Data Protection for a Mobile World

Data Breaches: A Growing Problem for the Private and Public Sectors

A data breach makes international headlines nearly every week. A metropolitan hospital reports that its patient and staff records are exposed. A university discloses alumni information is missing. Personnel records are lost from another government agency.

The problem is only getting worse — both in terms of the number of records exposed and the number of affected organizations. And the cost? Beyond the impact to an organization's reputation and credibility, such occurrences often result in legal liability with steep financial penalties. Considering the expense of legal counsel, public relations efforts and notifying customers (along with providing credit monitoring services to those impacted), a data breach can easily cost up to $200 per customer record.

Increasingly, a lost or stolen laptop is to blame. Consider this: Within U.S. and European airports alone, an average of 834,000 laptops are reported stolen or lost every year, according to the Ponemon Institute.

The vast majority of these missing laptops are carried by frequent flyers who routinely have access to sensitive and confidential information — corporate executives, attorneys, consultants, sales representatives and the like. And the number of lost or stolen laptops is set for a precipitous jump over the next five years as the amount of U.S. and European workers who use a laptop as their primary computing device increases from an estimated 30 to 60 percent. The ever-growing mobile workforce combined with the escalating number of regulations requiring public disclosure in the event of a suspected data breach have prompted businesses to assess their options for protecting mobile data — often leading them towards encryption.

Software Encryption: A Step in the Right Direction, But Not Good Enough

The first generation of whole disk or full disk encryption (FDE) solutions proved a significant advance. With full disk encryption, data on the drive is only accessible when the operating system is booted and the encryption keys are unlocked. Whole disk encryption has a distinct advantage over alternatives such as file or folder encryption in that everything on the drive — including swap and temporary files — is protected. This takes the decision of what to safeguard out of the hands of the user.

But software-based FDE has its drawbacks. Relying on the PC's memory and processing resources often causes a marked degradation in overall system performance — longer boot times and slower response times frustrate users and hamper their productivity. And running intense applications, such as virus scanning, can take up to twice as long on a machine with software FDE than one without. There are also nagging fears about security vulnerabilities since software encryption keys are accessible. Whether it's the fear of a "cold boot" attack, whereby secrets are dumped from memory at power down, or the more recent threat from the "Evil Maid" (sniffing drive passwords with a removable storage device) organizations have grown increasingly concerned about the level of protection that software-based FDE provides.

By far the biggest issue with software is the burden it puts on IT to deploy and maintain it. Software encryption takes — literally — hours to install and configure. According to a recent study, encrypting a 500 GB hard drive can take anywhere from 3 ½ to 24 hours.

While encryption can run in the background, doing so can seriously hamper system performance, essentially rendering a computer unusable. For large enterprises, with tens of thousands of employees, the time and effort to deploy software FDE can be cost and resource prohibitive.

A Better Bet: Hardware Encryption

Several years ago, leading drive manufacturer Seagate Technology introduced the first mainstream hard drive with encryption "built in." This hardware-based FDE solution — also known as self-encrypting drives (SED) — marked a significant advance, offering a higher level of security and better performance.

Disk drives, by their very nature, offer a more secure environment: they have their own processor, dynamic RAM and pre-boot environment. Unlike general purpose computing devices, these drives impose strict limits on the code that can run on them, making them impervious to conventional software attacks. Plus, encryption keys are stored in the hard-drive controller and never sit in the system's memory, making them unavailable to attackers.

Additionally, unlike software FDE, self-encrypting drives have no impact on performance. Commands are executed by dedicated processors, therefore eliminating any need to consume system resources.

Also, since drive encryption is turned on during manufacturing, the drive simply encrypts anything written to it and decrypts anything read from it. By design, this bypasses the "bulk encryption" step required by software FDE — eliminating hours of installation time. "Always on" encryption is essential in proving a computer is protected in the event it goes missing. Data protection laws mandate this burden of proof in order for organizations to avoid notification penalties.

PC OEMs Make SEDs Universally Available

Adoption of hardware encryption advanced in January 2009, when the Trusted Computing Group released its standards for building self-encrypting drives, called Opal. The broadly endorsed "blueprint" sparked Toshiba, Hitachi and Samsung to join the movement by announcing hardware-based FDE drives of their own. Along with the drive vendors, Lenovo, Panasonic and HP joined Dell in making the drives available on many of their business-class laptops.

Strong Access Control: A "Must Have" for Security

Security best practices (and most compliance regulations) call for both encryption and strong access controls. Therefore, self-encrypting drives are designed with their own, drive level, pre-boot environment — a tamper-proof area that provides secure authentication. Drive-level verification blocks all read/write functions until the user has supplied the correct logon credentials. This is far superior to OS, BIOS and ATA passwords, which are fairly easy to hack and do not meet the "safe harbor" requirements set forth in 45 states' notice of breach laws.

Self-Encrypting Drives and Wave's EMBASSY® Software = Problem Solved

A complete data protection solution requires more than just encryption. Policy-based access controls, centralized administration and proof of compliance are all "must haves." An organization needs to be able to centrally provision security polices across the enterprise, limit access of encrypted information to only authorized individuals, remotely reset user passwords and perhaps, most importantly, prove whether or not a laptop's data was encrypted at the time it went missing. Wave's EMBASSY® software provides these essential capabilities and more.

Wave's Trusted Drive Manager is a client application that activates the on-board security features of encrypting drives, including pre-boot authentication and secure erase for the safe retirement or disposal of laptops and drives. The client software enforces policy-based access controls when the PC is powered on. Support of Windows® single sign-on means fewer passwords for users to remember and fewer help desk calls. Additionally, integration with Windows password update allows the drive access policies to be automatically updated with the OS, ensuring compliance to company password policies.

For large-scale, enterprise-wide deployments, Wave's EMBASSY Remote Administration Server allows IT to manage policies, credentials and access rights from one central location. Through native integration with existing directory structures and policy distribution mechanisms, assigning users and policies can be performed within the directory framework, dramatically simplifying deployment, saving time and money.

03-000232/version 2.02

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication