



White Paper: **Mobile Security**

Mobile Security: The Essential Ingredient for Today's Enterprise

In a well-publicized case, a data analyst employed by the U.S. Department of Veterans Affairs (VA) took his laptop home to suburban Maryland. Burglars entered his home and stole the laptop. Suddenly, the personal information of some 26.5 million veterans was at risk. The incident became an international news story raising caution flags about managed security at the VA.

Incidents like this one are not unusual today, and the risk is increasing as the mobile workforce grows. Gartner reports that 83.9 percent of businesses have a remote workforce, and by 2011 an estimated 46 million employees globally will telecommute at least one day per week and 112 million will work from home at least one day per month.

Software and technology solutions help mitigate security risks and safeguard organizations from threats, but they require IT staff to select, deploy and maintain them. The problem is, today's IT environments are lean. This paper examines the current mobile security landscape, including myths surrounding the risks and threats, and how organizations can establish a solid mobile security strategy.



Custom Solutions Group

The Mobile Landscape

The mobile workforce is increasing. More than 17 million Americans got their work done via telecommuting in 2008, a 74 percent increase over the previous three years, according to WorldatWork Telework Trendlines.

How is this changing our workforce? Mobile work encourages cross-pollination of different cultures with fresh ideas and innovative practices for collaborative teams. In a telecommuting survey sponsored by Robert Half International, 53 percent of respondents said the ability to work at home is important to their employment choice. In the most recent annual telework survey by CDW Corp., 40 percent of the respondents agreed that “the option to telecommute would influence their decision to remain with their employer or take a new job.”

On the one hand, teleworkers help alleviate the daily minutiae of managing in-house employees, giving management more time to strategically develop initiatives. But on the other hand, a dispersed team of mobile workers creates more work and new concerns for IT managers. For example, in a recent survey of CIOs, 45 percent said they were not confident that their company’s policies and security measures prevent mobile employees from sending confidential information to unauthorized third parties—such as sending company information from a laptop to a home PC (IDG Research Services on behalf of Fiberlink Communications, 2008).

Ensuring security is a formidable challenge for IT managers. Mobility creates opportunity for hackers and predators and increases other threats and vulnerabilities. It requires a new approach to security management, including an assessment of security plans and policies and, ultimately, the creation of a mobile security strategy.

Identifying Myths

Before development of a strategy for securing mobile workers and data, some common myths about IT security practices should be clarified and dispelled.

MYTH 1: Having a core security program in the office environment means that IT assets and data are safe everywhere.

Mobile security is not confined to the office or headquarters location. Wherever a mobile worker goes, so goes a virtual office. The price and performance of laptops, coupled with wireless access availability, have created

a work-from-anywhere preference. However, working outside the office guarded by firewalls and intrusion measures can increase risks for businesses. Dispersed employees have lower visibility than those in the office. It requires resources, time and technology to remotely monitor and control which sites users visit, the information they exchange and the online connections they use.

“Given our business as an international communications solution provider, our challenges are often compounded by the need to support customers and business functions in a variety of locations,” says Michael Glenn, director of Information Security and chief information security official (CISO) at Qwest Communications International Inc., a managed security provider.

Employees now connect and work via wireless networks and Wi-Fi hotspots and expect to access data 24x7 from their personal smartphones. Unencrypted wireless access points often do not offer the security levels necessary to protect corporate data. Unencrypted public wireless access makes it possible for an outsider to detect a user, enter a wireless network and potentially steal data. The same scenario is not true with encryption, where data is modified to prevent access.

Unencrypted hotspots are causing concern about the integrity and safety of wireless access; 47 percent of CIOs and IT leaders say they are not very or not at all confident that their company’s policies and security measures prevent mobile employees from accessing the Internet via unencrypted public wireless access points (IDG Research Services for Fiberlink Communications, 2008).

MYTH 2: Existing mobile security programs are good enough as is and don’t require investment or long-term planning.

Many IT managers believe that their existing mobile policies are sufficient to mitigate risk. However, vulnerabilities and threats constantly change, as do the ways predators exploit weaknesses in IT infrastructure.

Mobile users and the technology used to accommodate them are growing and changing. For example, it took BlackBerry five years to get its first million users, just another 10 months to get its second million and six months for the next million. Today the company has more than 28 million users. The steep increase in usage and the evolving need for new features and capabilities have heightened the risks and vulnerabilities.

Complying with encryption regulations and controlling threats requires vigilant monitoring processes, because blind spots exist when assets are deployed in remote places. Workers travel everywhere with their laptops, smartphones and other equipment. They can work virtually anywhere. An unnoticed vulnerability potentially exposes proprietary data to unwanted parties.

MYTH 3: Do-it-yourself managed mobile security is a better, less costly alternative to outsourcing.

In recent research, CIOs declared that privacy and secu-

rity concerns are the leading objection to outsourcing. However, roughly half of these IT executives reported that they are still likely to outsource some type of data, voice or network service over the next 18 months (IDG Research Services and Fortune on behalf of Qwest Communications, May 2009). In the research, cost savings were the most frequently cited benefit of outsourcing, followed by access to expertise.

Building an in-house program requires staff and technology, and ultimately, investment. And sometimes having

Five Steps to Reduce Mobile Blind Spots

Today's mobile workers are everywhere. From their kitchen tables to airports to remote office locations to headquarters offices, they roam past geographic boundaries and operate on many different networks. A wide variety of vulnerabilities can potentially threaten and damage an organization's IT systems and data. Here are five steps security managers can take to reduce these risks and ensure that mobile blind spots do not bring unwanted publicity and costs to the organization.

