

# Compliance Week

## Data Breaches And SOX: Where Your Worries Are

By Christine Dunn — March 6, 2007

[http://www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article\\_ID=3144](http://www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article_ID=3144)

In January, retailer TJX Cos. joined the long list of businesses tarred and embarrassed by losing sensitive customer information. One mildly consoling thought for compliance executives: loss of customer data doesn't really harm the integrity of financial statements, so a breach doesn't necessarily plunge you into Sarbanes-Oxley difficulties. Or does it?

Actually, experts say, breaches of customer data can cause companies to trip over the finer points of SOX compliance in at least three ways:

1. A data breach is considered by many auditors a failure of internal controls that must be reported;
2. Section 302 requires reporting any act of fraud; a data breach would require that it be included in a company's annual and quarterly reports;
3. If a potential fraud would be large enough to have a material effect on the financial statements, that would need to be reported as well.

And if all that weren't enough, a new law being proposed in Massachusetts—TJX's home state—may make compliance burdens in that state even heavier for companies that experience information-security violations.

Massachusetts lawmakers are considering a bill that would make retailers responsible for the financial consequences of a data breach. Currently, banks are responsible for credit-card losses, including due to fraud or data theft; the Massachusetts bill would pin liability on any company participating in the commercial transaction, if its IT system is hacked. The proposed legislation would be the first of its kind, and would impose fines separate from whatever other fines might be imposed by federal or other state regulators.

**“The SOX implications of this bill are that if the financial impact of the loss has a material effect on the financial condition of the company, it must be reported,” says Marie Patterson, vice president of market strategy for AXS-One, a records compliance-management business. “So far, other states have imposed penalties on the company where the breach has occurred, but the penalties have not dealt with the issues related to reissuing the card. Banks have long been held responsible for the details of [the] risk of breach.”**



Bookwalter

**At least 35 states, including California, have laws regarding the responsibilities of companies to protect sensitive personal information. Some fine companies that are deemed to have stalled too long before informing a customer, says Thomas Bookwalter, an advisor to AXS-One, and founder of the consulting firm FMDC. “There are specific monetary penalties per customer, per incident,” that can create liabilities large enough to be material to a company, Bookwalter says.**

### Assessing IT Risks & SOX

As organizations have begun to assess their enterprise risks, they have started to realize how a breach of their IT systems can create an event that may cause a Sarbanes-Oxley compliance

issue, says Wain Kellum, president and chief executive of Trusted Network Technologies. In addition to the exposure or loss of sensitive and confidential information, companies are exposed to potential financial fraud and wide-scale business disruption, he says.



“The current methods that most organizations use for control of those critical assets are transparently inadequate,” Kellum says. “One could argue that the current number and severity of breaches makes a conclusive argument that existing controls are insufficient.”

**Kellum To begin establishing controls to curtail the threat of data-privacy breaches, companies should determine who has access to the information internally and externally, and set up oversight procedures. Second, the data needs to be encrypted, preferably at 128-bit or higher, Bookwalter says.**

The reality may be quite different, says Scott Laliberte, a director at consulting firm Protiviti. Many employees send information, such as spreadsheets, across the Internet in unencrypted form. “People don’t know and don’t realize they shouldn’t be sending unencrypted email. User awareness is a big” issue, he says.

## BREACH NOTIFICATION

The excerpt below is from an "eDiscovery Update" published by the law firm Vedder, Price Kaufman & Kammholz; February 2007:

...When determining whether to notify individuals of a security breach, consider whether the information is in the physical possession and control of an unauthorized person (such as in the case of a lost or stolen computer or other device containing notice-triggering information). Also consider whether the information has been downloaded or copied and whether the information was used by an unauthorized person to establish fraudulent accounts or for identity theft. When notification would allow individuals to take action to protect themselves from possible harm, consider providing notice even if the compromised information is not notice-triggering information. However, keep in mind that continual notification of non-notice-triggering information can make many individuals complacent, which minimizes the effectiveness of the notice.

Notify the affected individuals in the most

expedient and timely way possible after discovery of an incident involving unauthorized access to notice-triggering information. Take steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

When notifying individuals, include a general description of what happened, the type of personal information that was compromised, what has been done to protect the individuals' personal information from further unauthorized acquisition, what your organization will do to assist individuals and information to help individuals protect themselves from identity theft (including contact information for the three reporting agencies).

