset protection

(continued from preceding page)

procedures, and that's done with no interaction with security," he said. "If something is missing, they make a phone call to security, and that's the first time that security is notified."

Despite the connections between Sarbanes-Oxley and security, a recent survey of 489 chief security officers revealed that only 42 percent of companies affected by the law have taken security measures directly related to the legislation. Only 27 percent of the polled security executives have an active role in their organization's compliance program.

#### Sarbanes-Oxley compliance

Enacted into law on July 30, 2002, the Sarbanes-Oxley Act, in Section 404, requires public U.S. companies and foreign private issuers to publish in their annual reports a management assessment of, and report on, the company's "internal control over financial reporting."

The final SEC guidelines clarified the definition of "internal controls" referenced in the legislation. The SEC adopting release states that "internal control over financial reporting" includes, among other things, "those policies and procedures that . . . provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements." According to the adopting release, the SEC specifically included this provision to clarify that asset protection is part of internal control over financial reporting. "You've got to have reasonable control over your material assets or, at the very least, sufficient controls to detect breaches prior to the issuance of financial statements," says the audit committee chair.

The legislation places greater accountability on organizations to assess the effectiveness of the security program. Now, management not only has the responsibility to ensure diligent protection of company assets, but also must acknowledge its

responsibility and document, test and report upon, the effectiveness of these systems in the company's annual report, disclosing any "material weaknesses" identified in the assessment. If any "material weaknesses" exist, management cannot certify their control system as "effective."

Management certification alone does not satisfy the act's compliance requirements. The legislation further mandates that an external auditor review management's documentation and tests. The auditor must then assess the internal system of controls and provide independent validation of its effectiveness, providing further incentive for an organization to ensure the integrity of its internal controls.

The legislation imposes significant consequences for non-compliance, expanding the scope of and stiffening criminal penalties for certain violations. Chief executive officers and chief financial officers have an obligation to ensure the accuracy of all public filings, including the documentation of the internal controls. Willful failure to disclose this information accurately may carry fines of up to \$5,000,000, prison sentences of up to 20 years, or both. While the law specifically holds chief executive officers and chief financial officers accountable for certifying financial statements, many firms have implemented internal controls that require successive levels of management to certify their reports before submission, thereby distributing accountability throughout the organization.

#### Proactive assessment

Prevention is more effective than remediation. While timely detection of breaches may satisfy compliance requirements in some instances, relying on an asset-monitoring system could cost more than implementing security measures to avert loss in the first place. Companies must work now to ensure efficient functioning of all processes related to the internal-control system.

Given the extensive publicity received both by the Sarbanes-Oxley legislation and the senior

---

executives indicted for their misdeeds, today's C-level leaders—the chief executive officers, chief financial officers and chief accounting officers—are extremely concerned with Sarbanes-Oxley compliance. Some companies have invested hundreds of thousands of dollars in consulting fees and security technology to ensure their financial-reporting systems meet legislative requirements. At the same time, many middle managers may not understand the complex legislation; they also may not understand how a poor security decision can represent a potential liability for the organization and its executives. In fact, financial incentives that reward budget savings could sabotage the compliance effort by encouraging managers to select low-cost security solutions that may jeopardize the integrity of the internal controls.

Because the definition of “internal controls over financial reporting” in the SEC guidelines explicitly addresses the safeguarding of assets, companies may have an implicit obligation to perform due diligence in selecting the partners that protect their assets. This responsibility could become a factor regarding both physical security of company assets generally and computer security, specifically—especially with regard to ensuring the integrity of an organization's financial data. Firms must be sensitive to protecting the computers and network components housing their financial reporting information through effective physical and procedural security.

Another potential disconnect lies in the fact that many organizations separate the responsibility for information technology (IT) security from the overall corporate security department. Such separation makes sense in many respects since IT security requires highly specialized knowledge that does not necessarily relate closely with the physical security realm. Even so, consultation with corporate security can prove very beneficial in creating an effective overall policy to govern security procedures, audits and investigations concerning a company's electronic assets. A col-

laborative relationship between these two entities can help an organization ensure the effectiveness of the total security program, ultimately strengthening the Section 404 compliance effort.

