

# Mobile Computing

By Brian Nickel, CISSP

Remember when cellular telephones were both large in size and price with questionable justification? Such a “luxury” was not commonplace, but something happened along the way that made a cell phone on the belt or purse as common as a watch on the wrist. Besides, the improvements in technology as one impetus for market growth and acceptance, the business and personal justification for such communication capability had to come first. Answers were needed for questions such as, “What can I accomplish with the mobile capability as an alternative to the status quo?” and “Is the price of the capability worth my definition of value?”

While the example above serves to highlight a common “coming of age” for communication while mobile, the purpose of this article is to explore requirements and commonalities of mobile computing environments for business endeavors. Mobile computing has become mainstream. It would be difficult, if not impossible, to discuss the great variety of specific needs and wants of any given entity regarding mobile computing. However, certain commonalities in approach bear out and are worthy of further evaluation. There is also a distinction to be made between wireless computing and mobile computing, although they are usually lumped together. This is discussed below. Hopefully, given salient points drawn from discussion, qualifying questions for assessment of supporting a mobile computing environment can be generated and an appropriate model can be designed to support current and future business requirements.

## The Trend of Workforce Transition to Mobile Computing

The motivation to embrace some form of mobile computing can be found in at least three areas of interest to business. First, the need for real-time remote application system access, which may very well include corporate e-mail, by increasingly mobile workers helps to support efforts for competitive advantage and work completion. Office-bound workers who must venture out to customers or business partners operate on potentially stale data, and must return to the office at some point to perform information gathering or other follow up activities. This delays progress in sales efforts, project work, collaborative research, etc. Further, such delays may open a window of opportunity to competitors armed with mobility and information access to complete actionable tasks while away from the office and/or present with the customer or business partner. The comparative result? Action item completion is delayed, resulting in missed opportunity and productivity or action items are accomplished and next steps are initiated.

The second impetus for mobile computing comes in the form of promoting worker productivity and job satisfaction by acknowledging employee need for work/life balance. Meeting business objectives may

require flexibility and mobility, but so does personal and family life. Corporate policies and support for telecommuting/home office can have many positive and tangible benefits for both the employee and employer.

Lastly, wireless local-area network (WLAN) technology and support can greatly improve productivity and worker collaboration by encouraging work in common areas and freeing the employee to roam from the desk.

As is evident in the areas of interest to business for mobile computing, there is a distinction to be made in regard to terms and subsequent discussion. This is understandable given the differing motivations and support requirements for wireless computing and mobile computing. The Information Systems Audit and Control Association (ISACA) provides a useful reference for wireless and mobile computing. In the ISACA Auditing Guideline, Mobile Computing (Document #060.010.020), the need for a guideline and distinction in computing models is presented. In particular, “Mobile and wireless computing refers to the use of wireless communication technologies to access network-based applications and information from a wide range of mobile devices.”

In further defining the distinction between wireless and mobile computing, the following ISACA definitions are offered. “The term wireless computing refers to the ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11x and other wireless standards and radio band services used by mobile devices. The term mobile computing extends this concept to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. It is comprised of PDAs, cellular phones, laptops and other mobile and mobile-enabled technologies.” In addition to these definitions and distinctions, mobile computing should also be considered in terms of “wired” connections that may originate in almost any location, including home offices, public kiosks, temporary office locations etc. to reach corporate application systems.

In today’s age of ubiquitous communications and computing options, one may think that mature mobile computing environments exist across various lines and size of business. However, some self evaluation and observation of the marketplace will indicate that the spectrum of mobile computing environments is broad. Support for mobile computing ranges from simple dial-up access to legacy remote access servers to highly redundant and sophisticated web-enabled portal environments supporting internet based remote access and employee intranets. Wireless LAN implementations vary widely from hot-spot support to provision of complete coverage. Personal data assistants (PDAs) and PDA-like wireless telephones are growing in popularity.

Where is the middle ground to the extremes? How does an enterprise control access and guarantee a trusted (and patched) client, whose

antivirus, antispymware, etc. are up to date? Based on business requirements, that which is appropriate for one enterprise may be unjustifiable to another. Those considerations aside, there is a certain baseline for support of mobile computing that represents the center point of the pendulum for almost any business. Given that remote access to corporate information resources is a primary motivation for supporting mobile computing, internet based virtual private network (VPN) methods of access are commonplace and are generally affordable since the implementation options scale widely and utilize existing resources, such as a corporate internet access circuit. Further, wireless LAN hot spots in meeting rooms contribute to team collaboration and real-time application and data access relevant to the work at hand.

Before rushing into support for mobile computing, however, some due diligence is necessary for performing requirements analysis and assessment for security and risk management.

## Requirements Analysis and Security/Risk Management of Mobile Computing

It is essential for a business enterprise to perform detail requirements analysis for support of mobile computing. Business process evaluation is necessary in association with relevant application systems, messaging systems, regulatory requirements, network infrastructure, support staff capabilities, information security, and risk management requirements. Answers are needed for questions such as, "Do staff members often travel out of the office and yet require mobile access to corporate systems and data to maintain continuity of workflow?" and "Is data at risk for loss or disclosure in any case, but particularly in a mobile computing model?" There are other considerations as well. Is staff productivity enhanced (or preserved) when wireless LAN support affords on-campus mobility? How many meetings are concluded with data gathering follow-up tasks that could have been accommodated in real-time via wireless LAN access to systems and data? The business process evaluation in respect to mobile computing should result in a matrix illustrating the related application system capability for remote access as well risk management issues. Business processes that tend to be highly automated, auditable, and database centric, even web-enabled, lend themselves to mobile computing. It is not the intent of this article to explore methods of detail requirements analysis, but rather indicate that such is an absolute necessity in the case of mobile computing.

