



January 14, 2010

(c. online)

How to Use Data Encryption to Secure Mobile Business Data

By: Kurt Lennartsson

A staggering number of enterprise mobile devices are lost or stolen annually, at a high cost to the organizations that own them. But there are solutions available to help secure the data left on the devices. Here, Knowledge Center contributor Kurt Lennartsson explains why it is imperative that organizations secure this data, and explains how to use encryption software to protect data that is in transit on these mobile devices.

Over the past two decades, private, public and governmental organizations have built walls to contain their businesses. More specifically, firewalls. These firewalls were built as safeguards to establish secure perimeters within which enterprise computing, communication devices and data are safe from attack from outsiders. However, the emergence of business mobility and the explosion in the number of mobile devices—laptops, smartphones, PDAs and thumb drives—within the marketplace have rendered firewalls alone somewhat obsolete when it comes to protecting an organization's sensitive data from theft, loss or hackers.

Currently, there are 25 million Blackberry users in the United States alone, with that number expected to expand by 25 percent over the coming year as more people abandon their typical cell phones for smartphones that allow them access to more data. Laptop, PDA and thumb drive sales are also predicted to rise. It's all part of an expanding mobile work force, which allows business to be done outside the typical four walls and the 9 to 5 workday schedule.

It's a numbers game

A recent survey estimates that 800,000 mobile devices are stolen each year and 97 percent are never recovered. A further breakdown of this number is even more eye-opening: business travelers lose more than 12,000 laptops per week in airports in the United States. On a weekly basis, major corporations suffer losses of 640 laptops, 1,985 USB memory sticks, 1,075 smartphones and 1,324 other devices from theft. Protecting an organization's data on those devices becomes more mission-critical and business imperative than ever.

Dollars and sense

Each time a mobile device is lost or stolen, the opportunity for a data breach of sensitive information increases. Since 2005, more than 245 million records containing sensitive personal information have been involved in security data breaches in the United States alone. The average cost of a data breach to organizations in the United States in 2008 rose to \$202 per compromised customer record, up from \$197 the year prior. According to recent estimates, data breaches cost companies in the United States an aggregate \$18 billion annually. The opportunity to conduct business anywhere, anytime, clearly comes at a price.

Rethink your strategy

To combat the rising cost of data breaches, organizations must rethink their strategy in regards to protecting data. No longer is a firewall the means to this end. While firewalls protect traditional computing methods, they do not protect data from theft via mobile devices. A stronger method of protecting data in transit on mobile devices is through the use of encryption software.

Encryption is the process in which an algorithm is used to transform information into a senseless jumble of characters and symbols, and it is the future of data security. Only authorized personnel have a "key" that is used to decrypt the information so that it can be readable again.

The rise in the mobile work force has changed the conversation on security methods from device-centric protection to data-centric security. When discussing data encryption, there are a number of solutions.

The whole truth and nothing but

Whole-disk encryption is designed primarily for desktops, laptops, notebooks and devices with hard drives. Whole-disk encryption is a comprehensive and transparent means to securing data. Through this method, data is encrypted and decrypted on the fly, as users perform their normal tasks. All the data on the hard drive is encrypted. Unlike firewall-only perimeter defenses, data encryption protects data wherever it goes and, therefore, is ideal in the ever-expanding world of business mobility.

No hard drive? No problem

File and folder encryption protects specific files on a device and requires an encryption key to gain access to the data. Because some mobile devices do not have hard drives, the whole disk cannot be encrypted. However, file/folder encryption is designed in such a manner that it allows encryption of the data on the device. This way, if an employee loses a flash drive or a CD/DVD, the data is not accessible if it falls into the wrong hands.

Regulations and mandates galore

Protecting data has become so critical that federal and state regulatory mandates have emerged requiring immediate action to properly protect Personally Identifiable Information (PII). In the United States, 45 out of 50 states have passed data protection and reporting laws. Most industries have regulatory requirements to protect data. The healthcare industry has the Health Insurance Portability and Accountability Act (HIPAA), the financial industry has the Sarbanes-Oxley Act (SarboX), retail and manufacturing has the Payment Card Industry Data Security Standard (PCI DSS), and state and local government and institutions have the Family Educational Rights and Privacy Act (FERPA). And this is just to name a few.

Business case for data protection and ROI

Because data security has become a strategic issue, companies looking to bolster their defenses need to evaluate the business justification for data encryption. Are the initial costs and ongoing maintenance fees for data security solutions worth the benefits?

In a recent study, the average cost of a data breach is \$6.65 million. It was also reported in a separate study that 73 percent of company respondents said they experienced a data breach in the past two years. To be conservative, assume that a company will suffer a data breach every three years. So divide \$6.65 million by three to come up with an average annual data-breach cost of \$2.16 million—or \$540,000 per quarter. Bigger companies with lots of devices and data to protect would have greater exposure. Smaller companies might have less.

From here, take a mythical company of 10,000 seats and outfit those seats with data encryption software, figuring the cost conservatively at \$100 per seat. The purchase price for that allotment would be \$1 million, with an annual maintenance fee of \$180,000—putting the total at \$1.18 million. With the cost of the data breach being \$2.16 million, and software coming in at roughly just under a million dollars less than the data breach, it is easy to see that the software pays for itself within one year.

Conclusion

The deck is stacked against businesses in terms of data security. With the many different types of devices on the market, the number of opportunities for those devices to be hacked, lost or stolen greatly increases. And as mobile devices become sleeker, faster and easier to use, they'll continue to be in high demand. Businesses will leverage these devices as the way to more readily do business.

In order to ensure an organization's data remains protected, it is a priority to secure it through the most up-to-date and stringent means available. Data encryption is the most cost-effective and secure form of data protection that ensures data integrity—inside the four walls and out.

*Kurt Lennartsson is the Chief Technology Officer at **Mobile Armor**. Kurt's more than 20 years of experience in the security industry has involved directing, architecting and developing software and hardware for computer security and large scale systems (both Web and mobile). Kurt is the co-inventor of more than 10 patent applications in the security field. Some of the strengths Kurt's extensive security industry background brings to Mobile Armor include significant experience in mobile device encryption systems, PKI firewalls, intrusion detection/prevention systems, smart cards and AAA authentication systems. Kurt also headed several government-mandated security certification projects for both FIPS 140 and Common Criteria (EAL4). He can be reached at klennartsson@mobilearmor.com.*