



## Is Outsourcing a Security Risk?

[It Starts with an Agreement](#)

[The Hands-On Approach](#)

[The Outsourcer's View](#)

[Addressing Vendors](#)

[Addressing Issues](#)

[Benefits and Risk](#)

Everyone has heard the stories of employees losing laptops filled with private records on the subway or of cyber criminals breaking into a company's computers and stealing customer data. With more and more information being stored electronically, keeping private records secure is a challenge all organizations face.

Companies that outsource accounts payable functions face a unique challenge. Outsourcers handle a great deal of sensitive client information, including supplier addresses, taxpayer identification numbers, and bank account numbers. Many organizations are uncomfortable with their supplier's data being managed by individuals outside their own organization, often in another country.

Although all outsourcers have internal policies and procedures for securing their clients' information, organizations sometimes develop additional security steps for the outsourcer to follow. The level of involvement the client has with data security varies among organizations.

### It Starts with an Agreement

It's in an outsourcer's best interest to prove to prospective clients early that their supplier data is safe. This starts with a non-disclosure agreement between the outsourcer and the client. According to Richard Yee, chief financial officer and chief security officer for accounts payable outsourcing firm API Outsourcing, NDAs are typically one of the first steps in developing an outsourcing relationship.

"A lot of organizations enter into these non-disclosure agreements long before we begin meaningful discussions about the outsourcing agreement," Yee says. "They will want it signed before they even provide their Request for Information (RFI) as they develop a full RFP describing what services they are looking for."

Typical non-disclosure agreements include language stating that the outsourcer will not divulge any of the client's confidential information. While these agreements usually do not specifically mention supplier account information, that data falls under the umbrella of the agreement.

Outsourcers do not sign non-disclosure agreements with their clients' suppliers. Large companies can easily have thousands of vendors. Expecting an outsourcer to maintain confidentiality agreements with each vendor is impractical. Instead, the confidentiality agreements signed between the outsourcer and client – in addition to agreements often signed between suppliers and their customers – are sufficient to determine liability if an issue arises.

## The Hands-On Approach

In 2005, multinational pharmaceutical company Pfizer outsourced its invoice processing to a prominent Indian BPO firm. Despite the outsourcer's status in the marketplace, Pfizer took no chances when it came to protecting their proprietary data. Their strategy was to take a hands-on approach with security.

"We have [the outsourcer's employees] go through all the training that a Pfizer employee would in terms of privacy and data confidentiality," says Julie Lord, Pfizer's senior director and global procure-to-pay and travel expense process owner. "And we require this training for any new hires that work on our process."

Training the outsource employees on Pfizer's processes had multiple steps. While invoice processing was still being handled domestically, the company flew several key BPO people to America for a train-the-trainer initiative. The outsourcers worked directly with Pfizer employees to learn the full invoice process – including supplier data management – before returning to India to train the rest of the staff.

Some Pfizer employees returned to India with them to oversee the on-site training. The goal was to make sure they had absorbed Pfizer's processes and were teaching the other processors correctly.

As a result, the team handling Pfizer's invoices in India is as qualified as the team in the U.S. For instance, the outsourcers now have access to Pfizer's vendor master file to make additions and deletions. The vendor master file is a sensitive file containing sensitive supplier information. When making changes, the outsourcer follows the same segregation of duties that internal Pfizer employees do, meaning individuals that approve invoices are not allowed to make changes to the file.

In addition to holding the outsourcer to the same standards as internal employees, Pfizer also requires the outsourcer to follow some key security procedures. These include performing annual SAS 70 accounting audits, storing all data on Pfizer-owned computer servers, keeping all of Pfizer's

AP processing separate from the outsourcer's other workload, restricting what information processors can see (they cannot see social security numbers, for instance), and storing all data behind Pfizer's own firewall.

"We did not want to be in an environment where all of our accounts payable were mixed and matched with other companies'," Lord says. "It might not be a big deal if those companies are a car company or a library, but it could be a problem if [the outsourcer] mixed our data with one of our competitors'"

Finally, Pfizer regularly visits the Indian office to inspect processes and data security. Lord realizes that this level of involvement may be more intense than what many organizations put into their outsourcing agreements, but believes it is important that the company be comfortable with their outsourcer's abilities.

"I don't know if everyone is as picky as we are, but it probably depends on the size and sophistication of your organization," Lord says. "It's expensive to set up and all of the infrastructure costs are things you underestimate. But, there are a lot of savings to be had in outsourcing and you have to be able to balance any additional risks."

## The Outsourcer's View

Pfizer's actions are atypical. For instance, most small- and mid-size companies do not have the financial resources to install their own servers in the outsourcer's facility. He says that some companies keep their data on their own servers, but most opt to have the outsourcer receive all invoices and store records for them on the outsourcer's servers.

"In addition to reducing costs, one of the main reasons companies outsource is so they can have access to technology they don't have," Yee says.

Smaller organizations that are considering outsourcing some or all of their invoice processing should not be discouraged if they cannot afford to have a significant presence at the outsourcer's facility. The security procedures in place at most accounts payable outsourcers are enough to meet the client's needs.

