Sarbanes Oxley and IT
– Threat or Opportunity?

Lee Thornbury J.D.

Maxelerate Systems Ltd.

Sarbanes Oxley and IT – Threat or Opportunity?

By Lee Thornbury J.D.

In 2002, Congress passed, and the president signed into law, a House bill sponsored by Representatives Sarbanes and Oxley. The bill was designed to combat financial crimes and fraud committed by corporate insiders, and to motivate senior executives and corporate board members to pay closer attention to what happens inside their own companies.

While this legislation appears to address just financial aspects of business, Information Technology departments are indispensable and crucial members of the compliance teams for companies. Working with other departments such as legal and accounting, the IT team is often in the best position to determine the current state of their company's IT systems security and integrity, as well as providing analysis and recommendations on ways to improve, correct, enhance or implement the systems. In fact there is a surprise area where IT could be directly implicated in Sarbanes Oxley violations.

What is Sarbanes Oxley?

The Sarbanes Oxley Act of 2002 (SOX, for short) is the federal government's response to corporate scandals such as Enron and WorldCom and other public company debacles that prominently featured fraud, embezzlement and looting of corporate assets by top management in giant corporations. It left them teetering on or falling over the edge into bankruptcy and devastating the financial lives and conditions of the company, their employees and stockholders.

SOX was designed to force executives and corporate boards to more closely monitor what was going on inside the henhouse. The Act requires, among other things, that a company's principal executive and financial officers, as well as the board of directors, certify that they have implemented internal controls to regulate the accuracy and security of the company's financial information and reporting. Further, SOX requires audit committees to maintain internal controls for a company's financial systems and to have those controls audited and certified by public accountants. SOX also requires companies to set up procedures for detecting, investigating and addressing internal and external allegations of fraud, establishes protection for whistleblowers, and mandates the implementation and enforcement of a corporate code of ethics.

SOX affects all public companies, both US and foreign, that are registered under the Securities Exchange Act of 1934, and therefore regulated by the Securities and Exchange Commission (the SEC). It also directly affects those companies' directors, officers, employees, lawyers and accountants.

Violations of the Act's provisions can lead to criminal prosecution of and jail time for the principal executive and financial officers of a company, as well as substantial fines running into the millions of dollars. In other words, the top brass now has a personal stake in this.

What about private companies?

SOX specifically target publicly-held companies for regulation and enforcement. However, street chatter recommends that private companies be familiar with SOX regulations and examine their own companies against the SOX measuring stick. Indirectly, non-publicly held companies have a new opportunity to measure and enhance their own corporate and IT security and integrity. That's just good business.

How does SOX apply to IT?

While SOX does not directly address IT in its rules and regulations, IT is intimately involved with SOX corporate compliance. SOX requires the establishment and constant monitoring and review of internal controls designed to protect the security, integrity and accuracy of a company's financial reporting systems and procedures.

Okay, that's pretty clear about minding the company store with respect to the financial end of a business. Here's where the IT part comes in. A substantial majority of a company's financial reporting, data, and information are generated, changed, housed and transported by the IT systems. If management is going to have to sign their name on the dotted line and verify to the SEC that their financial housekeeping is completely in order, management is dependent upon the security, performance and integrity of the IT systems to protect, detect, enforce, report and verify financial data.

What specifically does this mean relative to IT?

It means that companies have to check and make sure that not only are the traditional paper processes covering financial information and recordkeeping is in compliance with SOX, but also that the IT processes and systems are compliant. The certifications by senior management are dependent upon good records, both on paper and electronically.

It also means that IT systems must be accurate and secure to ensure the integrity and reliability of financial information and records. IT procedures can be put into place to prevent, detect, identify, and report problems such as fraud. The SEC commented that "internal control" means more than just the accounting functions of a company. It also must include policies and procedures that "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [company's] assets that could have a material effect on the financial statements." (68 Federal Register 36636, 36640, June 18, 2003). This can include security breaches of data and/or financial information, intellectual property theft, misappropriation of customer information, and unauthorized use of third party software.

