| THE ROUNDTABLE SPONSORED BY **LITTLER MENDELSON** |

010DATA011
DILEMMAS

Security breaches raise the stakes on employee privacy protection

Employees are demanding more privacy protection in the wake of widely publicized security breaches. At the same time, advances in technology are expanding the potential for personal data to be both used and compromised. And in the absence of comprehensive federal legislation, states are stepping into the gap, passing a patchwork of privacy laws.

As these trends converge, corporations are challenged to develop effective privacy policies and procedures without sacrificing the benefits in efficiency that come with the collection and storage of employee information.

The issue is taking on a sense of urgency as the number of security incidents multiplies. According to a report from the Privacy Rights Clearinghouse, more than 150 publicly reported data breaches occurred between February 2005 and March 2006, putting at risk the personal information of more than 54 million Americans. Some of the nation's largest companies—including MCI, Boeing, Time Warner and Honeywell—found themselves coping with the fallout of compromised employee information.

At Littler Mendelson's 2006 Executive Employer conference in Phoenix, experts offered ideas on this timely topic in a roundtable discussion titled, "Privacy Policies Alone Will Not Work: The CPO's Perspective on How to Secure Employee Data and Protect Employee Privacy." Sharing experiences and best practices on data protection and privacy crisis management, they offered practical solutions to a vexing problem and discussed the impact of data breaches on both employee morale and the bottom line.

"The cost can be astonishing," says Philip Gordon, chair of Littler Mendelson's Privacy Task Force and roundtable moderator. Costs can include notification, providing credit monitoring services and lost employee time. Gordon cited a 2006 Javelin/Better Business Bureau survey that found ID theft victims spend an average of 40 hours resolving the issue.

"You can be sure if a laptop from the HR department is lost with the database of payroll information and Social Security numbers, your employees will need to spend time protecting themselves," Gordon says. "And they are going to spend that time between 9 and 5, Monday through Friday. It will be on your nickel that they clean up these potential identity thefts."

Moderated by Philip Gordon, Shareholder, Littler Mendelson

Photographs by Geoff Reed

PROTECTING PRIVACY

Philip Gordon, Moderator: We've seen a huge change in U.S. privacy law over the past three years. In 2003 HIPAA was the only data protection regulation in the U.S. that had a true impact on employers, and that impact was fairly narrow because the HIPAA security rule applies only to health information. But in the past three years, the states have become increasingly active in the area of data protection.

Twenty states now have statutes that impose restrictions on the use and transmission of Social Security numbers. Six states have set general standards for information security. We also see states starting to implement statutes requiring appropriate disposal of records. In June 2005 the Federal Trade Commission passed regulations that require proper destruction of consumer reports, because more and more employers are ordering background checks, credit history checks and criminal conviction checks on job applicants and employees.

The statutes that probably have attracted the most attention in the press and in the public are notices of security breach statutes. Last year, California was the only state that had a notice of security breach statute. Now, 33 states do.

With this patchwork of requirements, we are seeing increasing pressure for a uniform federal standard. There are probably 10 to 20 bills in Congress dealing with various aspects of data protection. It's very likely we will see some form of data protection law in the next year or two.

So, with that background, I'd like to ask: What do you recommend to safeguard employee information? How has your organization implemented those steps?

Brian O'Connor: We have employees in 100 countries around the globe, and security is even more important in the European Union than in the U.S. We try to get control over that data and ensure adequate security by integrating our human resources data into a single database. We haven't accomplished that yet throughout the company, but we have in our U.S. operations. You simplify security problems if you have just one system to worry about and to control. If you have multiple databases, you multiply the risks that you will have a security problem.

And you need to have some regular review process to analyze who has access and what level of access rights they have to the data. You need review that every six to 12 months and have some automated system to end access rights for people who have left the company.

Amy Yates: Considering privacy issues is like peeling the layers on an onion. You have technical safeguards and adminis-

ROUNDTABLE PROFILES

PHILIP GORDON is a shareholder in Littler Mendelson's Denver office and chair of the firm's Privacy Task Force. He litigates a wide variety of privacy-based claims and lectures and publishes articles on privacy issues. He holds degrees from Princeton University and New York University School of Law.

BRIAN O'CONNOR became chief privacy officer of Eastman Kodak Co. in January 2005 and now holds the title of chief security and privacy officer. A graduate of Tufts University and New York University School of Law, he previously practiced employment law at the Rochester, N.Y., firm of Harris, Beach & Wilcox.

AMY YATES is chief privacy officer and an attorney in the office of the general counsel for Hewitt Associates, a human resources consultancy in Lincolnshire, Ill. A graduate of Georgetown University and Northwestern University Law School, she was acting privacy officer of Andersen prior to joining Hewitt in 2002.

RICK DAKIN is president of Coalfire Systems, a Superior, Colo.-based provider of information technology risk-management services. A graduate of West Point, he began his career at United Technologies Corp. and was president of Centera Information Systems, an e-commerce and systems integration firm, prior to cofounding Coalfire in 2001.

