

PRIVACY BREACH EXPOSURES ON THE UPTICK; KNOW WHAT THE RISKS ARE

Panel Recap From PLUS 2008 Professional Risk Symposium on May 7, 2008

The scope of privacy breaches is on the upswing. With no uniform approach to protecting sensitive personal information, millions of people are at risk. If you're underwriting, identify the information, classify data and understand how information is classified, panelists told the Professional Risk Symposium, sponsored by PLUS.

According to **Jay Foley**, executive director, Identity Theft Resource Center, among the common sources of breaches include lost or stolen laptops, records lost by third-party partners, misplaced or stolen backup files and malware programs. "There was \$94 million in privacy breach activities for TJX between 2000-2007; Visa/Amex/Mastercard \$40 million and America online \$30 million," he said. "The first quarter of 2008 there were 167 breaches affecting more than eight million people."

Foley noted that insider theft had 28 breaches. "It can be as a result of a bad employee, but it can also be the guy who fills your vending machines, the plumber, the guy who cleans your buildings, or even the fire marshal."

Looking at the organizational risks, **Thomas Srail**, vice president, Willis, New York, Inc., said that a wide range of data and information includes customer data, employee data, vendor data and confidential information. "Confidential corporate information breaches are

happening. A hospital will want to pay close attention to health data."

Randall J. Krause, Esq., CEO, YourHRDepartment Inc., noted that there isn't a uniform approach to protecting sensitive personal information (SPI). "Under federal law we have this silo-like approach which covers only certain types of data or certain types of entities. HIPPA, for example, only provides comprehensive data privacy and security standards; it applies only to certain types of health information."

Krause said that ADA medical records must be kept confidential and separate from personnel files. "FCRA requires reasonable measures to protect. There are some proposals on the horizon that may provide a more federal approach. When we get to the state laws, we're all over the lot; the state laws are crazy."

According to Krause, states have tried to regulate in five basic areas: protection of personal information, protection of social security measures, protection of medical information, destruction of records, ensuring personal information is undecipherable and notification of security breaches. "42 states require breach notification. As a general rule, a law of that state applies to the citizen of that state. If there's a security breach, you must comply with the law of that state for that resident."

Looking at recent state developments, Krause said that Virginia requires businesses to notify individuals (and the AG) regarding breach of computerized personal information only if the breach causes or is reasonably believed to cause identity theft or other fraud to Virginia residents. "South Carolina has a more comprehensive rule. Enacted April 2, it covers data breach notification provisions, required methods for data disposal and limits on use/disclosure of SSNs."

Krause said that California law is a state model. "It is the most comprehensive. It also provides protection for SS from use by any manager or employer and also the company has the duty to notify the employee of any breach in the system. As far as I can see in any state whether they have a private right of action or not, they can sue if the state has a more comprehensive approach to data protection."

Krause noted that Europe is 20 years ahead of the US in terms of international regulations. "They set their first regulations in 1980. They're much stricter including state laws. US employers sometimes have to collect race and ethnicity data. But if these employees are based in Europe they can't do that. If employee gives specific consent you can do it. In France you can't do it."

Krause discussed the largest breach to date which was TJX. "They stored personal information on their systems. Tens-of-millions of records. A 'cyber thief' hacked into their software in July 2005 and harvested the information," he said noting that from July 2005 to January 2007, 94 million records were breached. "The FTC brought an action against TJX. The settlement included cash benefits, ID theft insurance, reimbursements for out-of-pocket costs. In addition, TJX had to identify risks to security, implement safeguards and retain a third-party auditor to do vulnerability testing of their system for the next 20 years."

Foley noted that other companies are going through similar situations. "They will differ from state to state, but I don't envy anyone going through this process; it's going to be ugly."

Foley said the first obligation a company has is to secure their data. "Encrypt your data and keep it encrypted. Take reasonable steps to protect the data both electronically as well as physically," he said. "It does no good to secure electronically if someone wheels out the file cabinets."

Foley said that if there is a breach the company needs to send out a simple, clear-cut letter. He noted that the standard response from a breach letter is usually only three percent, which isn't very good. "What do you have to do to mitigate the risk? You need a privacy policy in place and observed by everyone in that company."

"There needs to be employee training. Junior level employees are the biggest problem areas. Train the employees, give the employees the knowledge they need to answer the questions properly," he

said. "There need to be controls and procedures for data gathering, storage, access and disposal."

"When looking to hire, look at an application without social security numbers," Foley explained. "Decide who you like the best then ask for the social security number. Many companies expose themselves to tremendous risk by doing this. Storage is critical."

Foley also questioned using a shredding company. "How about if it ends up in Dallas, Texas, on a raid? You're the medical provider who created the file. Think about all these things and by the way, even if they claim they are NAID (National Association for Information Destruction), doesn't mean they are all NAID certified."

In terms of hiring practices, Foley advised to go "with a more prestigious group; insist on a good report."

Strail said that there are a lot of risk management strategies to use. "Conduct proper risk assessment. If you're underwriting, identify the information, classify data, and understand how they classify that information. Think about whether you should buy a liability policy, and if so, what retention? What limits?"

Strail said to forget traditional insurance coverage. "GL, EO, Crime, Property weren't designed to respond to these privacy issues. Privacy network security policies are a good place to start."

"Do a complete analysis of your needs," he said. "Is there exclusion for hacking? If the claim is brought from a client, if it meets the definition of a lawful act, then it's E&O. It may not be excluded. It's different from adding more broad coverage. It can be built in from some providers."

Strail said not to refer to it as cyber insurance but as privacy/network policies. "It is much broader than cyber insurance. We find as we're talking to companies, they think of cyber insurance when first hacker virus coverages came out. The trigger then was a failure of network security, and that was the only trigger on the coverage. Today we've got a host of issues—negligence, vendor negligence and a laptop stolen or lost."

Laura Johnson, vice president, Euclid Managers, moderated the panel.