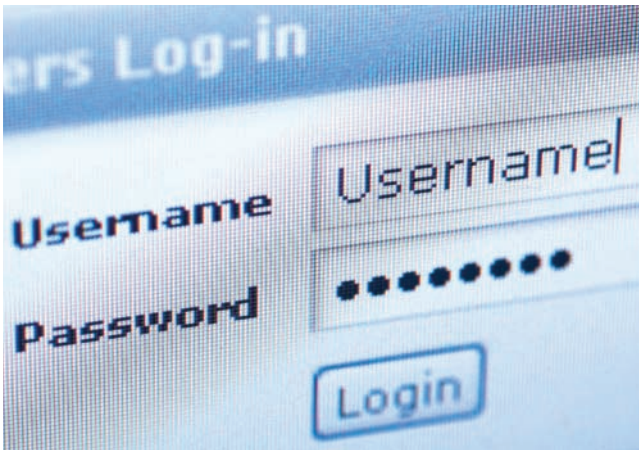
by Lark Allen and Kelly Purcell

Encrypting Sensitive Data

As data losses have become more public, mortgage lenders have to respond with **greater security strategies**.

TOUGH DATA PROTECTION AND PRIVACY LAWS are making full disk encryption of all data on laptops and other devices mandatory. The cost of the average data breach in 2008 rose to more than $6.6 million per incident, according to Ponemon Institute LLC's 2008 Annual Study: Cost of a Data Breach. In addition, the violating business is frequently flogged in the press. The storage industry has responded with a new generation of industry standard Self-Encrypting Drives. These new "trusted" drives are designed to be "set it and forget it" while providing better security, higher performance and lower cost than the traditional software for doing full disk encryption. To better assure legal compliance, Self-Encrypting Drives provide the industry's best solution for data protection and should be a standard feature in all new laptops.

Managing financial information such as income statements, financial accounts, investments, loans, payment histories, credit cards, tax returns, Social Security numbers, credit scores, credit applications, etc.: the list of personal information which is in the possession of the lender/investor or related business partners is very long and highly sensitive. Is your company prepared for the inevitable data breach?



As data losses became more public, state and federal governments around the world passed a broad range of privacy and data protection legislation typically with heavy penalties for any business, which lost data and did not take adequate precautions to protect the data. Nearly every regulation and law specifies that if the data can be proven to have been encrypted when it was lost then "safe harbor" provisions allow the guilty entity to escape public notification, including notification of all affected individuals. The SED and management software provides the proof of encryption.

If you have ever originated, bought or serviced a loan that includes a borrower from the state of Nevada or Massachusetts read on. The next generation of even tougher data security legislation has started to appear in bills passed recently in Nevada and Massachusetts and similar bills are expected to appear in other states and government mandates. While the first generation regulations required disclosure, the new laws require the encryption of the data. Under the Massachusetts regulation all laptops and portable devices containing personal and identity information on any Massachusetts resident must be encrypted.

Encryption software has been available for more than 20 years. The Gartner Group estimated that more than 52 million copies of encryption software for full disk encryption were shipped in 2008. There are significant challenges with doing encryption in application software. It can have a negative effect on the system performance and the overall security of the encryption application, especially the keys, is dependent on the operating system security, which is notoriously vulnerable to network and software attacks. Finally software FDE can be complex to manage. Proving that the data was encrypted for compliance reasons after the laptop has been lost can be difficult for software based solutions which can be turned off and potentially compromised, which is another reason to invest in the more secure SED solution for future.

> The Gartner Group estimates that **more than 52 million copies of encryption software** for full disk encryption were shipped in 2008.

Five years ago an industry standards group was formed called the Trusted Computing Group. (www.trustedcomputinggroup.com). In January 2009, the TCG Storage Work Group published a set of specifications for including encryption and access control security features directly within the hardware of storage devices. Self-Encrypting Drives have already been announced by Seagate, Hitachi, Fujitsu, Samsung and Toshiba and are being offered by multiple PC OEMs as options on their laptops and some desktop machines.

Drive manufacturers have integrated government grade Advanced Encryption Standard hardware within the drive. The encryption is always on and cannot be turned off so that all data written to the drive is automatically and transparently encrypted and everything read from the drive is decrypted. The encryption hardware works at the full data rate of the drive; therefore there is no performance impact. Whenever the laptop is shut down the drive will lock itself, thereby protecting the data whenever the system is not in use or the loan officer has left it in the local Starbucks. When the loan officer wants to restart their laptop the SED presents a pre-boot screen where the user can input their password, biometrics, or smartcard. Multiple users and multiple administrators, each with unique identities and authentication credentials for auditing purposes can be supported on the same drive. The drive authenticates the user and when successful, the drive unlocks and Windows and applications will restart or reboot normally.

The lender can also choose to have Single Sign On from the drive to Windows and to have passwords synchronized between the two to make it easy for users to log into their systems without compromising security. When it is time to either repurpose or decommission a system with SED, the data can be rendered completely useless and unreadable by merely having an administrator perform a Crypto Erase function which deletes the encryption key in the drive. When there is turnover of personnel and the drive is being repurposed then a new key is automatically generated and the drive is immediately ready for usage. This feature of SED will save IT personnel hours of rewrites and formats in order to delete data from old drives and make sure that no drives show up on eBay with the data still on them.

What are the benefits of SED? Self-Encrypting Drives are the industry's best solution for meeting data protection and compliance requirements. SED provides the following benefits over software full disk encryption solutions:

- High Performance: Encryption performed a full speed with no main processor overhead.
- Stronger Security: Encryption keys are generated and used inside the protected hardware of the SED and never leave the data they are protecting so no encryption key management is needed. User authentication is performed by Trusted Access Control within the drive.
- Ease of Use: Encryption is completely transparent to the user and to the operating system. The system itself has been designed to be "set it and forget it".
- Lowest Cost: Overall management complexity is reduced significantly for the IT staff. The drives are integrated with the normal infrastructure and all tools work normally. When it is time to dispose of the drives, they can be instantly and securely erased.

If these benefits aren't enough, having the CEO stay out of jail and off the front page of *The Wall Street Journal* is a bonus. MT

Lark Allen is executive vice president at Wave Systems Corp. Mr. Allen is responsible for the corporate strategy, technology guidance and market development for Wave's client architecture and developing strategic relationships with platform, technology, network, content, security and services companies. He participates in the International Security, Trust and Privacy Alliance, the Trusted Computing Group, the Carnegie Mellon University Security Research Program, and the Liberty Alliance on digital identities and ebusiness.

Kelly Purcell is executive vice president, global sales and marketing at Wave eSignSystems. Ms. Purcell is responsible for the marketing strategy, business development and sales activities of the eSign Transaction Management Suite. Wave's eTMS was designed to allow organizations to manage business processes and digital transactions entirely online by using e-signatures and e-vaulting.