Storage, Security, and SOX

By David Miner and Mike Marchi

Perhaps not since the U.S. securities laws of the early 1930s has a piece of legislation had such an impact on corporate America as the Sarbanes-Oxley Act of 2002 (SOX).

The law calls for publicly traded institutions and accounting firms to:

- Have management sign-off on the veracity of financial statements [Section 302],
- Document and test internal controls and procedures for financial reporting to ensure that each and every business transaction that feeds the financial statement will have to be safeguarded against operational risk, including fraud and errors [Section 404]
- Maintain record retention for seven years [Section 802].

Along with rigorous reporting, section 409 mandates that institutions will have to report in "real time," material weaknesses that may impact financial statements and events that are found to impact financial statements. These weaknesses could be losses that are the result of lax controls or of business events. In summary, SOX is driving new standards for institutions to ensure that key information is secure and available.

Different aspects of SOX are driving specific technologies. For example, the main security driver for SOX is information integrity—or ensuring the integrity of information for the financial reporting process. Storage solutions must support information integrity through secure backup and data permanence capabilities while also enabling fast recovery for the "discovery" of information.

As a result of SOX and other industry and government regulations, the line between security and storage is beginning to blur. With data protection, availability, and recovery as key objectives in meeting regulatory requirements, the convergence of information security management and information storage management represents an effective compliance solution.

Assess, Protect, Retain, Recover

Enterprises are scrambling to put the best practices, policies, and technologies in place to address SOX compliance issues. For example, to proactively identify and isolate threats in order to minimize their impact on business information and infrastructure, enterprises are implementing intrusion detection systems, integrated security solutions, antivirus, discovery tools, and incident management software. Vulnerability detection requirements are met with the help of policy and compliance managers, vulnerability assessment tools, deployment solutions, and backup and recovery software.

SOX is also driving institutions to evaluate their storage systems and technologies. After all, the intent of the law is not just to keep financial information secure, but to keep it available as well. From an IT perspective, meeting the requirements of SOX means that financial records must remain protected at all times, that secure and up-to-date financial data is backed up and retained, and that these secure and reliable records can also be retrieved in the event of an audit. An enterprise must not only document and have sign-off on their internal controls, but also maintain an immutable record of all information considered material to the ongoing operations of the enterprise for long periods of time.

Sound compliance begins with strong corporate policies for security and storage that are linked to the institution's corporate goals and business strategies. This requires the input not only of individuals in the finance, legal, and compliance departments, but also of IT and personnel from each line of business. Processes and procedures must be identified and documented that demonstrate compliance with SOX requirements. And reporting and validation processes and tools must be established to provide evidence of ongoing compliance.

So Much Data, So Little Time

While SOX does not specify which types of records should be retained or for how long, or how quickly archived records should be recoverable, it also does not rule out certain types of information. As a result, many organizations are opting for the "better safe than sorry" approach by choosing to include the security and storage of more rather than less data in their compliance efforts. Records-retention regulations often require that e-mails, documents, audit information, and other files be archived on WORM (write once, read many) media. In the past WORM tape or optical solutions have been used to provide support for regulatory compliance. These legacy solutions have not only proven to be expensive in terms of management, but also lead to relatively slow and complex retention and restore processes. In comparison, WORM technologies now available on high performance magnetic disk arrays not only enable granular and low overhead implementation of retention policies, but also provide cost-effective and fast access to archived records when required.

Needless to say, the volume of data to be securely retained can be massive, particularly since the amount of corporate data steadily increases year after year. This mountain of information must be stored on an infrastructure that mitigates the risks associated with regulatory compliance while still ensuring high availability and performance.

But threats to information can appear seemingly out of nowhere and put information assets at risk in an instant. The Slammer worm of 2003, for example, infected 90 percent of unprotected servers in just 10 minutes. Even though Slammer exploited a vulnerability that had been disclosed more than six months earlier, giving IT organizations a fair amount of time to patch systems, it still spread at lightning speed.