Make sure that the notice is clear, concise and conspicuous. Use clear, simple language, guiding subheadings, and plenty of white space in the layout. Avoid using jargon or technical language. In addition, avoid using a standard format, which may result in complacency toward the notice.

Send the notice by first-class mail. Alternatively, consider sending notice by e-mail if you normally communicate with the affected individuals by e-mail and have received their prior consent to that form of notification. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in groups likely to have been affected. When a large number of individuals have been affected (e.g., 500,000), or you do not have

adequate contact information on those affected, provide notice using public channels. Post the notice conspicuously on your website, notify through major statewide media (television, radio and print), and send notice by e-mail to any affected party whose e-mail address you have.

If you believe that the incident may involve illegal activities, report it to the appropriate law enforcement agencies. When contacting law enforcement agencies, inform them that you intend to notify affected individuals within 10 business days. If a law enforcement agency tells you that giving notice within 10 days would impede the criminal investigation, ask them to inform you as soon as you can notify the affected individuals. It should not be necessary for a law enforcement agency to complete an investigation before notification can be given. Upon notification from the law enforcement agency, send notice to affected individuals immediately.

These recommendations can serve as guidelines for organizations to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. However, these recommendations do not include all the practices that should be observed. Organizations should periodically review and update their own situation to ensure compliance with the laws and principles of privacy protection. It should be recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

---

**Source**

**All sensitive customer information and other important business records should be archived and consolidated in a controlled environment, where encryption and identity management can be most effective, Bookwalter adds. “The fundamental principle here ... applying in all kinds of jurisdictions and in litigation, is that you have got to have robust control of your data,” he says. “You have to know what it is, where it is, and which information should be completely destroyed.”**

 [eDiscovery Update: Data Security Breach Notification](#) (Vedder Price; February 2007)

Kellum suggests that companies also determine which assets are critical, and then approach control of access to those servers in a more detailed way. This means overseeing every inbound and outbound connection by defining, managing, and auditing a very specific access policy.

Companies can implement stronger authentication methods for all users by using tokens, biometrics, and certificates and can use technologies that allow for the identification of machines, Kellum says. Real-time audits of information also can provide insight into who accessed the servers, and who attempted but was denied, he says.

“Network administrators appear to be losing the battle with hackers, malware and crimeware,” Kellum contends. “The attacks are becoming more sophisticated and are increasingly able to evade traditional methods used to secure computer networks. Organizations are having to change their approach to control of critical information assets on their computer networks. As the threat changes, the response must change.”

### **Getting Out Of A Mess**

If a breach occurs, companies should be prepared with a “reputation management” program as part of their business-continuity plan, in addition to developing the internal controls for operational processes and procedures outlined under COSO and Sarbanes-Oxley.

“Sometimes the damage to a company’s reputation is the most damaging risk one can face,” says Paul Sobel, head of internal audit for Mirant Corp. “It’s probably good for companies who have this type of [customer] data to go through a test and run through a scenario” for if a breach occurs.

Security violations that involve customer data typically are disclosed to the public fairly quickly because clients need to know that their private information may have been given to unauthorized individuals, Sobel says.

A company’s corporate communications group should remain informed throughout the assessing the severity of a breach—from identifying the systems involved and the number of customers affected, to notifying law enforcement authorities and legal counsel—so that they understand who needs to be told of the problem, how information about the issue is being obtained, and how inquiries will be handled, Sobel says.

A delay in making a public announcement not only potentially damages a company’s reputation, but can result in financial costs as well. Expenses related to handling the breach, lawsuits, and fines will affect the financial statements of a business, says Heriot Prentice, director of technology practices for the Institute of Internal Auditors.

TJX, which operates the T.J. Maxx, Marshalls, and HomeGoods retail chains, waited about a month before publicly disclosing that part of its computer network that handles financial transactions for customers, including credit and debit cards, had been compromised. A class-action lawsuit has been filed by a woman from West Virginia who claimed TJX was negligent for keeping quiet about the breach.

The company's chairman, Ben Cammarata, has taken out full-page advertisements in newspapers and posted a video message on the TJX Web site as part of an effort to address the issue.

"I want to say how deeply I regret any difficulties our customers may experience due to this incident," Cammarata said in a statement dated Jan. 29 on the company's Web site. "Our business is about relationships—with our customers, our associates, our shareholders, and the thousands of communities we serve around the world."

A call to company spokeswoman Sherry Lang seeking comment wasn't immediately returned.