

CHOOSING THE RIGHT TECHNOLOGY RESELLER CAN KEEP YOU OUT OF JAIL

By Joseph Marion

This week, Cardsystems Solutions got in a lot of “hot water” for failure to safeguard millions of Visa and Mastercard records. On June 17th, Former Tyco International CEO Dennis Koslowsky and finance chief Mark Schwartz headed for prison for partially for violation of Federal compliance regulations in connection with honest financial reporting and safeguarding of corporate records.

The new laws that enable the stricter Federal regulations have as their centerpiece the Sarbanes-Oxley (SOX) Act of 2002, but there are an estimated 10,000 to 15,000 regulations that businesses must deal with today to avoid being out of compliance in some manner. It isn't always as easy as identifying extravagant parties and \$6,000 shower curtains as in the Koslowsky case. Many times, conformance with the new compliance regulations has more to do with how the backups were run, where the data is stored and protected, and how well documented and consistent are the practices associated with data protection.

Why should IT Managers Care?

IT Managers who are found to not be in compliance with this new Federal legislation face jail sentences and large fines for non compliance. In order to comply with SOX, the technology reseller industry anticipates a large investment in IT infrastructure to meet mandated regulations by Congress, the Security and Exchange Commission, Federal Drug Administration, Commerce Dept, DOD and other banking and financial oversight agencies. This investment will come in the form of the purchase and leasing of equipment and software.

The SOX set of regulations, more than any other, are having the greatest impact on the new world of compliance. That is because any company with market capitalization greater than \$75 million came under its jurisdiction last year and those with smaller market capitalization are due to fall under it by mid-July this year.

If your company has an exit strategy of being bought by a public firm, you **MUST** meet SOX compliance regulations in order to be considered a desirable candidate for merger or acquisition.

The Regulations

Some of the Federal laws that specifically pertain to the storage and safeguarding of electronic records include: Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act of 1996 (HIPAA), FDA Part 11, DOD 5015.2 and other compliance regulations. Many of the legislated mandates pertain to the requirement that data be stored in a form that is not erasable and not alterable. Furthermore, the storage of computer records must be such that any attempt to do either is recorded and immediately

reported. Finally, computer records covered by these mandates must be readily available for audit anytime a regulatory agency so wishes. Failure to meet these mandates, for the organizations under their jurisdiction, can lead to significant fines and quite possibly the IT director's job.

The Role of the Equipment Vendor

These new requirements are impossible to meet with some of the older storage equipment. Newer technologies have been devised to provide capability to meet some of the mandated regulations. IT managers need to choose equipment vendors who understand the implications of these new laws and which solutions comply. And it isn't just new hardware that's involved. New forms of media, specialized software products and better records management controls will also be required.

Implications

Most SOX regulations focus on the way records are managed, recorded and stored. They also specify long periods of time up to 30 years for certain types of records. Many storage technologies only last for ten years. That means that at least three data conversions must take place between the time the data is originally recorded on disk or tape and the final point ten years later when it can be finally destroyed. Therefore, users and their computer suppliers must plan for significant data conversion processes to the next storage technology for all data that falls under SOX and other data-focused mandates.

Measures that are available to prevent the data from being altered in any way include WORM (write once read many) tape and disk storage, records management software, storage vaults with sophisticated technology to restrict access to only authorized individuals, and hardware designed to protect that data from erasure or alteration,

Some new challenges

The requirements to protect more data for longer time periods is extended beyond normal database files to other types of data including email, instant messaging, faxing and other non-standard documents and forms. These must be captured and retained for periods typically longer than the expected life of the medium they are initially stored on. Furthermore, secure duplicate backup data sets must be maintained offsite in secure locations that can control access to the stored media. And under SOX these records have to be indexed, and this index has to be easily searchable in order to fulfill unanticipated requests for data by oversight agencies.

Sound like a lot to learn about? You bet it is. But it's the new reality IT Managers, equipment vendors and lessors need to master the compliance world to be a successful part of it.

Thanks to David Breisacher, CEO/Chairman at [GST, Inc.](http://www.gstinc.com) for assistance with this article. For more information about the company please visit <http://www.gstinc.com>