

# Mobilise IT: Securing Mobile Workers to Ensure Data Protection

“

*The impact of thieves entering the network is significant. For example, the second most significant computer crime that contributed to corporate losses during 2004 was unauthorised network access, falling just behind viruses.*

”

“

*When mobile devices are stolen, forgotten or lost, they put critical data at risk. Often, employees use simple-to-guess passwords or write them down on notes in their laptop case, the equivalent to leaving a house key under the doormat.*

”

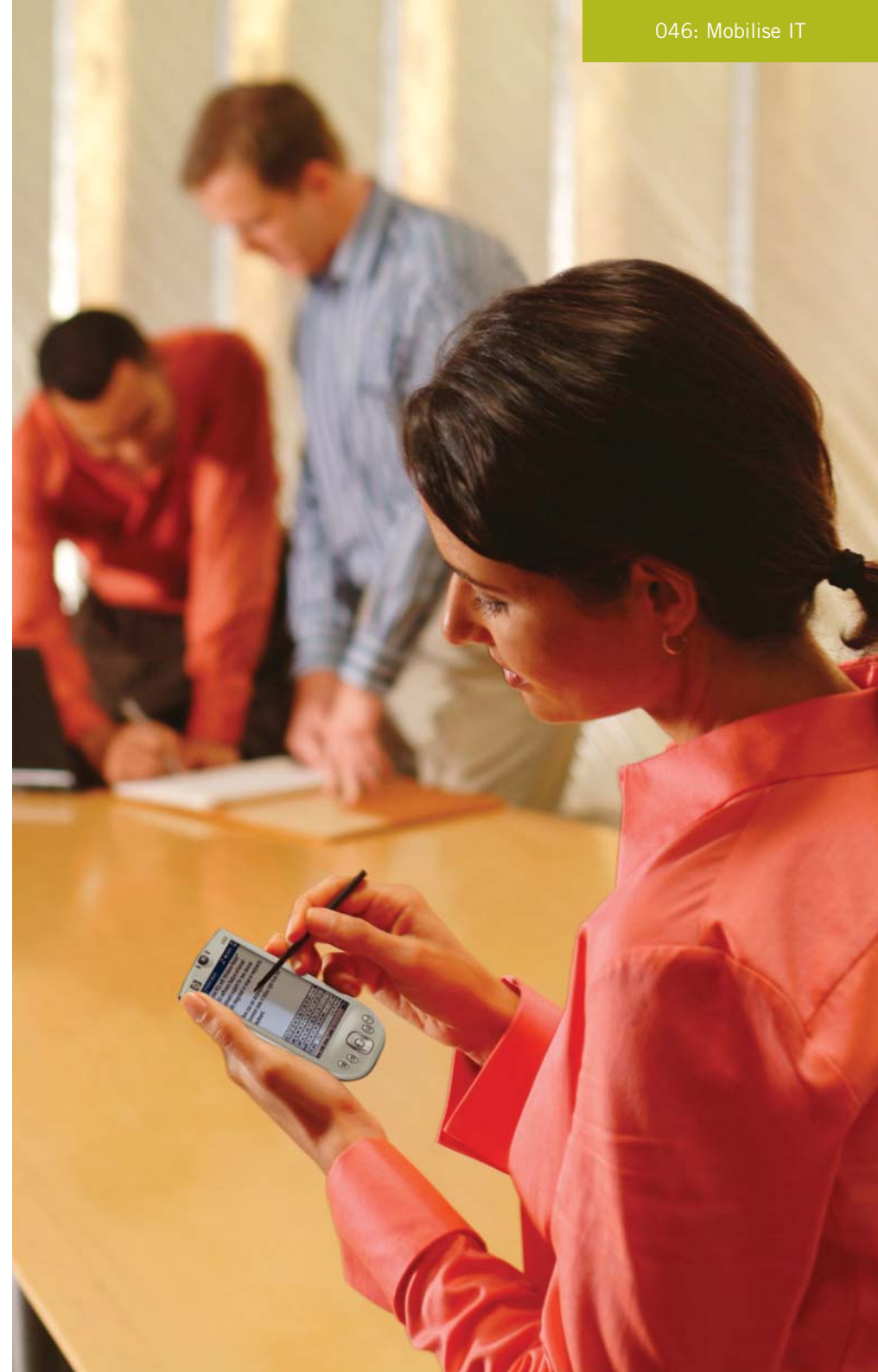
***The growing mobile workforce is extending the network perimeter beyond traditional business offices and into airports and cafés. As remote employees become more commonplace, so do threats to business data and intellectual property. Stolen laptops, compromised passwords and weak security procedures are opening critical business information to thieves and hackers.***

***When confidential information ends up in the wrong hands, organisations can experience bad PR, regulatory violations and even terminated business relationships. To overcome these challenges, businesses need to adopt strict security procedures that leverage the latest in mobile security technology. This paper will examine some of the security challenges caused by mobile workers and introduce products that are adding significant levels of protection to the IT environment.***

## ***Mobile Security Market Drivers***

Mobility is now mainstream. Laptops and other mobile devices are more economical than ever and improve productivity by enabling employees to take their work wherever they go. For the first time, laptop sales have exceeded desktop sales in the United Kingdom. Tens of thousands of wireless hotspots, combined with cellular, Bluetooth and infrared technology, enable employees to go anywhere—from coffeehouses to airports—and connect with the infrastructure.

