Dangerous liaisons

Recent incidents in the US have highlighted the problems in outsourcing data processing to third party vendors. **Kirk J Nahra** looks at how companies can minimise the risks.

One key impetus for privacy laws and regulations is the "interconnectedness" of most commercial activity in the United States. Internet retailers use a wide range of suppliers to monitor customer activity and deliver products and services. Banks use marketing firms, "data crunchers" and others to serve their customers. Health insurers use claims managers, pharmacy benefits managers, and mental health vendors to deliver integrated products to their customers.

Accordingly, privacy rules - for example, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GBLA), and the Children's Online Privacy Protection Act (COPPA) - have regulated and restricted how these relationships develop, and have imposed regulatory or contractual requirements upon participants in these relationships.

The most comprehensive of these requirements to date has involved the "business associate" requirements of the HIPAA rules. Covered entities under HIPAA have struggled to complete the monumental task of executing new agreements with all vendors that have access to, or use, customer information, numbering in the tens of thousands for large covered entities. The dilemmas presented by these requirements have occupied significant attention over the past few months (including the "battle of the forms" between covered entities and vendors that both deal with volume contracting), and the operational significance of this avalanche of last minute contracting still remains to be seen.

But it is clear that these operational entanglements present substantial legal liabilities for covered entities and others that routinely use vendors to perform certain kinds of services. What are the risks in this area? Are they practical, or merely theoretical? And, as our commercial society becomes more integrated, how can companies realistically and effectively protect themselves from liability resulting from the activities of third parties?

Higher prominence of third-party risks

A series of recent examples have driven home the reality of risks created by third party vendors.

Internet vendors

For example, in In *Re Pharmatrak Inc.* Privacy Litigation, the First Circuit evaluated the potential liability of Pharmatrak, whose business involved tracking website users, primarily for pharmaceutical companies. According to the Court, the pharmaceutical companies "were emphatic that they did not want personal or identifying data about their website users to be collected." They "sought and received assurances from Pharmatrak that such data collection would not occur." Nonetheless, Pharmatrak did collect certain individually identifiable information about the users in the course of their activities. While the pharmaceutical companies were dismissed from this case by the trial court, and their dismissal was not appealed, this case presents real concerns for companies retaining vendors where, as here, the vendor ignored specific contract requirements, placing the principal - in this case, the pharmaceutical manufacturer - at risk.

> ...companies must not focus only on their own compliance activities. It is also important to consider how best to prepare for risk management involving vendors.

Financial institutions

These concerns also are present in the financial services industries. Several government agencies responsible for regulating various financial institutions recently issued guidance for their regulated entities, raising the risks of "linking" with other websites. These agencies - the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Controller of the Currency and the Office of Thrift Supervision - issued their warning because "while weblinks are a convenient and accepted tool in website design, [t]heir use can present certain risks," mainly what the agencies called "reputation risk" and "compliance risk." According to these agencies, "[a]ny link to a third party website creates some risk exposure for an institution."

"Reputation risk" is straightforward - and can arise in several ways identified by the agencies:

- Customer confusion in distinguishing whether the financial institution or the linked third party is offering products and services.

- Customer dissatisfaction with the quality of products or services obtained from a third party.

- Customer confusion as to whether certain regulatory protections apply to third party products or services.

The "compliance risk" identified by the agencies is perhaps of more concern. For example, "compliance risk could arise from the inappropriate release or use of shared customer information by the linked third party. Compliance risk

also arises when the link to a third party creates or affects compliance obligations of the financial institution." This guidance (which can be found at www.occ.treas.gov/ftp/bulletin/2003%2D15a.pdf) also identifies some means of mitigating these risks, focusing on due diligence, contract protections, disclaimers and disclosures, and responding to customer complaints.

HEALTHCARE

The widely publicised TriWest incident is another variation on this theme. TriWest, a contractor for the Department of Defense (DoD) healthcare programme, was the victim of a break-in, resulting in theft of various computer-related equipment. The equipment contained sensitive personal information on more than half a million healthcare members of the TRICARE plan sponsored by the DoD. While the "principal" on this problem has not been the subject of media criticism (perhaps because it is the Department of Defense, rather than another commercial entity), this relationship with TriWest is one replicated in healthcare entities across the country.

TriWest's response to this problem is perhaps a model for the industry. Promptly upon discovering the theft, TriWest issued a release to all its beneficiaries announcing "that one of TriWest Healthcare Alliance's offices in Phoenix was broken into and computer equipment and data files containing personal information about our TRICARE beneficiaries were stolen. Since the motives for the crime are unknown at this time, it is important that you are aware that there is the possibility that the information may be misused, exposing beneficiaries to the potential of identity theft."

Triwest posted ongoing updates on its website about the situation and worked closely with the DoD to mitigate any harm from the situation.

