Safeguarding Businesses from Mobile Data Breaches

Combating the Threat of Laptop Theft and Loss

A Zenith Security Solutions White Paper

Executive Summary

The time is long past when the only threat to a company's sensitive and proprietary data came from hackers targeting its Web site. Today, with business professionals turning to laptop computers as their most powerful information management tool, the rates of laptop theft and loss have risen dramatically.

Laptops and the huge amounts of data they can store have become high-value targets for thieves. Each missing laptop magnifies the probability that valuable data will fall into the wrong hands. Companies ignore this risk at their peril.

A data breach from a missing laptop can expose a company to a variety of catastrophic scenarios —causing potentially irreparable damage to an organization's reputation, its brand, its market share and its earnings.

A data breach from a missing laptop can expose a company to a variety of catastrophic scenarios.

Hardly a week goes by without some news report about the impact of a data leak from a missing laptop. Businesses that haven't experienced such a traumatic event should consider themselves fortunate, but it's only a matter of time before they join the ranks of the victims

Fortunately, there are concrete steps that companies can take to minimize the risk of such a breach. In fact, there are so many technologies available for laptop security that the choices can seem overwhelming.

This white paper is intended to simplify the task of selecting an appropriate technology, in order to help decision makers meet the ongoing mobile data security challenge. It surveys and evaluates a variety of laptop security options and presents some recommendations as to which ones businesses should implement in order to combat the growing threat of a data breach.

It's vital to recognize the dangers of mobile data theft or loss. Equally crucial is taking prudent security precautions to safeguard data.

Introduction: Mobility & Vulnerability
The Growing Threat of Mobile Data Theft & Loss

In today's global marketplace, laptops have replaced traditional desktop computing for most business professionals. Mobile computing has many advantages. It makes workforces more flexible, responsive and productive. The nearly limitless storage capacity and powerful processing capability of laptops puts unprecedented amounts of information at a user's fingertips, no matter where they may be.

But along with these benefits come substantial risks. Every year, laptops by the thousands vanish from airports, hotels, cars, taxicabs, offices, restaurants and even homes. According to the FBI, a laptop is stolen in the USA every 53 seconds, and 97 percent of them are never recovered. Even the FBI's own laptops have disappeared, many of them containing sensitive and classified information.[1]

Much of the value of a lost or stolen laptop resides in its data rather than its replacement cost. According to a study by the Ponemon Institute, a data breach represents almost 80% of the total cost of a missing laptop, compared to just 2% for replacing the computer,[2] as Figure 1 illustrates.

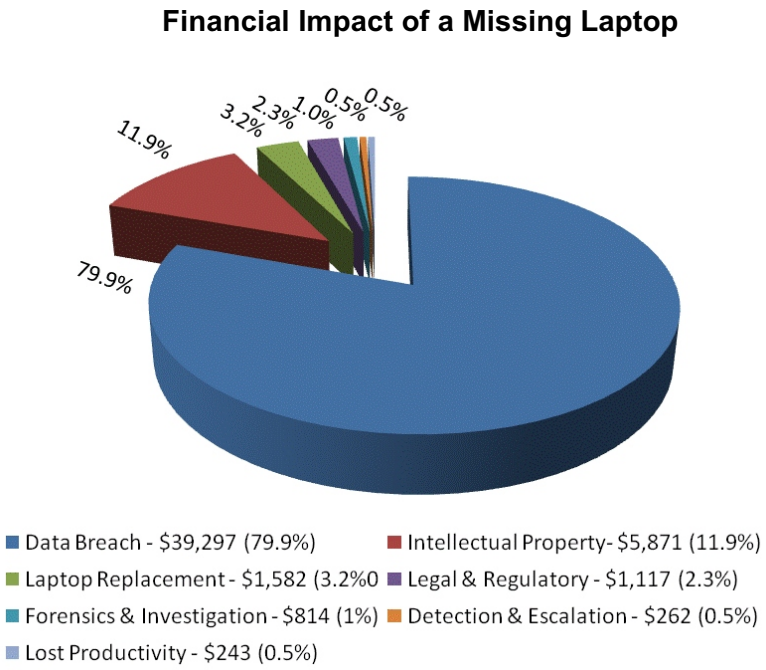

Figure 1: Data Breach Represents 80% of the Cost of a Missing Laptop

The lost data can include not only valuable information about a company's operations, finances, strategy, planning, contracts, customers and competitors, but also Social Security numbers and other private and personal employee data that can be used to perpetrate identity theft.