For instance, API has a three-tiered approach to protecting their client's data. The first piece is procedural safeguards. All of API's security processes are formalized and follow an ISO 27002 (formerly known as ISO 17799) standard, an international data security standard covering 12 sections including risk assessment, access control, physical protection of computer equipment, and incident management.

"The provider should have specific security policies and procedures implemented," Yee says.

"Information security is a corporate governance issue and we engage our board of directors and

audit committees so that they are aware of the different aspects of the security we are providing for our customers' data."

The second tier involves physical safeguards of the outsource facilities. Outsource facilities typically feature secured access, meaning security badges are required to gain entry. Facilities are also subject to video monitoring. Inside the facilities there are areas off limits to anyone but company employees.

The third tier comprises electronic safeguards such as firewalls that prevent outside access to the computer system.

Outsourcers also should regularly review their security processes. API undergoes an annual SAS70 Type II audit, which involves testing controls for weaknesses. (Type I audits, on the other hand, review an organization's controls but do not test them.) In addition, larger clients will come in and review the data security processes with their own staff.

However, Yee says that clients don't typically provide direct oversight of the processes. They are interested in how their data is stored and who has access to it. "Clients are very active in the first part of an outsourcing agreement to ensure that the processes are transitioned correctly and controls are in place, but as the relationship continues their involvement in many cases will lessen and their focus will shift to their core business and how they can improve their ability to service their customers," he says. "We also collaborate with our clients to identify changes for continuous process improvement."

## Addressing Vendors

When suppliers learn that one of their customers is outsourcing payables, they usually understand that it's a business decision and in no way impacts their buyer-seller relationship. However, in rare cases vendors are unhappy that their private data is being accessed by a third party.

Addressing vendors' skepticism involves helping them understand that outsourcing is in both organizations' best interests. For instance, because outsourcers have access to streamlined payables processes and sophisticated technologies, vendors often receive accurate, reliable payments more quickly than if AP were handled by the client in house.

"Outsourcing can make things better for the suppliers," Yee says. "We have web portals to give suppliers access to information, there are fewer missed payments and more discounts are captured. There are few skeptics among suppliers because they care about getting timely payments."

It's also important to let suppliers know that any data that the outsourcer has access to is completely secure. For Pfizer, this meant explaining that all data was on company-owned servers

and that the processors were fully trained in Pfizer's security practices. The aim is to demonstrate that their invoices, account numbers, and other information are not in danger.

"Some vendors think you are literally shipping their documents overseas when it's actually electronic," Lord says. "An electronic exchange of information can be protected in so many more ways than if you were sending paper back and forth, which is something we don't do."

While it's important to make sure suppliers know that their data is secure, Lord says that few vendors complain about outsourcing. She says suppliers are often more concerned about getting adequate telephone support from the outsourcer than they are worrying about data integrity. Provided the individuals fielding vendor calls understand your processes and can give strong customer support, then you will likely meet minimal resistance from suppliers.

## Addressing Issues

Regardless of what security is put in place to protect supplier data, no AP process is flawless. Although data breaches are rare, a crucial part of the outsourcing agreement is how potential problems are addressed.

The laws in India, where many BPO firms are located, place severe penalties on organizations that lose or misuse a client's data. According to the Indian Penal Code of 1846 and the Information Technology Act of 2000, employees that misappropriate company data for personal use face up to seven years in prison. In addition, arrests under these statutes do not require warrants and offenders are not subject to bail.

A security breach is more likely to be an accident than a malicious attack against you or your vendors. Many potential issues you might face – including individuals accidentally taking electronic data outside the office or information somehow being stored outside the protected firewall – are risks you take with internal employees and are not unique to an outsource relationship.

Including language in the agreement between the client and the outsourcer outlining the penalties for security breaches is an effective way to avoid potential problems. "We have clauses in our agreement concerning the right to discontinue the relationship if necessary," Lord says. Some agreements also mandate financial penalties in the event that protected records are lost or stolen.

## Benefits and Risk

According to TAPN benchmark data, 65 percent of organizations outsource no accounts payable functions. For the minority that are outsourcing, the benefits include improved economies of scale, access to robust payables technology, and the ability for internal employees to focus on analytical tasks instead of invoice processing.

With these benefits also comes a certain degree of risk concerning supplier account information. Whether an organization takes a direct role in training the outsource employees or relies on agreements with the outsourcer, there are steps they can and should take to guarantee integrity.

"There's not much you can do without giving the outsourcer some degree of access to private information," Lord says. "This is why the contract agreement between you and your outsourcer is absolutely critical."

---

---

### ***Copyright Notice***

This material is protected by copyright law. Copyright © 2002-2009. Financial Operations Networks LLC. No part of the materials including articles, files, graphics, and logos, available in this Web site may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent. Distribution for commercial purposes is prohibited.

---

This article comes from The Accounts Payable Network  
<http://www.theaccountspayablenetwork.com>