For information about participating in or hosting an **InsideCounsel** Roundtable contact AUSTIN HOLIAN at 312.651.0342 or e-mail: austin@insidecounsel.com

| THE ROUNDTABLE SPONSORED BY **LITTLER MENDELSON** |

trative safeguards. You set up a policy, but then you need to train employees on it, so everybody knows that protecting data is important. What sort of data do you need to use and how do you need to use it? How do you disclose it? How do you protect it? So training is one thing that we consider to be an administrative safeguard.

Rick Dakin: You have to start with administrative controls and a strategy to protect the data, because the technical teams cannot protect everything. You aren't going to be able to achieve 100 percent security. As you are putting together your plans, it's important to have reporting capabilities for those technical controls to determine whether your administrative controls are working. That's very, very hard to do, because technical people use a jargon that sometimes doesn't match your administrative people's language. You have to train the two groups on how to talk to one another. Then you can determine what level of risk you have actually mitigated.

DANGERS WITHIN

O'Connor: The two primary risks to your data are your employees who have authorized access and your vendors who have authorized access. The greatest risks are not from outside thieves.

It's often easy to overlook vendors in your security review. Whenever Kodak evaluates a vendor, in addition to just negotiating a contract, we also negotiate security measures. You need to evaluate their security processes to see whether they meet certain standards—ISO standards, the EU Directive on Data Protection or whatever standards you choose. Make sure that you have contractual language in place that holds vendors accountable if they fail to meet those security standards.

> "The two primary risks to your data are your employees ... and your vendors .... The greatest risks are not from outside thieves."
>
> —Brian O'Connor, CPO, Eastman Kodak Co.

Yates: The issues change every year. The issue two or three years ago involved including Social Security numbers on things we sent to individuals. It's important to always revisit your training and find out what employees and clients are sensitive about. Every time you think you've got it nailed down, you look up and see another issue you need to address.

One additional technical safeguard that Hewitt has put in place involves using a secure pipeline for e-mail transmissions. A lot of times companies send personal information back and forth. So we have implemented with our clients and our trusted vendors various types of technologies to ensure that these transmissions are sent securely.

Dakin: Brian O'Connor led off with the best advice. Get all the cattle into one pen. Get all the data into one database. You have a better chance then of deploying the controls, whether they are access controls or encryption. But, as an organization if you decide your data is so valuable it must be encrypted, that's a risk-based decision you can make.

From the ground up, encrypting data at best is very difficult to do—imagine putting armor on your kids as your send them off to school. It takes more resources, more attention. You've got to make sure that you lock it up right. The way it's done is there is an extra process inserted in your application that takes a bit of data, encapsulates it and then surrounds it with a key that only the custodian can unlock. Some databases just cannot be feasibly encrypted very quickly. So very early, get with your IT department and say, if we get all of our data in a central location, can you reasonably encrypt it? The chance of it being encrypted in place is probably only 50/50.

PLANNING AHEAD

Gordon: What have you learned from your own experiences are the most important steps that organizations can take to prepare for a data breach? What are your recommendations on the steps to take when a data breach does occur?

O'Connor: The best thing is to form a crisis management team for information security incidents. It's good to give that some thought before a crisis occurs, so you can quickly react. As you probably know, laws require that you give notice as quickly as is reasonably possible, whatever that might mean. To do that, you've got to get a lot of people together and gather a lot of information.

On your team, you need a technical expert to give some advice on what was or might have been on the hard drive and what might be recoverable. You also want the chief privacy officer or a chief information security officer. You want your physical security people if you have to investigate whether, in fact, something has been stolen and sold. You want public relations people involved, because if the incident is sizeable at all, it's likely to end up in the papers. You need to have a larger team that includes your vendor, if in fact your vendor is involved in the data incident. We've had a couple situations where vendors have been involved in handling our data and—usually through no fault of their own—the data is stolen or lost. We had one recent situation where the data was lost by the post office.

Another key aspect is having a call center response available. Just as you have a certain number of employees who get extra excited about problems at work, when data is lost, a certain percentage of that affected population goes ballistic. They want to talk personally to the CEO and find out whether the FBI has gotten involved. You've got to have a way to manage that, and that's your call center.

Yates: We have somebody within Hewitt who likes to call himself an old doughnut cop. I get him in right away and he matrixes these problems and I can't tell you how many times, had he not been involved, things might have actually turned into a big issue that were instead very containable. So before you get to the crisis standpoint, make sure you get the information to the right people within your organization. Oftentimes it can be resolved internally.

O'Connor: If you have an incident involving a vendor, one of the first questions the legal department gets is, what does the contract with the vendor say? Who is going to pay for this problem? Who's going to pay for the mailing of 200,000 letters to people whose data was lost? Who's going to pay for credit counseling for all of those people? We've spent a lot of time changing the boilerplate language in our vendor agreements. That becomes a very hotly negotiated issue with vendors, because any savvy vendor is going to push back and there will be a big struggle to place the liability hot potato in the other person's lap.

