

# Protecting Legal Data

*Does Your Legal Technology Provider Compromise Corporate Security? By Eric Smith*

In today's environment of well-deserved hypersensitivity to corporate compliance as mandated by the SEC and the Sarbanes-Oxley Act of 2002 (SOX), the thought of unauthorized parties viewing or altering privileged corporate records should strike fear in the heart of any corporate compliance officer. That threat can quickly evolve into a reality if your corporation's law department implements an electronic invoicing and matter management system in an application service provider (ASP) environment.

In the past three years, ASP-based legal electronic invoicing providers have collectively processed an estimated \$6-\$10 billion worth of privileged legal invoices on behalf of the law departments of Fortune 500 corporations. These third-party providers, popular for their easy-to-install systems, automate the invoice delivery process from law firms through a corporate law department's approval and payment cycle. In doing so, these vendors also accumulate a database of legal information and store it in a warehouse outside of all established security procedures and protocols.

These same providers also host matter management systems for many of their clients. The matter management systems catalog and document sensitive legal case information, such as early case assessments, key strategy documents and case-by-case budget reserve amounts. This data is also stored outside of a corporation's infrastructure.

The ease of deployment and the ability to quickly process invoices, track case progress and evaluate legal spend are significant benefits and very attractive to law department staff. However, it is critical for a compliance

officer to weigh this against the very real risks of keeping the data on a server outside of the client's network and infrastructure and largely independent of a corporation's internal SOX compliance efforts.

The primary questions surrounding an ASP-based legal e-invoicing and matter management system concern the security of a corporation's legal data. Before implementing this technology, you should ask your vendor the following questions: Will my corporation's privileged invoices and matter data be encrypted while stored on the vendor's system, not simply while in transit? Will my invoice and matter data be viewable by unauthorized corporate representatives or any other third party? Does the third-party vendor controlling the pathway of incoming invoices alter the SOX-mandated chain of control for corporate records? Does the third-party vendor duplicate the corporation's compliance control process?

If the ASP-based legal technology system does not use the same security and audit controls the corporation executes for its other internal and confidential data, there may be compromises to a corporation's SOX compliance.

## BACKGROUND

The core of the issue lies with SOX Section 404. Section 404 requires that each public company's annual reports include a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedure for financial reporting. Additionally, management is bound to confirm the effectiveness of the company's internal control structure and procedures for financial reporting.

The legal penalties for violating Section 404 can be steep; however the business implications can be even steeper. Earlier this year, an audit of the Calgon Carbon Corporation law department uncovered \$1.4 million in unreported legal invoice expenses. Consequently, the company's stock dropped by double digits, it was forced to restate earnings for the first three quarters of 2005 and the general counsel was fired.

## AUDIT THE PROVIDER

Corporate compliance officers should audit their ASP-based legal electronic invoicing and matter management system providers. The following five steps are recommended to determine if a vendor's practices support SOX compliance efforts:

- **Audit Security.** Determine what security policies a vendor follows. If a security breach occurs, is the vendor capable of identifying it? Has a security breach occurred in the past? Verify if the vendor is contractually obligated to share information about the breach with its clients.
- **Audit Encryption.** The vendor should encrypt all sensitive data during each transaction step — from delivery to storage.
- **Audit Storage.** A company's electronic billing and case information should be stored in a secure, dedicated environment installed behind that company's firewall. If that sensitive data is stored off site, it may be co-mingled with other companies' invoices.
- **Audit Access.** Vendor employees should *not* have the authority to view, alter or distribute your confidential legal and invoicing data.
- **Audit Termination Procedures.** An employee — either of the vendor or the corporation — should have access to confidential matter management and invoicing data cut off immediately upon termination of employment. Any lag in revoking privileges can lead to unauthorized access and SOX violations.

Security of legal and financial data is a critical matter that is often overlooked when selecting a technology provider for a law department. In addition to legitimate compliance concerns, there is also an array of potentially serious business implications. As a compliance officer, who may or may not be a member of the law department, this is an important issue that should be explored before any compliance concerns arise.

---

**Eric Smith**, DataCert's chief technology officer and a member of the founding DataCert team, has more than 15 years' experience managing software development. Prior to DataCert, he developed industry-specific software applications for the legal and credit management industries and developed accounting and quality assurance applications for both PWC and Compaq Computer Corporation.

**THE CORPORATE LAW DEPARTMENT AND ITS ROLE**

Sarbanes-Oxley audit compliance affects nearly every aspect of corporate operations from the top down, including the corporate legal department, its operations and the manner in which new legal technology is purchased and deployed.

If an audit of the law department is initiated, corporate auditors will want to review key aspects of a legal invoice's life cycle, including:

- Who has access to the system that manages invoices?
- Who has actually accessed those invoices?
- What actions have been taken on each invoice?