One way to approach this extended compliance responsibility is for companies to perform a comprehensive risk assessment that specifically identifies and corrects potential vulnerabilities in information security, as well as the overall corporate security effort, which also contributes to the protection of electronic assets. “Corporate security has to get more involved in the planning and the requirements of Section 404,” said the security authority cited above. “Companies have to include their security manager in all aspects of the program so that corrections can be made periodically. Not doing this, they're missing a great oversight tool by not involving the security mind.”

Failure to protect an organization's assets by either neglecting the risk assessment or not adequately testing the effectiveness of the security controls implemented could produce far-reaching consequences beyond non-compliance with Section 404. Managers should consider the potential impact of a workplace violence incident on the premises or the two-day loss of a key computer system due to hacking. Such a security breach would create extraordinary costs in terms of business interruption, legal fees, public relations and crisis management costs, increased insurance premiums, and lost shareholder and customer confidence—all factors that can have a negative effect on shareholder value, if the company even survives. A security failure that forces a company to put business on hold for eight, 12 or 24 hours could produce catastrophic results. Today's global market demands business recovery in minutes or, at most, a few hours, depending on the organization and its industry. Beyond compliance with federal guidelines lies the fact that a grave misstep in a company's security program could ultimately lead to its destruction.

**(continued on next page)**

## Dangerous disconnect

Companies risk non-compliance with Sarbanes-Oxley by ignoring asset protection

(continued from preceding page)

### Legislation compliance

To ensure compliance with the new federal guidelines, companies need to analyze the corporate security program and identify vulnerabilities that could compromise the assets and systems involved with the internal controls over financial reporting. The following steps can help in this effort:

- **Educate all management levels on Sarbanes-Oxley compliance.** Managers may believe that the legislation only affects the finance and accounting functions within an organization, not realizing that the act has much broader implications for the overall safeguarding of the company's assets. The security directors and purchasing departments, in particular, need to understand that senior management must report on and attest to the effectiveness of the systems and procedures they use to protect corporate assets. Any management team would be extremely embarrassed, at the very least, to have to disclose a "material weakness" that would prevent it from certifying the effectiveness of its internal-control system.
- **Establish and exercise a comprehensive security plan.** Companies must take a comprehensive approach to security and create a detailed plan of action. For some firms, this step requires working with the security team to manage physical assets, such as product inventory; for others, it means developing a collaborative effort between the IT and security departments. Companies must practice the established procedures on a regular basis to ensure their effectiveness—a critical step that will serve management well as they document their internal controls for the annual report.
- **Monitor the systems and procedures that protect the accounting system.** The corporate security department can serve as an important ally in verifying adherence to an identifiable chain of control in accounting procedures.

While performing patrols, security personnel can assist in managing and documenting inventory. Security can also help investigate reports of unusual or suspicious incidents by maintaining detailed employee access logs. One control involves entrusting separate personnel to perform functions such as authorizations and payments; by including the security department in the planning and implementation of procedural security, security employees can help ensure policy adherence.

*The message is clear: the American people will not tolerate impropriety by the nation's corporate leaders. Greed and betrayal have eroded the confidence that U.S. workers and consumers once placed in the business community, and firms must now tread lightly to avoid a backlash that will make legislative penalties appear comparatively light.*

*As they assess their respective organizations' progress toward compliance with Section 404 of the Sarbanes-Oxley Act, C-level leaders must make sure that middle management does not unwittingly undermine their efforts by overlooking certain aspects of the internal control chain. The overall security program—particularly the systems and procedures that protect the firm's electronic assets—must be evaluated to ensure the integrity of the financial data and to identify any potential misappropriation of resources. This critical task requires widespread cooperation throughout a company; in the absence of such cooperation, senior executives could face potential liability.*

*Recent headlines demonstrate that the stakes at hand are no less than the company's viability, which can have an impact on employees, shareholders, reputation and the ultimate future of the brand.*



The Lipman Report Editors