

A New Standard of Due Care: Full Disk Encryption

In the nearly four years since California passed Senate Bill 1386, the face of information security has become more visible. The glare of public and media attention is now illuminating what was once nearly a black art – or at least the realm of technical wizards. Since the passing of the California law, 34 states have passed similar legislation requiring that people be notified when their personal information has been, or even may have been, compromised.

Even without these state laws, and without a Federal law, companies are beginning to recognize a duty to notify. The public and media have since come to believe that notification is their right. The seminal ChoicePoint incident of 2005 became such a large issue precisely because the company initially only notified their California customers, as required by law. Pressure from the media and public eventually forced the company to notify all affected customers.

In 2006, insurers were responsible for the loss of personal information on over one million people. Companies ranging from the largest US insurer to a small community health plan lost information and had to notify customers. AIG had the largest incident, losing 930,000 pieces of information when a server was stolen from an office in Indiana. Buckeye Community Health notified 72,000 customers when four laptops went missing. CS Stars, a subsidiary of Marsh lost a laptop containing information on over half a million people and had to notify them even though the laptop was recovered. The total number of records compromised in the United States since 2005 reached 100,000,000.

Fortunately for those of us charged with protecting information and for our firms, it is now fairly simple and inexpensive to achieve fully adequate protection. Long gone are the days when encryption was too computationally expensive for everyday use. Both the laws, and it seems, the court of public opinion, provide safe harbor from the disclosure requirements if the information was encrypted at the time of the breach. If the information cannot be accessed in any reasonable manner, there is little risk that the data can be misused.

However, merely encrypting the data is the easy part. Other considerations are always in mind with security technologies. Cryptosystems, the software that does the encryption and manages the keys, have significant technical complexity and can easily be done incorrectly. But these difficulties are largely esoteric for a typical corporate threat environment. While some companies operate in extremely competitive environments where highly sophisticated and expensive technical attacks are probable, the vast majority of organizations seeking safe harbor from disclosure and reasonable protections for their customers are more concerned with the day-to-day requirements of an implementation.

SafeBoot: Vendor-of-Choice for Laptop Encryption

SafeBoot designs, develops, supports, and markets leading-edge mobile data security solutions for mobile devices and network systems. In use at nearly 170 Fortune® 500 companies, SafeBoot® is the vendor-of-choice for mobile data security solutions that protect data, devices and networks against the risks associated with loss, theft, and unauthorized access, anytime and anywhere. SafeBoot solutions offer powerful encryption and strong access control technologies that seamlessly integrate with existing enterprise systems. SafeBoot's centralized management capabilities provide enterprises of all sizes with operational efficiency and ensure the lowest possible total cost of ownership. Founded in 1991, SafeBoot operates in the U.S., The Netherlands, United Kingdom, Sweden, France, Germany, Brazil, Belgium, and Australia — and hosts a worldwide network of more than 50 certified distributors. SafeBoot is privately held and consistently demonstrates growth and profitability.

Like all IT projects, the total cost of ownership is the primary consideration for most organizations when looking at any technology. No matter how important the security goal, it is irresponsible of security professionals not to consider how a package will integrate with existing systems like directories, provisioning systems, software distribution, public key infrastructures, and other enterprise applications. Furthermore, ease of use for front-line technicians and integration with organizational structure are necessary. Too many implementations have failed because the tool was too hard to use or required organizational changes that were either impossible or too expensive. All these factors need to be weighed against the measurable benefits of the technology.

Perhaps even more important than these somewhat mundane, yet critical, considerations is the need to prove that the software really performed as advertised. Just as SB 1386 changed the face of protecting personal information, Sarbanes-Oxley has created a need to demonstrate the protections and capabilities of an IT shop more than ever. By today's mandate, companies need to say what they do in policy, actually do what they say, and prove it was done. Many companies struggle with this last requirement to produce the necessary evidence and sometimes cannot. Where the evidence can be found, the challenge is to produce it consistently and efficiently. Many information security programs are becoming de facto compliance offices, spending more time on audits and paperwork than securing information.

In an area like full disk encryption, where the primary goal is one of obtaining legal safe harbor from disclosure, there is a clear need to prove that the protection was actually in place. Should litigation ever ensue, a plaintiff's attorney would be irresponsible not to ask how the organization confirmed that information was encrypted.

In addition to negative press reports and customer notification, the Federal Trade Commission has also weighed in heavily on this issue, charging companies with not taking reasonable measures to protect information (they usually cite encryption as a reasonable measure) and imposing fines on some companies and consent decrees on others. Given the cost-effectiveness and widespread adoption of full disk encryption, we can be confident that it can now be considered reasonable.

¹<http://www.zdnet.com.au/insight/security/print.htm?TYPE=story&AT=339272771-139023764t-110000105c>

Written March 2007 by Scott S. Blake, CISM, CISSP. He is CISO-in-Residence and VP of Operations for Echelon One, an executive security intelligence firm. Prior to Echelon One, Mr. Blake was Chief Information Security Officer of Liberty Mutual Insurance, VP of Information Security for BindView Corporation, and a variety of other executive and consulting roles in IT and information security.

SafeBoot sponsored the development of this research note.