1. ENSURE VISIBILITY

- ✓ Continually monitor the health and compliance of all laptops with tools for monitoring applications, flagging those that are out of company compliance and encrypting and locking down sensitive data deployed in a laptop or other device.
- ✓ Enforce policies and do remediation as needed.

2. PROTECT SENSITIVE DATA ON BUSINESS ENDPOINTS

- ✓ Monitor, protect and update mobile devices, including those outside the corporate LAN, with tools that provide secure access to the company network via an optional virtual private network (VPN) client, as well as authentication and encryption.
- ✓ Monitor and enforce rules about and remediate obsolete software. Provide adequate security protection for device use from any location.
- ✓ Disable noncompliant endpoints.
- ✓ Set boundaries for information transfer.

3. DEVELOP A SPECIFIC POLICY TO PROTECT THE ORGANIZATION

- ✓ Develop a policy for damaged, lost or stolen mobile devices, and protect sensitive information as necessary.
- ✓ Monitor deployment of encryption tools, and prevent employees from copying or distributing sensitive data. Ensure your company's ability to meet e-discovery obligations.
- ✓ Make sure your policies enable you to monitor company data and meet all compliance and legal obligations from company-issued as well as personal mobile devices.
- ✓ Track and document the status and condition of mobile and remote systems software.

4. TIE ACCESS TO DIRECTORIES, IDENTITIES AND ROLES

- ✓ Allow access to the resources on the corporate network based on the individual, that person's role and organizational policy.
- ✓ Ensure that licensed content, digital rights and the distribution of content are protected.
- ✓ Secure integrated communications for VoIP, e-mail and e-commerce transactions.
- ✓ Enable the image that appears on the remote workstation to be identical to that on the home office workstation.

5. ENFORCE PRODUCTIVITY

- ✓ Notify employees that instant message conversations are monitored and that logs are stored for possible management review and e-discovery obligations.
- ✓ Monitor, audit and collect usage statistics for management purposes.

an internal, dedicated staff equipped with the most-up-to-date security technologies can turn out to be more expensive than hiring a managed service provider. It's important to perform a cost analysis of do-it-yourself versus outsourced managed security.

MYTH 4: In-house staff is always up to date on the latest security threats and trained in the processes, solutions and equipment needed to combat them.

Managed security providers bring expertise in finding solutions to fit complex problems, solutions that may not be available in-house. With cross-industry experience, an outsourcing provider must stay abreast of developing threats and investigate products and security solutions to address them. Their experience affords recommendations that save time and money.

The Compliance Conundrum

Understanding misconceptions is the first step toward improving mobile security. However, the steady growth of industry compliance requirements makes the task of managing it even more daunting.

Some of these regulations, or parts of them, promote data protection within particular industries. For example, the Gramm-Leach-Bliley Act (GLBA) has privacy stipulations to protect information in the financial services industry. The Healthcare Insurance Portability and Accountability Act (HIPAA) sets standards for health care coverage and transactions, including safe-harbor provisions if data is encrypted to specific standards. Payment Card Industry (PCI) standards govern data used in payment card transactions. The U.S. Federal Trade Commission (FTC) also has information protection rules that apply. Not meeting compliance requirements can mean hefty fines and expensive consequences.

In addition, some states in the U.S.—including Massachusetts and Nevada—will soon require encryption on all mobile devices, including smartphones, if they contain personal information. Further, companies must be able to retrieve data from mobile devices if the information is pertinent to a discovery motion or lawsuit.

New compliance requirements necessitate safeguards such as network monitoring, data tracking, firewall configuration and access control programs—areas where outsourced security services are valuable.

Complying with regulations and identifying vulnerabilities are significant business benefits of using an outsourced mobile security partner. A provider can also help prevent costly incidents that degrade the brand identity of the organization and that have extended costs. For example, the Department of Veterans Affairs incident led to an outcry from the general public and government leaders who questioned the security governance of its mobile workers. This reflected on the integrity of the organization.

In addition, a security breach has costs that extend beyond those directly related to the incident. A recent study by the Ponemon Institute found that the loss of one laptop costs an average of \$49,246. On top of the actual replacement of the notebook, larger expenses include costs associated with investigating the incident, the loss of intellectual property and data and compliance with regulatory requirements related to the breach.

A managed security provider can help protect the organization by establishing a mobile security strategy to prevent such incidents. For example, having a comprehensive inventory of mobile assets and the ability to remotely disable them can prevent consequential damage from theft and intrusion by predators.

A managed security partner also provides metrics for ongoing security maintenance and protection—such as how mobile workers communicate, how often they are online, the Web sites they visit and when and how data is exchanged. This knowledge aids in decision-making and overall security strategy.

Conclusion

Our universal mobile workforce is steadily growing. Likewise, the need to manage the security of the devices and data used by these workers is also increasing. It's important to understand the challenges and misconceptions about security in terms of complacency, cost, experience and do-it-yourself security management.

In addition, a rise in compliance requirements has caused IT managers with limited resources to seek outside help to meet these requirements. Having a mobile security program that incorporates a trusted managed security provider is a best business practice and an essential ingredient in protecting today's enterprises.

For more information, visit www.qwest.com/business.