Talking of assets, here is one area where IT could be directly implicated in SOX violation: a public company experiences a surprise audit by one of their software vendors. The audit has been triggered because the vendor was sued for allegedly using the intellectual property of a third party (the software product), and as part of the discovery process, the vendor has to disclose its licensees and the terms of the license, including authorized use and copies. The vendor audit turns up unauthorized use of the software by company employees, and unauthorized copies of the vendor product running on the company's systems, leading to company liability to the vendor and possibly the third party (depending on who is the actual owner of the intellectual property) for license fees, audit fees, and intellectual property infringement damages, not to mention the cost of litigation to sort this mess out. SOX requires the senior executives and board to disclose

to the SEC, in documents available to the general public and the press, how this snafu might affect the financial condition of the company.

What can IT do?

One specific directive of SOX is that senior management, directors, and auditors (both internal and external) are required to certify under their individual signature in annual and quarterly reports that (a) they have reviewed the company's financial records and reports and believe them to be true and accurate, (b) the reports fairly represent an accurate picture of the financial condition and financial information of the company, (c) they have established internal controls that protect and ensure the accuracy and integrity of the financial information, and (d) these internal controls also make sure that all material financial information about the company is made known to the company's senior management, officers, directors, and auditors (see Section 302 of SOX).

IT can conduct an investigation into what IT systems and programs are currently in place that (1) produce the information and data directly relating to the financial statements of the company, (2) the security controls that are in place to ensure the accuracy and integrity of the company's financial information, (3) make sure the financial information gets routed to the appropriate people, and (4) report and contain breaches of this system, both from the inside and from the outside, and preserve all records relating to any such incidents.

IT can also make recommendations on modifications or additions to the IT systems that will increase the security of the IT systems and financial data of the company. SOX also requires active and ongoing monitoring of the "internal controls" that protect and preserve the financial data of a company. IT can assist here by designing programs and infrastructure that will monitor and report any problems, as well as assisting the company's internal and external auditors in collecting and reporting the company's compliance with SOX directives.

And speaking of monitoring internal controls, remember your own responsibility for IT assets. Practice good IT asset management. In particular make sure that all your software is properly accounted for, licensed and registered.

Conclusion

Now that top executives are personally responsible for the design, implementation, and maintenance of "internal controls" protecting and defending the accuracy and integrity of a company's financial information, executives and boards are moving quickly to figure out what to do to find and fix any problems. IT is an integral and indispensable member of any corporate team tackling SOX compliance.

The SEC looks favorably upon companies who implement self-policing measures, self-report any misconduct, take proactive steps to monitor, modify and improve their processes, and cooperate with law enforcement officials (see SEC Release 2001-117). IT departments stand in the best position to investigate, facilitate and design solutions for companies moving into compliance with SOX regulations.

This means that the IT environment must include controls to ensure the overall performance and integrity of a company's IT systems as they interact with and affect financial systems and business process application controls. Further, strong technical safeguards that prevent violations of policies and procedures will strengthen the effectiveness of the overall IT control

environment, significantly reduce initial compliance and subsequent testing costs, mitigate risk within the IT environment, and enhance the overall quality of business operations. Talk about wearing the white hat!

Maxelerate's goal is to help Sourcing, Procurement, Purchasing, Engineering, IT and other professionals in all industries and government agencies to get better deals from suppliers. We accomplish this by providing Consulting, Training, Seminars and Leadership Implementation.

To get more information about us and find out how you can get better results contact us at:

MAXELERATE
Maxelerate Systems Ltd.

1600 Golf Road, Suite 1200
Rolling Meadows IL 60008
Phone Toll Free: (866) 855-5335
Phone Direct: (847) 483-5014
Fax: (847) 483-5015
e-mail: BusDev@maxelerate.com