©2005 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

Today, zero-day threats appear to be just around the corner. These threats, so named because an exploit actually appears before vulnerability disclosure, are likely to move even faster as they spread without restriction across unpatched systems throughout the Internet. Currently, the average time between the disclosure of a vulnerability and the release of an associated exploit is just 6.4 days, according to Symantec's most recent Internet Security Threat Report—a significant difference from Slammer's much larger vulnerability-to-exploit window.

To add to this challenge, most institutions have come to rely on tape backup mediums that are already stretched beyond their limitations to protect and archive important data such as e-mail. If this information is deleted, it could take days, if not weeks to recover important information. In the case of a regulatory audit or discovery in a legal matter, e-mail needs to be produced in hours, or stiff penalties can follow. A recent challenge is the threat of tapes being lost or stolen where corporate and customer information could be exploited.

In such a climate, ensuring the integrity of financial records is a real challenge—especially in IT organizations with limited storage staff and no plans for adding more personnel. For these institutions, the task to do so much more with so few resources appears to be insurmountable.

Easing Compliance

To ease the burden of ensuring compliance with the requirements of government regulations such as SOX, IT organizations must be able to leverage data protection and data storage technologies to provide more proactive, automated tools. Also, the IT team and the chief information security officer (CISO) should enlist the support of the business process owners throughout the enterprise as well as the external auditor to ensure that plans can be put in place and compliance goals met.

An effective compliance solution includes security monitoring tools such as early warning systems that deliver personalized alerts about vulnerabilities and malicious code to keep organizations informed about potential new threats. By delivering notification of vulnerabilities and exploits as they are identified, an early warning system gives IT organizations timely, actionable information and guidance to help mitigate risks before they are exploited.

But that's not all. When the early warning system detects a new, applicable security threat such as a virus, worm, Trojan horse, or blended threat somewhere in the world, it triggers backup and recovery tools to automatically increase the backup frequency of relevant desktops and servers to networked storage systems. Moreover, the backup and recovery system quickly captures frequent point-in-time snapshots of the operating system of the entire server or desktop, without interrupting user productivity or application usage. These point-in-time snapshots include all files and volumes, applications, and settings in a single file.

And the solution doesn't stop there. Based on the compliance policies defined in the backup and recovery system, the solution then notifies data permanence software which data should be saved to meet regulatory requirements and how long it should be saved on the network-attached storage system, if encryption or a copy to a remote site is needed. Backup and recovery solutions commonly available with disk-based archival solutions enable enterprises to recover quickly from unexpected disruptions, resulting from security issues, hardware or software failures, or simple human error or theft. At that point, even if a storage disk or tape is physically removed, the data remains safe and satisfies the records-retention requirements such as those outlined in SOX.

Then, when the risk has been mitigated by the creation, release, and deployment of security updates or virus definitions, the system is notified to return to its normal backup schedule.

The compliance solution also ensures timely response should records be requested. Whether accessibility must be available within 48 hours of a request, as many interpret SOX requirements, or even less, stringent recovery time objectives can be met by rolling back systems to a point-in-time without taking hours to rebuild systems and restore data using traditional recovery methods.

A Look to the Future

The challenge of demonstrating compliance with SOX and other government and industry regulations offers organizations of all sizes an opportunity to boost their bottom line with improved business process and customers perceiving their information is safe and secure. Regulatory compliance is not optional, and failure to comply can bring penalties and fines, loss of customer confidence and corporate reputation, and more.

At the same time, the benefits of meeting high data availability, permanence, and security standards enable organizations to mitigate risk, simplify data management, and increase profitability. By leveraging security and storage technologies in evolutionary ways, organizations can gain a competitive advantage that enhances their business not just today, but into the future as well.

David Miner is Director of Financial Services at Symantec Corporation and Mike Marchi is Senior Director of Marketing at Network Appliance.

The ISSA Journal

©2005 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.