The DoD also acted aggressively. The top military health official, Dr William Winkenwerder Jr, Assistant Secretary of Defense for Health Affairs, according to one report, characterised the theft of computer hard drives from a TRICARE health services contractor in Phoenix, AZ, as a "very serious" matter that "got our full attention". In a subsequent press release, Dr Winkenwerder announced specific steps that had been taken to reduce any harm, focusing on the identity theft possibilities:

• All 562,000 military beneficiaries whose information was contained on the computer files have been notified by mail of the theft as of December 31st 2002, and informed of the actions they should take to protect themselves from identity theft or other misuse of their personal information.

• Fewer than 25 persons also may have had personal credit card information compromised. Each of these individuals has been contacted by phone and informed of the incident and proper actions to take in response.

• Every TRICARE contractor worldwide has been notified of the theft, and directed by the DoD to conduct an assessment of information security procedures. The DoD will evaluate each assessment with its contractors.

• The criminal investigation remains active, led by the Defense Criminal Investigative Service and supported by the US Attorney in Phoenix, the Federal Bureau of Investigation and other law enforcement agencies. TriWest has posted a $100,000 reward for information leading to the arrest and successful prosecution of the perpetrators and return of the stolen items.

The break-in also led to significant re-evaluations of overall security for military contractors. In particular, DoD ordered additional steps to enhance the security of healthcare information, including:

• A worldwide healthcare information security assessment will be conducted at every military treatment facility and contractor location to review existing procedures and to ensure physical security of sensitive information.

• A health information security task force comprised of DoD and Service medical leaders and information system experts will assemble promptly, consult with TRICARE contractor representatives, and recommend any additional requirements for information security.

• New health information systems to be introduced in the coming months will be compliant with, or exceed, the HIPAA legal requirements for protection of patient information.

The legal ramifications of this situation are still developing. Despite TriWest's aggressive response, a class action suit, brought on behalf of more than 562,000 members, has been filed against TriWest (a follow-on step that may raise new concerns for any company bearing responsibility for any privacy or security breaches).

WHAT SHOULD COMPANIES BE DOING NOW?

As these recent examples illustrate, companies must not focus only on their own compliance activities. It is also important to consider how best to prepare for risk management involving vendors.

UNDERSTAND THE LEGAL RULES

The first step is to understand the applicable legal rules. Most statutes regulating vendor relationships have focused to-date on contractual requirements. The HIPAA Privacy Rule, for example, requires substantial privacy language, but does not require ongoing monitoring or audits of vendor behaviour. It requires action against a vendor only when the covered entity knows that the vendor has breached the Privacy Rule. A more aggressive monitoring requirement (contained in the draft of the Privacy Rule) was rejected in the final version.

Accordingly, there are limited mandatory monitoring or due diligence requirements. Some companies, responding to the limited nature of regulatory requirements, may take a 'bury your head in the sand' approach to vendor relationships. However, this approach is shortsighted, given the potential liability risks raised by vendor behaviour. Third party plaintiffs may challenge the lack of monitoring and cite the contractual provisions in support of their contention. And with the advent of the new HIPAA Security Rule, healthcare entities should heighten their concerns about vendor security even more, because of additional due diligence requirements stemming from that rule.

TAKE A PRACTICAL APPROACH

Presumably, no company is going to conduct full onsite audits of all vendors, large or small, regardless of the amount of information held by these vendors or the sensitivity of the information. However, the fact that not everything can be done should not lead to the conclusion that nothing can be done. Companies need to group their vendors into categories that factor in the size of the relationship, sensitivity of the data, sophistication of privacy and security practices, etc. Focusing resources on key vendors is important. Companies should also increase the resources dedicated to reviewing third party relationships so that a more effective triage process can be developed. New vendors should undergo a more sophisticated 'due diligence' process, particularly now that the frenzy of GBLA and HIPAA contracting deadlines has passed.

HAVE A CONTINGENCY PLAN

It is also critical that companies have a realistic contingency plan. This plan should involve both the need to replace vendors that have privacy/security problems, and a plan for responding to problems if they do exist. The proactive TriWest model is one approach to consider - a full disclosure model focused on alerting individuals to realistic risks and minimising resulting harm through full disclosure.

CONCLUSION

All in all, as privacy laws expand and inter-corporate liaisons increase, companies must be careful to consider more than their own practices—to make sure that relationships designed to improve a company's customer performance do not cause more trouble in the end.

AUTHOR: Kirk J Nahra is a Partner with the Washington, DC law firm of Wiley Rein & Fielding LLP. He represents a wide range of insurers, health plans and others on issues related to the privacy and security of information. He is also the editor of *Privacy Officers Adviser*. He can be reached at: Tel: +1 202 719 7335, E-mail: knahra@wrf.com.

FURTHER INFORMATION: This article originally appeared in the June edition of *Privacy Officers Advisor*, the official monthly newsletter of the International Association of Privacy Professionals (IAPP). For more details, see: www.privacyassociation.org