With mobile freedom comes great risk. The news is abuzz with reports of stolen credit card and social security numbers from major corporations. Bank of America, CardSystems and Citigroup each reported millions of compromised





# Mobilise IT: Securing Mobile Workers to Ensure Data Protection

accounts. In the case of CardSystems, industry professionals speculate that a hacker entered the company's network via a company-owned PC, such as a laptop.

The impact of thieves entering the network is significant. For example, the second most significant computer crime that contributed to corporate losses during 2004 was unauthorised network access, falling just behind viruses. The average loss from unauthorised information access rose from £28,000 in 2004 to more than £168,500 in 2005.

As IDC explains, "Users are often the weakest of the weak links. In the case of passwords, for example, users have too many to manage reasonably. As a result, they tend to write them down on a piece of paper that may be found easily." IDC explains that the majority of businesses are not adopting encryption and strong authentication solutions at a sufficiently rapid pace.

## *The Challenges of Unprotected Mobile Users*

Critical customer, patient or company confidential intellectual property is at risk when mobile user devices are not properly secured. At the most basic level, a person could be looking over an employee's shoulder and watching him or her type in access codes and passwords. At the extreme opposite, highly skilled criminals can target devices for theft. For example, the CEO of Qualcomm stepped away from a podium at a national press meeting and 15 minutes later his laptop was gone, along with trade secrets that were considered highly valuable to foreign governments.

When mobile devices are stolen, forgotten or lost, they put critical data at risk. Often, employees use simple-to-guess passwords or write them down on notes in their laptop case, the equivalent to leaving a house key under the doormat. In some cases, business secrets may be replicated on

local hard drives as matter of policy, opening data to greater risk following laptop theft. Personal digital assistants (PDAs) and smart phones may also contain unprotected information.

Stolen passwords or devices can enable a thief to access business data and quickly pull down information in minutes. Data equals dollars to information thieves because customer credit card information can be quickly sold online. Over the past 18 months, hackers have increasingly teamed up with organised criminals to execute sophisticated schemes, such as taking data hostage. When sensitive business information is compromised, it can cause embarrassment, costly damage to reputation and create a significant financial or commercial impact.

## *The Solution: A Suite of Technology*

A combination of authentication and encryption procedures and network protection is critical to protect data from hackers and thieves.

**Authentication and Encryption:** Beyond the obvious use of virtual private networks (VPNs) for tunnelling securely into networks and using the secure socket layer (SSL) when transmitting information via the Internet, there are some additional steps that can be taken to ensure that a user is who he or she claims to be.

**Passwords:** A first and obvious step is to encourage remote employees to regularly change their passwords and create strong passwords that are alphanumeric in nature. A strong password contains at least eight characters, includes a combination of letters, numbers and symbols, and is easy for the user to remember, but difficult for others to guess. Microsoft's Web site explains the advantages of passphrases: "A passphrase is a sentence that you can remember, like 'My son



# Mobilise IT: Securing Mobile Workers to Ensure Data Protection

Aiden is three years older than my daughter Anna.' You can make a pretty strong password by using the first letter of each word of the sentence. For example, msaityotmda. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. For example, using the same memorable sentence and a few tricks, your password is now M\$8ni3yOtm@d@."

**Biometric Authentication:** Biometrics are also becoming excellent forms of authentication.

Fingerprint verification is becoming more common for mobile devices. A fingerprint cannot be forgotten, misplaced or shared. Biometrics are part of a multifactor authentication model, which includes something you have or something you are, and something you know. For example, an ATM card is a two-factor authentication model because a user must have the ATM card and know the personal identification number (PIN). If the card is lost, it is of no significant concern because the person who finds the card does not know its PIN code. Similarly, with fingerprint authentication, a password should still be required to access systems. Newer laptop systems are emerging that include built-in fingerprint readers.

**Authentication Devices:** Authentication devices can also add an extra layer of security for laptop users.

Following the multifactor authentication model, authentication devices are physical products that plug into a computer and must be presented along with a password for authentication. These devices are small enough that they can be added to an employee's key-ring or be embedded in a smart card, and are useless without knowing the accompanying password. Some authentication devices are capable of holding user credentials and certificates for public key infrastructure (PKI) exchanges.

