

HIPAA makes encrypting some laptops mandatory

Dan Stone arrived early at Logan Airport. When he reached the waiting area at Gate 25, he still had 45 minutes until his flight would begin boarding. He relaxed, checked his voice mail, and called a few clients he hadn't reached the day before.

When the boarding announcement came, Dan clipped his cell phone to his belt, grabbed his jacket from the seat next to him, and discovered his laptop bag was no longer where he had placed it on the floor near his seat. Apparently while on the phone, he hadn't paid close attention to his carry-on bag, but

someone else had. In a few short moments, Dan had become one of the many victims of laptop theft.

Most people in Dan's shoes would have immediately called their office to report the theft and missed their departing flight. But as Northeast client services manager for a Boston-based insurance company that prefers to remain anonymous, Dan knew his laptop might appear on eBay, but its data-

base of confidential client data would never be exposed.

Dan's company decided in early 2006 to place laptops in the hands of their client services managers who spent most of their time on the road personally interviewing clients. Since the laptops would contain a portion of the company's client database, **Andy Ross**, the company's information systems manager, insisted that every laptop be fully encrypted before being allowed to leave the IT area.

Andy considered laptop encryption a necessity to properly protect confidential client medical and financial data that would reside on managers' laptops. He chose laptop encryption software designed for a

corporate environment, with enterprise-style management and features. Not only would it prevent a laptop thief from reaching a Windows startup screen, but even if the thief removed the laptop's encrypted disk drive and attached it to another computer, they would still have no access to confidential client data. It also ensured the laptop could not be used for remote access to the company's network.

As companies deploy laptops and other mobile devices for enhanced service to clients, patients and business partners, the likelihood of highly sensitive data being stored on these ubiquitous computers becomes a near certainty. According to the **Privacy Rights Clearinghouse**, a nonprofit consumer information and advocacy organization, more than 1.2 million people had protected health-care information compromised through theft of unencrypted computer equipment in the past six months.

While the Privacy Rule under the Health Insurance Portability and Accountability

The general public has woken up to the **growing problem of corporate data loss leading to identity theft**

Act may not mandate notification when leakage of confidential medical information occurs, since those same databases frequently contain confidential financial data on patients, health-care providers and insurers likely face the same privacy laws as other businesses. As the general public has woken up to the growing problem of corporate data loss leading to identity theft, legislators have responded with new state regulations requiring companies to notify individuals when their private information has possibly been breached. Most state disclosure laws do not require proof that the confidential data that was exposed has actually been accessed or used

by third parties. The fact that the unencrypted data exists on the lost computer or media, and that the computer is no longer under the control of the data-owner, is enough to require the notification of all people potentially affected.

These new regulations are designed to encourage organizations to properly secure confidential personal data, whether it resides on servers, desktops, laptops or USB drives. By requiring notification of patients, consumers, or employees whose confidential data may have been exposed, the organizations that suffer these data losses are penalized via the expense of notifications, credit-watch services, damage to their brand name, and loss of confidence, in addition to possible financial or criminal penalties.

In all cases where portable devices containing confidential medical or financial information has been lost or stolen, the data would have been protected and the data-owner would have avoided notification requirements had the laptop or media been properly encrypted. Today, data-owners can completely encrypt laptops, smartphones, and portable storage media, rendering the data unreadable if lost or stolen.

Founded in 1985, Networks Unlimited, Inc. serves the information security needs of mid-market organizations across a variety of industries, including financial, healthcare, manufacturing, and legal. Networks Unlimited performs security audits and deploys information security systems that protect computer networks and help customers avoid business disruptions, loss of confidential information, and the other detrimental effects of security breaches.

Networks Unlimited, a privately-held company headquartered in Hudson, Massachusetts, with a satellite office in Austin, Texas, is recognized as one of the nation's foremost information technology consulting firms specializing in information security. The company has been featured editorially in influential *Computeworld*, *IT Week*, *Financial Executive* and *Network World* articles. Further information is available at their web site: www.networksunlimited.com.

Harry J. Segal, President & Founder, Networks Unlimited
Prior to founding Networks Unlimited, Harry Segal was vice president of Microcom, a manufacturer of modems that was best known for its invention of the error-correcting protocol still used in today's dial-up modems. His career in the computer industry began over 30 years ago, after receiving a bachelor's degree in information and computer science from Georgia Tech. He can be contacted at harry.segal@networksunlimited.com.

GUEST COLUMN



Harry J. Segal