Business Security Advisor – Final Copy
September Issue, 2001

From Desktop to Desert – Protect Your Devices, Protect Your Data

by John Muir

The use of portable computers is estimated to grow by more than 50 percent in the next few years. The META Group projects 20 million PDAs and handheld devices will be in use by 2003. The Gartner Group forecasts that more than one billion handheld computers and mobile telephones with wireless network connectivity will be in use globally by 2003. This surge in use of mobile devices means that companies need to make sure their growing mobile workforce use devices that are secure so that handhelds do not become the weakest link in their security system.

Just as many organizations have completed multi-year projects protecting network security perimeters with firewalls and VPNs, a wave of mobile computing devices threatens to make perimeter defenses as ineffective as if one had locked all the doors but not the windows before leaving on a long trip. Notebook PCs, PDAs and Internet-ready 'smart phones' move in and out of a company's security perimeter on a daily basis, carrying strategic information out and possibly bringing in hidden viruses, trojan horses and malicious code. Worse still, these devices frequently store the user passwords or scripts necessary to access the organization network from the outside.

Easily stolen and quickly accessed, mobile devices are attractive to data thieves and malcontents because they hold large amounts of data often with little or no security protection. Recent data privacy legislation has focused on securing information stored on mobile devices, specifically within the healthcare and finance industries. Recent compliance guidelines in the U.S. for the *Healthcare Insurance Portability and Accountability Act* (*HIPAA*) and the *Gramm-Leach-Bliley Act* state that individuals within an organization are equally responsible for the integrity and security of company information, regardless of the type of device on which the data resides. Further, both pieces of legislation state that professional certifications can be revoked if information falls into unauthorized hands, even if that information was illicitly accessed. *Other countries have similar data protection and privacy laws.*

Steps to Protecting Data Enterprise-Wide

The increasing use of mobile devices coupled with legislative and liability concerns means that executives need to review security policies and architecture. First, you should conduct a survey to ascertain the number and types of devices that are currently in use or planned for use near-term. Prioritize your security objectives for mobile devices and determine which of the following requirements pertain to your organization:

- maintaining confidentiality and integrity of all data and applications stored on PCs, laptops and PDAs;
- protecting all the devices and resident applications from trojan horses, viruses and other malicious code that can compromise data and network security;
- protecting passwords, scripts and other information required to access networks and other devices;

- providing a secure platform to conduct secure interactions with trusted entities across networks, including financial transactions, virtual private networks, email and other messaging tools.

Second, consider the operating environment, or combination of environments, where mobile computing devices will be used. The work environment is a major determinant of the type of security that your organization will require.

Third, to be successful, mobile device security solutions must be:

- automatic and transparent to the user to avoid to prevent lapses in security procedures – convenience is paramount when dealing with portable devices;
- sufficiently strong for the type of information to be protected and the environment in which the device is used – from inside Fort Knox to wireless connections in the jungles of Borneo;
- capable of being centrally deployed and administered across the network, including wireless administration;
- designed to avoid loss of performance of the device while in use – processing power and speed do not need to be compromised for security.

Once the fundamentals are understood and agreed, consider the types of security technologies necessary to implement your security strategy:

- Physical device protection, such as key locks to prevent unlawful operation and tethers to prevent device theft.
- Access control software to restrict the use of a device to authorized and authenticated users only. This includes password control software, smartcards and token solutions.
- Hard drive encryption. It should encrypt the entire hard drive. Data is decrypted on-the-fly as needed – automatically, with no user-discretion required, and it is almost always coupled with access control
- File encryption to "scramble" specific high-risk files to prevent unauthorized disclosure – when used with PCs and laptops user-discretion is required.
- Removable hard drives that can be removed and stored in a safe place to prevent theft or intrusion.
- Virus and trojan horse prevention that is essential to preventing corruption to or loss of stored data. It prevents a PC from being used in DNS attacks on other machines.
- Personal firewalls to control and monitor network access to the devices that connect directly to the Internet; these examine data packets for malicious code.

Sustainable data security for mobile devices requires implementing the proper measures in light of the risk profile and the environment where the devices are used. For example, what is appropriate for a home office desktop PC will be far different than what is required for the laptop or PDA containing critical and strategic information needed by an executive of a large organization or government agency. While the following table illustrates some likely scenarios, careful consideration of all factors must be made before determining which security measures to implement.

Suggested Security Measures

	Essential Security Elements for Small Business	*Essential Security Elements for Enterprises*
Laptop	Encryption Anti-virus	Access control Full disk encryption

	Personal firewall	Anti-virus Removable drive
Desktop	Anti-virus Personal firewall	Access control Full disk encryption Anti-virus
PDA	Access control Encryption	Access control Encryption

Finally, view mobile device security as an enterprise issue, because it really is. An enterprise approach to security may require the organization to standardize on a few devices in order to facilitate a workable security policy. A large-scale implementation will require web-based administration software that deploys and manages security modules across the network for use with the various devices that operate on multiple operating systems. Such a system allows for centralized auditing of all security-related activity on mobile devices.

In summary, the proliferation of mobile computing devices will undoubtedly change your organization's risk profile and require additional policies leading to the implementation of an enterprise security system. Effective mobile device security prevents unauthorized access to data or credentials and the use of the device as a carrier or gateway for malicious code to enter the network.

John Muir is a co-founder and member of the board of directors for Pointsec Mobile Technologies, Inc. (www.pointsec.com), a leading developer and marketer of security software.