**Encryption:** Modern laptops also include embedded security chips that protect sensitive PKI private keys that decrypt sensitive data. Files, folders or entire hard drives can be automatically

encrypted to prevent unauthorised viewing of data when a mobile device is attached to a network or in the case of physical theft.

In addition, password managers can store and encrypt Windows passwords, user IDs and even common form entries. A passphrase, fingerprint or authentication device can be used to decrypt critical data.

**Network Protection:** Data network systems have evolved to protect internal systems from unauthorised access while providing timely access to legitimate users. These solutions can identify and prevent malicious behavior before it spreads, heading off known and unknown security risks.

Classic network security capabilities include identifying users, providing access control and inspecting data traffic. Newer solutions examine the context of the user by examining credentials at user sign-on and reacting to anomalies, such as quarantining a system that has been infected with a virus. In addition, modern network security systems establish a level of trust that a user is who he or she claims to be by validating that credentials have not been revoked, and confirming the user's identity and the location of the device.

Advanced solutions can prevent worms and viruses from gaining control of systems or from spreading across the network by rapidly communicating with other systems to reduce the effect of an attack. Advanced solutions simplify threat identification, investigation, validation and mitigation by providing visuals of real-time hotspots, incidents and attack paths.



# Mobilise IT: Securing Mobile Workers to Ensure Data Protection

The security state of a laptop can also be examined and users can be quarantined, restricted or denied access based on the operating system, patch updates and virus signatures. Thus, an older, less secure operating system could be prevented from connecting to the network and introducing potential vulnerabilities. In addition, security credentials can be verified, preventing a stolen system from achieving network access.

Non-compliant or untrusted devices, such as PDAs, can be restricted from entering the network. Furthermore, advanced VPN solutions can securely remove client information such as cookies, browser history, temporary files and downloaded content after a secure session has been terminated.

## What to Look for in a Mobile Security Solution Provider

When looking for a mobile security solution provider, many key issues should be examined. Look for the following:

**Proven methodology:** Be sure to work with a solution provider that has successfully helped secure mobile devices and the network infrastructure. The methodology should include a formal assessment process, solution design and implementation.

**ISO 9001:2000-certified configuration:** Seek a vendor that can perform custom integration, configuration, testing, authentication and activation at an ISO 9001:2000-certified configuration centre to guarantee consistency, ensure thorough testing, and provide a rapid deployment. The vendor should also have high-quality assembly procedures and expertise to ensure the integrity and functionality of built-in security technologies.

**Many strategic relationships:** Work with a provider that understands the full range of available mobile security technology and can offer the best mix of products to meet the mobile security needs of the business.

**Vendor-agnostic:** Work with providers that are not limited to specific hardware manufacturers or software vendors so the best solution can be developed for each need, based on all available options. In addition, work with a vendor that has strong partnerships and co-development efforts with top-tier manufacturers.

## About Insight mobile Security Services

Insight offers full-service mobile security services for organisations of all sizes. Insight begins with a comprehensive assessment of existing security practices and recommends security methods and products best-suited for each client. With a strong relationship with major security-related manufacturers such as Symantec, Cisco, IBM, HP and Lenovo, Insight can design a mobile security solution that is highly customised for each project.

Leveraging its proven methodology, ISO 9001:2000-certified configuration centre and a national presence, Insight is an excellent choice for mobile security initiatives. Insight's unique relationships with more than 1,500 manufacturers and software vendors empower businesses to match the best technology to their needs while securing the best price. Insight features extensive consulting, engineering and managed services that cover topics ranging from regulatory compliance to strong authentication to email security.

To learn more about Insight's mobile security services, contact Insight or visit [www.insight.com](http://www.insight.com).



# Mobilise IT: Securing Mobile Workers to Ensure Data Protection

Insight and the Insight logo are registered trademarks of Insight Direct USA, Inc. All other trademarks, registered trademarks, photos, logos and illustrations are the property of their respective owners. ©2005, Insight® Direct USA, Inc. All rights reserved.

## References

*Paul, P. (June 21, 2005). TechNewsWorld. CardSystems Unsure How Data Was Breached.*

*Gordon, L., et al. (2005). 2005 CSI/FBI Computer Crime and Security Survey.*

*Ibid.*

*Kay, R. (February 2005). Validation of Hardware Security in PC Clients.*

*See <http://wired-vig.wired.com/news/business/0,1367,38855,00.html>*

*Rubner, J. (July 1, 2005). Atlanta Business Journal. Information theft fast becoming big business.*

*See <http://www.microsoft.com/athome/security/privacy/password.msp>*