SANDIEGOSOURCE The Daily Transcript®

Tuesday, March 22, 2011 **editor@sddt.com** **http://www.sddt.com** Source Code: 20110322crb

Encryption is key to protecting private data

By DOUG SHERWIN, The Daily Transcript
Tuesday, March 22, 2011

When it comes to protecting confidential information, encryption is a company's best defense -- both practically and legally.

Using passwords to protect private data not only helps keep unauthorized personnel from gaining access, but it also lessens a company's liability under the law.

"Encryption, encryption, encryption," said Jeremy Roth, managing shareholder of **Littler Mendelson**'s San Diego office. "That is the key. Make sure you have protocols for requiring passwords to be changed frequently. Password changing really does work. Workstation security really does work."

Roth said companies should remind employees to turn off their computers when they leave for the day or for a long duration, so the computer is not accessible to those who walk by. He also said small steps like employing an alphanumeric password and not sharing passwords also are helpful.

Companies now are choosing to be more selective about what information they gather from employees, according to Bill Whelan, a partner in the labor and employment practice group of **Sheppard Mullin Richter & Hampton**. The idea is you can't lose what you don't have.

"Before it was too easy to ask for anything under the sun," Whelan said. "Now some folks are rethinking and saying, 'We don't use that info, so we'd rather not have it.'"

California has an identity theft provision in its civil code. The law requires businesses to disclose any breach of unencrypted personalized data to those potentially affected. That information can include Social Security numbers, California identification cards, driver's licenses or any medical information.

The disclosure can be a written notice. If there are more than 500,000 people affected, the company can give notice through e-mail or by issuing a statewide media report.

There is no civil penalty, but the law allows the state attorney general to sue and, if necessary, issue a fine.

There's a potential for federal government enforcement in the case of a large breach or if the governing agency feels the breach is more than just an isolated incident. The Federal Trade Commission could issue some sort of penalty or require improvements in information security.

"The FTC has gotten more aggressive (lately)," said San Diego attorney Andrew Serwin, founding chair of **Foley & Lardner**'s privacy, security and information management practice. "They're bringing more cases and doing more investigations that aren't made public."

The FTC recently announced a settlement with Twitter. The social networking site allegedly had a lack of information security, allowing people to take over certain Twitter feeds.

"The fines are one thing, but the real costs are for compliance that you have to do related to the settlements," Serwin said. "It's not just writing a check. It's having to comply, in some cases, for 20 years with a consent decree."

Other potential remedies include private rights of action by individuals whose data was compromised, but most times those are not successful, Serwin said, because victims of security breaches don't have any compensable damage under the law.

"There's reputational harm for companies having a breach if it's in an industry where there's brand awareness," he said.

When it comes to notifying clients or employees of a data breach, company officials have to be careful not to create an unnecessary panic among those potentially affected.

“It’s best to err on the side of over-notification so no one can fault them later, recognizing that in many cases it really is much ado about nothing,” Sheppard Mullin’s Whelan said.

“All these various statutory schemes are just making people rethink how much information do we want to load into our company (databanks) because it takes up space,” he added.

Roth, of Littler Mendelson, said it’s not a bad idea for employers to be proactive and offer to pay for a credit monitoring subscription for employees, which would alert them if someone tries to use their credit information.

He also said it’s also important to clean hard drives of extraneous private information, much like using a paper shredder to dispose of documents containing personal information that’s no longer needed.

“It’s important to have written policy,” Roth added, “saying this is how we treat private and secure data, and make people aware of it.”

Serwin said organizational training is key, as well, to prevent future breaches and show the FTC that an effort is being made to protect private data.