[1]FBI Reports on Missing Laptops and Weapons, Washington Post, February 13, 2007
[2]The Cost of a Last Laptop, Ponemon Institute, April 2007

Regardless of where and how it occurs, a data breach from a missing laptop can produce a host of nightmarish consequences—including negative publicity, damage to corporate brands, missions and careers, government scrutiny and liability lawsuits. It can even jeopardize a company's financial viability, as Kevin Rowney, Director of Breach Response at Symantec, points out: "It is conceivable that a company can lose its corporate life through a large scale data breach." [3]

"It is conceivable that a company can lose its corporate life through a large scale data breach."
- Kevin Rowney, Symantec

The potential repercussions could hardly be more severe. The goal of this white paper is to help companies avoid them, by making informed decisions about how to protect themselves from a mobile data breach.

[3]BBC News, February 2009

The Four Components of Laptop Security

Technologies for securing laptops and their data give companies a wide range of security options. The choices can seem bewildering, but they become more comprehensible when classified into the four primary components of laptop security: deterrence, detection, authentication and protection.

The many choices for securing laptops and their data become more comprehensible when classified into the four primary components of laptop security.

1. Deterring Laptop Theft

The most desirable and cost-effective way of avoiding the risk of a data breach from a stolen laptop is to prevent theft from occurring in the first place. The technologies for deterring laptop theft fall into two main categories: locking devices and alarm systems. Both are generally inexpensive and easy to use. They do, however, have some weaknesses.

For example, locks can be effective deterrents, but they're somewhat cumbersome, especially when traveling. They are also far from foolproof. There have been cases of laptops being stolen from offices even while secured to desks with heavy-duty cable locks in a secure building.

The most sophisticated laptop alarm systems are based on either motion detection or passive immobilization technology. Motion detection causes an alarm to sound when a laptop is moved beyond a perimeter pre-set by the user. The immobilizing system blocks access to the computer's operating system to keep it from starting up.

2. Detecting a Missing Laptop

Tracking software installed on a laptop can trigger a lost or stolen computer to make a call to a monitoring service each time the laptop is logged on to the Internet. This presents the possibility of recovering a missing laptop.

According to the Ponemon Institute's study[4], the quicker the discovery that a laptop is missing, the lower the financial impact of the loss.

3. Authenticating the Laptop User

Authentication technology is designed to prevent unauthorized access to a laptop, generally by anyone other than the user or a company's IT administrator.

Operating system-level authentication systems such as passwords can block access to a laptop's operating system. However, if the hard drive is moved to another computer, or if the laptop is set up to allow startup from a floppy disk, password authentication can often be bypassed by an attacker and the operating system and data files can be accessed. It's therefore advisable to use a more robust method of authentication, such as biometrics.

[4]The Cost of a Last Laptop, Ponemon Institute, April 2007

Biometrics is the science of identifying a person by reading his or her unique body features. The most common type of biometric identification for laptops is by fingerprint. The system authenticates users based on the similarity of their fingerprints to that of a stored fingerprint template created when the system first runs.

Some laptop manufacturers offer built-in biometric fingerprint identification systems. However, many of the built-in systems operate independently of the operating system, so that a false negative (the failure to correctly identify a user) will prevent the laptop from starting up at all.

Another disadvantage of built-in systems is that they generally store biometric fingerprint template data on the laptop's hard drive. An attacker who succeeds at retrieving the template data can use it to create a counterfeit fingerprint and gain access to the laptop's data. External biometric devices diminish these risks.

4. Protecting Data

Encryption is the process of transforming data to make it readable only by those possessing a digital key to decrypt it. It has long been used in military and espionage operations, and is generally considered the most effective data protection technology.

The most robust type of authentication is biometrics, while encryption is generally considered the most effective data protection technology.

There are two main types of encryption: full disc and flexible. **Full disk encryption**, as its name suggests, encrypts all the data on a disk. Since the decision about which files to encrypt is not left up to the user, there's no risk of leaving sensitive files accidentally unencrypted.

The major vulnerability of full disk encryption is that an attacker who manages to decrypt the drive will have access to all of its files.

Flexible Encryption, on the other hand, allows the creation of different decryption keys for various portions of the disk, such as particular files, folders or partitions. Thus, an attacker cannot decrypt the entire disk at once. In addition, the user can decrypt individual files on a need-to-know basis while working with colleagues and customers, leaving the remaining data encrypted and secure.

Encryption key storage is another important security consideration. Many laptop encryption systems store the keys on the laptop's hard drive, making them vulnerable to attack by cold-booting the laptop (i.e. turning the power off and then back on), then dumping the contents of memory before the data disappears. It's far more secure to store the keys in an external hardware device.

# # # # # #

Given the exposure that a mobile data breach represents for a business, an understanding of the comparative strengths and weaknesses of all these available technologies is essential, in order to meet the continuing laptop security challenge.

