

## One firm's story: Your data isn't as secure as you think

### State's upcoming data security mandates call for hefty fines

BY JACKIE NOBLETT  
JOURNAL STAFF

The firm thought it was ahead of the privacy curve, setting up a secure e-mail portal, encrypting company laptops and even requiring employees to change their network password every 90 days.

But as executives found out last week, all of those technical efforts do little to secure personal information when employees can choose to bypass those protections.

The revelations were contained in a data leakage audit of a Boston-area accounting firm. The Business Journal was given access to the presentation of those findings on the condition the firm's name be withheld.

"Our policies are actually tougher than state laws," said a high-level executive of the firm before the meeting. "We want to see what is getting out so we can set our internal policies. We want to protect our customers' information."

So when the executive and network manager sat down with Segal's team to see the results of the audit for the first time, they were surprised to see what was on the slides.

In the 38 days Networks Unlimited Inc. monitored for data leaks, the company recorded more than 3,200 leakage events that violated some sort of government or industry regulation, although some leakages could have been recorded twice.

The actions that triggered personal data leakages ranged from the innocent to the potentially dangerous.

For example:

- Staff e-mailing tax details to a client's

personal e-mail address with personal information that could be embarrassing if leaked included in the body of the e-mail.

- Staff e-mailing two spreadsheets with a total of 2,000 clients and personally identifiable information to his or her personal e-mail account to work at home, saving that information on a computer that could be stolen or broken into.

- Allowing vendors to request background check information be sent to generic e-mail addresses that could be fake.

The executive said she was less surprised of the number of breaches than how they occurred. For example, the company has technology that enables employees to securely access their work computers from home rather than have to download files directly to their notebook computers.

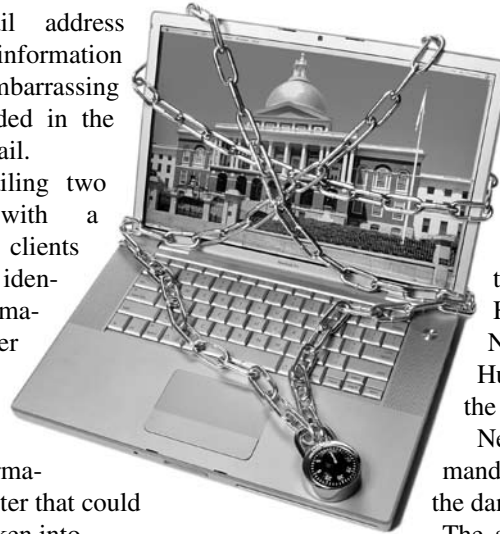
"We invested a lot of money in that and people just decided to go and take what they think is an easier way. That's disappointing," the executive said.

One thing became clear to the accounting firm during the presentation.

"I personally think this is proof you can't rely on the users," the IT manager said.

So the company expects to use the results to educate the staff on the impact their choices have on the firm's data security as well as implement tools that block sensitive data from accidentally leaving the network.

Network security experts say the results are common among companies, large and small, that simply do not recognize the



myriad ways information can seep out by human error.

"They know from reading the newspaper that it's happening, but rarely they realize the extent of data leakage in their organizations," said Harry Segal, president of Networks Unlimited, the Hudson firm that performed the audit.

New state data security mandates make understanding the dangers of data loss critical.

The state Office of Consumer Affairs and Business Regulation crafted regulations that require companies to identify where personal information is stored and protect it with access controls and encryption software by May 1.

Businesses that fail to meet the regulations can be fined up to \$5,000 per offense and could be held liable in civil litigation if a breach results because of inaction.

Data security audits have grown in popularity of late, as businesses become aware of the impacts of breaches.

A variety of firms perform audits and risk assessments as a stand-alone service or a part of a larger consulting or technology contract. Boston is a major hub for audit and tax firm Deloitte and Touche LLP's computer forensics unit, and PricewaterhouseCoopers LLP also provides such services. Several other area vendors such as Fidelis Security Systems Inc. of Waltham and Tizor Systems Inc. of Maynard sell software that allows businesses to monitor data leakage.

Jackie Noblett can be reached at [jnoblett@bizjournals.com](mailto:jnoblett@bizjournals.com).