"From the ground up, encrypting data at best is very difficult to do—imagine putting armor on your kids as you send them off to school."

—Rick Dakin, President, Coalfire Systems

Dakin: Usually, by the time we get involved, we work with law enforcement and define the event so the company can start mitigating the damage. So many times companies focus on what caused these incidents. But there are a number of agencies that are willing to issue multi-million dollar fines these days for failure to protect information. The immediacy with which you stop the bleeding goes a long way toward mitigating the damage.

Make sure the IT guys are trained to keep a timeline on what they are doing. In some of the most recent incidents we've been helping support, management didn't even know there was an ongoing situation until it hit the newspapers. Then you really look foolish when Channel 9 news puts a microphone in front of you.

Gordon: There is a real challenge about whether or not notice needs to be sent when an incident occurs and, if the notice does need to be sent, to whom does it need to be sent? That's very controversial. And the standards in the states vary. If you have information from employees or customers from 30 states, you are going to have to look at the statutes for each of those states whose residents' information you possess.

I've had to draft a significant number of notices to either customers or employees whose information has been compromised, and it's a real challenge. On one hand, you don't want to create Exhibit A in the next piece of litigation against your client. On the other hand, you do need to tell people what happened and what they need to do to protect themselves. Because the more damage that is done to the victims of a security breach, the higher the risk that you will end up in litigation. If people promptly cancel credit cards and start monitoring their credit, the risk of ID theft drops substantially.

NEW TECHNOLOGIES

Gordon: Let's turn to the next topic, which is new technology in the workplace. Employees bring camera phones and iPods to work. Maybe your businesses have implemented global positioning systems to track service people who are out all day driving around. But all these technologies have potential privacy and security implications. As the new technologies become a part of the workplace with increasing regularity, what advice can you give about successful implementation?

Dakin: I had to debate whether the area of high technology that concerns me the most as an IT security professional is WiFi or cellular broadband communication. But I decided mobile storage devices concern me the most. These little sticks with 5 to 6 gigabytes of mobile storage are deadly. Take a look at establishing policies and training and enforcement, because you really need to take a look what type of hardware you are going to allow to connect to your company's information system. Non-encrypted mobile computing devices should never, ever, ever be allowed on your network. Or say somebody gets a new computer for Christmas. They bring it in and plug it into your corporate network and they have you. They own you, you don't own them.

Yates: I have a love/hate relationship with instant messaging, because it's like having a 4-year-old child pulling on you all the time. It's blinking, blinking, blinking. But it does get your answer really quickly. We only permit it on the internal, corporate network. You also may want to look at records for instant messaging, which may not go through the backup protocol that e-mail does.

It's always a cost/benefit analysis. We at Hewitt love to work our consultants to death, so we would like to have them working 24/7 if possible. But you've got to figure out smart ways to do it, so they can't hook up their own computers into the network. That can lead to viruses within your system.

O'Connor: BlackBerrys are becoming a concern now because they are so easy to lose. People lose laptops regularly and now we're starting to see people lose BlackBerrys fairly regularly because they are small, they're light, they can fall out of the holster or you can leave them on a desk at lunch, or whatever. We limit how many people have BlackBerrys to just a couple hundred people in the company. That's a financial decision, but it's also a security decision. You have to have a really strong need to have one. And we install software in the BlackBerrys that mandates a secure password and that must be changed every 90 days. If one gets lost, at least that provides a little bit of security, although a password is minimal security at best.

> "I have a love/hate relationship with instant messaging, because it's like having a 4-year-old child pulling on you all the time."
>
> —Amy Yates, CPO, Hewitt Associates

MONITORING EMPLOYEES

Gordon: What are your organizations' practices for monitoring employees' use of corporate electronic resources? How does your organization respond to misuse of these resources and what recommendations do you have for other organizations?

Yates: In the European Union there are data privacy rights for your own employees. So if you have a global organization and you are contemplating doing e-mail content filtering or you are looking at what Web sites your employees are visiting, you may be violating your own employees' privacy rights and that is a problem. So, it is one of these areas where a lot of global companies are kind of looking for some guidance and it hasn't been forthcoming from Europe yet.

O'Connor: It's just impossible to have a global policy on use of the Internet or e-mail. You really need to have a U.S. policy and then a separate one for Europe and maybe for other regions of the world as well. It will vary based on the laws in those countries. In the U.S., we focus more on the excessive personal usage of the Internet and e-mail as opposed to the content. But you also have to take into account sexual harassment and other types of harassment policies and laws, which will make you liable if people are visiting porn sites and then displaying the results on their screens or forwarding files around to all their friends in the workplace.

Dakin: In one case we were doing a financial fraud digital discovery, and we imaged the disc, brought all the files back and some of the deleted files had pictures on them. As soon as we opened up one of the pictures and it became obvious that it was child porn, we had to stop. That immediately becomes a criminal investigation, and the FBI has to be called in. It actually slowed down the primary investigation, because when the child porn was identified, a whole new investigation started. ■