

Mobile Data Security Strategies: Real World Case Studies

Leading Regional Bank Protects Sensitive Data

Heritage Bank of Commerce has installed the same technology used in Iron Mountain's DataDefense solution -- Lost Data Destruction software from Iron Mountain partner Beachhead Solutions Inc. -- across all its laptops in order to offer the highest level of protection possible for sensitive customer data. San Jose-based Heritage Bank of Commerce, with more than \$1 billion in assets, is a wholly owned subsidiary of Heritage Commerce Corp.

"We want to proactively protect our clients from the possibility of their data falling into the wrong hands," said Richard L. Conniff, President and Chief Operating Officer of Heritage Commerce Corp. "The ease of implementation and the transparency to our end users made the Lost Data Destruction technology an ideal choice."

The software automatically eliminates specified data on a lost or stolen laptop to prevent its compromise or misuse. Unlike most other data security products, this solution does not depend on user compliance or involvement and is particularly suitable for banks, insurance companies, medical institutions and other government and business entities that are custodians of confidential data.

Recent legislative acts such as California SB 1386, HIPAA, Graham-Leach-Bliley, Sarbanes-Oxley, FISMA and FACTA include measures that compel organizations to publicly notify customers when data has been lost or exposed to the public

With increasingly stringent data compliance requirements and more than a million laptops stolen each year, companies have too much to lose to simply rely on users and policies to keep critical data safe and secure. Iron Mountain's DataDefense solution can complete the security chain broken by lax user behavior, and protects enterprises from legal liability, reputation damage and financial losses.

CPA Firm Protects Sensitive Data Despite Laptop Theft

When an auditor with Mohler, Nixon & Williams stored his laptop computer out of sight in the locked trunk of his car, he was confidently following company policies for the physical security of this important asset and the client data it contained. Unfortunately a thief broke into the vehicle and stole the hidden laptop from the trunk. The good news for Mohler Nixon & Williams and its clients is that the thief only ended up with a data-free computer and the auditor's guitar.

Mohler, Nixon & Williams employees have many tools to help assure that client data is safe and secure. Laptop users have cable locks to physically secure laptops while at a client site; client data is transmitted securely over the internet using data encryption

algorithms; and data on the local laptop is locked in a 256-bit encrypted data vault when not in use.

Months prior to this incident, Mohler Nixon & Williams executives had the foresight to anticipate that computer theft can occur despite many reasonable precautions and took the additional proactive step of installing the same technology used in Iron Mountain's DataDefense solution -- Lost Data Destruction software from Iron Mountain partner Beachhead Solutions Inc. -- on all of the firm's laptops. Due to this extra level of protection, the software wiped all files from the laptop's hard drive when the crook turned on the computer.

The solution reported back to Mohler, Nixon & Williams with a receipt that revealed the laptop's data was destroyed and supplied the crook's unique IP address showing where the computer was when the data destruction occurred.

"As one of the 100 largest public accounting firms in America, we handle a great deal of sensitive information on behalf of our clients," said Clare Piech, Chief Operations Officer for Mohler Nixon & Williams. "With the encryption and elimination software in place on all our firm's laptops, we know that the intellectual property of our firm and our clients is safe from misuse by computer thieves. We wanted a solution that would keep our client's data secure and confidential even in situations where the theft may not always be preventable. Now Mohler, Nixon & Williams' clients can be sure that even in the worst case scenario, their sensitive information will be protected."