These same questions can apply for the law department's matter management system in the event of an audit. Access and the ability to alter privileged legal information — either financial or case-related — is a key concern for the auditing process.

**POSSIBLE BREACHES**

Most ASP-based legal e-invoicing and matter management vendors have implemented minimal technical requirements for securing their corporate client's legal invoices and privileged case information. However, these providers routinely face new challenges related to security, especially in the areas of access, security and data storage.

**Access**

It is critical for a corporation to know who has access to its privileged legal information (*i.e.*, legal invoices, case assessments and budgeting). In many cases, personnel from ASP-based legal vendors have access to a corporation's privileged data. In fact, many ASP vendors permit their own staff to have access to their clients' financial data and case materials. This is a huge risk for any corporation as client data is often co-mingled on the same server with other corporations' privileged information and therefore at serious risk of exposure.

Once logged into the legal e-invoicing system, ASP, law firm and corporate client personnel can view invoices and export and download sensitive legal information and confidential financial data to personal computers from anywhere outside of the company's network and security infrastructure. The same access is also granted for ASP-based matter management systems.

However, there is a potential for access-related breaches that presents three serious control issues.

First, a company must identify which personnel (company only or company and vendor) have access to the ASP-based system. It must also determine if that access is logged, and if a historical record can be obtained to show that data was acted on, altered and/or approved during the submission process.

Second, the company must verify what

controls and restrictions are in place to ensure that only authorized company personnel (and no vendor personnel) have the ability to export sensitive data out of the ASP system.

Finally, the company must determine where the data is being exported. An ASP system can be readily accessed from anywhere using the Internet. Is a corporation comfortable with their personnel — or potentially a vendor's personnel — logging into the ASP system from home and downloading confidential corporate financial and legal data onto a home computer? How does a compliance officer ensure the integrity of the information when law firm personnel are not removed from the system when they leave a firm or are reassigned?

These issues lead to a fair question for corporate counsel and risk management personnel: *Does an environment and opportunity exist for an individual to adversely alter a corporation's legal data without any entrenched independent oversight?*

Unfortunately, the answer with many ASP-based e-invoicing and matter management solution providers is likely to be yes.

**Security Protocol**

As a user of an ASP-based application, you must ensure that the vendors are particularly careful when it comes to the security of your data. They should be diligent in implementing and maintaining top security standards to protect your data.

Many e-invoicing and matter management vendors assign login information based on a user's corporate e-mail address. This is a standard practice industry wide. However, if the vendor does not require a complex, alphanumeric password for login access, or permits passwords to be the same as the user's last name, it is easy for an unauthorized user to break into the system.

Likewise, ASP-based vendors must also be wary of unauthorized entry attempts such as "phishing." Phishing involves mirroring a Web site to illegally obtain an authorized user's login and password information.

Finally, a good practice is to revisit the vendor's contract with your law department. Is there a provision in the contract that requires the vendor to notify the corporation of a known or possible breach? The vendor must be responsible for promptly notifying the law department of all suspected and actual breaches.

**Data Storage**

The basic structure of an ASP-based legal technology solution includes the storing of privileged legal data outside of a corporation's secure infrastructure. Corporate compliance officers should consider not only *where* their data is stored, but also *how* their data is stored.

Typically, ASP-based legal electronic invoicing and matter management vendors do not encrypt corporate client data while it is being stored. If an unauthorized viewer

accesses a company's legal database, he or she will have little difficulty reading (and possibly modifying) the privileged legal invoicing and data.

There may be little, if any, encryption or security around the transmission of the payment file back to the corporate client. In many cases, payment files that contain detailed information and result in checks being issued to law firms are routinely e-mailed by ASP-based vendors back to the corporation without any encryption or security.

Problems also arise from *where* a company's invoicing data is stored on a server. If the ASP-based provider has more than one company's legal data stored on a server, there is a chance that the data can be co-mingled with another company's information and accessible by not only hackers, but also by other company personnel. Having your company's data on the same server as a competitor's adds another level of risk to be considered from both a compliance and business perspective.

**PROTECT LEGAL E-INVOICING DATA**

There are three basic steps that can be taken to help enforce corporate compliance.

1. Require the third-party vendor to deploy the e-invoicing and/or matter management system behind your corporation's firewall;
2. Demand superior security. Discover if your vendor requires user-unique alphanumeric passwords for system access; and
3. Insist that all stored and transmitted data is encrypted. This includes the data itself, backup tapes and media. All forms must be encrypted to guard against inside threats of unauthorized access or theft.



This article is reprinted with permission from the December 2006 edition of the LAW JOURNAL NEWSLETTERS - THE CORPORATE COUNSELOR. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit [www.almreprints.com](http://www.almreprints.com). #055/081-04-06-0001