Features of an Ideal Laptop Security System

Despite the claims of some security experts, no system is 100% secure. A determined and resourceful thief can foil the most allegedly “bulletproof” technology. The objective of a security system is to make the effort and time needed to “crack” the system so astronomical as to be impractical, so that the attacker goes elsewhere in search of easier pickings.

The ideal laptop security system addresses multiple security risks and vulnerabilities. It deters theft, detects it when it happens, prevents unauthorized access and protects data. The system should address all four components. Systems that focus on one component while neglecting the others ignore substantial risks. A higher overall level of security is achieved when a combination of approaches is used.

A higher overall level of security is achieved when a combination of approaches is used.

1. The Ideal Deterrent System

Theft deterrence should always be the first line of defense in any laptop security system. The deterrent system should include both motion detection and passive immobilization technology, Alarms alone are insufficient, since those that are accidentally triggered (often by the user, after forgetting to disarm the system) will usually be ignored.

Arming and disarming of the system should be easy to accomplish via an external device connected to the laptop. The system should also offer the option of automatically arming itself under specific circumstances, such as when the operating system starts up, when the screen saver comes on, or when the system enters suspend/hibernate mode.

2. The Ideal Detection System

When deterrence fails and a laptop is lost or stolen, the security system should have the capability of tracking and locating a missing laptop.

After discovering that a laptop is missing, the user should be able to contact the security system provider by phone or email or by logging in to a user account on the company’s Web site.

An additional and highly desirable feature would be the ability to surreptitiously retrieve data remotely over the Internet and then delete it from the laptop’s hard drive.

3. The Ideal Authentication System

For cases when both deterrence and tracking fall short, the system should be equipped with the strongest available authentication technology—that is, biometrics.

Storing biometric fingerprint template data on a laptop’s hard drive exposes it to theft, counterfeiting and replication. The ideal system should be equipped with an external tamper-resistant biometric device that stores the template data and does not allow access to it by unauthorized persons.

For added security, the device's biometric fingerprint scanning and recognition capability should meet National Institute of Standards and Technology (NIST) benchmarks.

4. The Ideal Data Protection System

For those rare instances when deterrence, detection and authentication do not succeed in stopping an attack on a laptop, encryption should become the last line of defense.

When deterrence, detection and authentication do not succeed, encryption should become the last line of defense.

Storing the encryption keys on a laptop's hard drive leaves them vulnerable to retrieval by an attacker. It's preferable to keep them on an external device that doesn't allow access to them and can perform encryption and decryption operations internally. These operations should take place only within the protected environment of the device's microchip, never on the laptop.

The system should also allow the option of either full or flexible encryption, at the user's discretion. In this situation, files could be either encrypted all at once or individually, by file type, folder or partition. Such a system would offer the user the ability to encrypt and decrypt related data together. The rest would remain encrypted and secure.

As the history of espionage illustrates, all encryption systems can theoretically be broken. The effective ones frustrate attackers with the most robust commercially available technology that meets the Federal government's Advanced Encryption Standard (AES) for encryption strength.

# # # # # #

Any solution to mobile data loss or theft must be not only comprehensive, but also convenient and easy to install and operate, with an intuitive user interface. To the user, it should be completely transparent. The importance of minimizing user inconvenience cannot be emphasized too strongly. If a system is a difficult and annoying to implement, there will be more calls to a company's IT tech support or, even worse, it will not be used at all.

Conclusion

Laptop computers give business professionals the data portability and access they need to compete in today's global business environment. But along with the substantial benefits of laptop technology come enormous risks.

With workforces increasingly mobile and laptops proliferating, theft and loss have become critical security issues that companies can no longer afford to ignore.

Today, business professionals are carrying more sensitive and confidential data than ever before on their laptops, and losing them at unprecedented rates.

Companies need to remain vigilant in safeguarding their laptops and the valuable data they contain. A single line of defense is not enough. Organizations must proactively protect their mobile data assets with comprehensive, multi-layer security technology that makes use of multiple components working in concert for maximum protection.

Organizations must proactively protect their mobile data assets with comprehensive, multi-layer security technology.

Zenith Security Solutions offers a completely integrated laptop security system, housed in compact, self-contained, portable peripheral devices. Zenith's mobile data security suite is simple and straightforward to use and addresses all four key components of mobile data security:

- ***Deterrence:*** Stopping thieves with a combination of motion detection and passive immobilization technology
- ***Detection:*** Not only tracking a missing laptop so that it can be recovered, but also covertly retrieving its data and then deleting it
- ***Authentication:*** Tamper-resistant biometrics technology that achieves the highest NIST benchmarks
- ***Protection:*** Data encryption that meets the most stringent Federal government AES standards

For more information about Zenith Security Solutions and its complete suite of laptop security solutions, please visit our web site at www.zenithsecurity.com.