Once business process requirements are identified and some form of mobile computing is deemed worthy of evaluation, some technical assessment is necessary as well.

Common network design requirements for mobile computing include the following. Technical assessments should include these items. This is neither an exhaustive list nor a representation of a detail design analysis, but rather a list of those things which are both desirable and important to the successful support of a mobile computing environment. These items are applicable to remote access/telecommuting as well as WLAN support.

1. Written mobile computing policy and instruction, endorsed by senior management.
2. Written enforcement and audit policy, endorsed by senior management.
3. In-house or contracted service for support of mobile computing environment.
4. Broadband access to the internet at target headquarters location. Remote side is variable.
5. Internet edge perimeter protection and VPN support (IPSec and/or SSL).

6. Authentication, authorization and accounting system support, preferably in conjunction with a directory services environment.
7. Application systems and data storage environment conducive to remote access.
8. LAN design supporting physical and logical segmentation and traffic containment.
9. Content protection systems such as antivirus, spyware eradication, and spam/email gateways. This includes remote client devices (personal firewall, antivirus, etc.).
10. Stability and scalability of the local area and wide area networks.
11. Network management support for availability monitoring and security incident response.

Every organization maintains its own marriage between business process and application systems and data storage. As such, what is common for one entity's processing needs may be irrelevant to another, even within a like industry or line of business. There are, however, common systems which most enterprises support and where remote access is most likely justified. Focus, here, will be placed on remote access and telecommuting.

Common application systems environments which are typically candidates for mobile computing include corporate e-mail, law enforcement inquiry(patrol car), sales/customer management, dispatch/delivery/repair, and telecommuting access to the corporate LAN. Certainly, this list can be easily expanded or contracted. This fact highlights the proliferation of mobile computing device types and capability, application enablement for mobility, and the expansion of the organization's physical and process boundaries.

Mobile computing devices have computing and data storage capability and, as such, represent an area of concern for information security and risk management. Information security and risk management is not limited to IT assets. Perhaps one of the more useful and clear definitions of risk management is contained in the National Institute of Standards and Technology (NIST) document, Risk Management Guide for Information Technology Systems (SP800-30). Specifically, "The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization." Defining risk further, "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level."

What are particular areas of organizational risk in a mobile computing environment? To answer this question, the perspective of an information security and audit function should be utilized. The ISACA Auditing Guideline, Mobile Computing (Document #060.010.020) points out that one should consider the risks associated with the use of mobile computing devices related to the business data stored and processed. This implies concern for the content of the device's storage capability as well as its use for application systems access. Further consideration should be given to backup/restore/recovery functions for support of the continuum of transactional data flow in the mobile computing environment, including physical security of the client device. Admission control is important to regulate the trustworthiness of the client device according to security policy. Specifically, this may include the use of digital certificates, presence and update status of antivirus, personal firewall, software patch levels, and

VPN tunnel permissions (i.e. disallowing split tunneling). Regulatory requirements must be considered from both a policy standpoint as well as within the application systems and network architecture.

In essence, the information security and risk assessment and management policy, implementation, and enforcement process should consider CIA (confidentiality, integrity, and availability) and control the following items at a minimum. These include loss or theft of data. Consider encrypted storage capabilities. Denial of service or compromise of application systems and network infrastructure due to malware. Authentication and authorization of users, application processes, and session control. Nonrepudiation and data integrity support within application systems and network traffic transmission. Accounting and auditing support. Security awareness training and policy enforcement.

With the appreciation of associated risk and the business justification for support of mobile computing, in particular remote access and telecommuting, an introduction to some common deployment models is necessary. Since the VPN model is most common in today's marketplace, with increasing support for browser based application capability on limited capacity computing devices (PDAs), the design options for general VPN usage include:

1. Business-to-business (B2B) or extranet.
2. Site-to-site for organizational branch office connectivity.
3. Remote access and telecommuting connectivity.

The first two design options are well-defined and implemented widely for more static connectivity. Some branch office connectivity is asynchronous, but predictable. Remote access and telecommuting capabilities continue to grow with both the advances in technology as well as the blurring of traditional organizational network boundaries. Within the VPN models for remote access and telecommuting, layers of complexity are added to address the business need. The remote access and telecommuting VPN model will be explored further.

### **Elements of Design/Architecture in Common Models of Mobile Computing**

Based on the outcome of an appropriate requirements analysis for mobile computing, including evaluation of business risk and pertinent legal implications, mobile computing environments could be categorized into groups of basic, more complex, and advanced.

In these cases, both IPSec and SSL based VPN technology could be deployed to meet requirements.

Basic VPN deployment for remote access can be characterized by the following, given consideration for that mentioned above in the discussion of requirements analysis and risk management.

1. Serves business purposes for telecommuting/home office support as an extension of the corporate LAN. This may include remote telephony extensions of the corporate voice systems environment. Voice of Internet Protocol (VoIP) may work well in this scenario.
2. Serves business purposes for mobile worker remote access to applications such as corporate e-mail and office automation/scheduling systems. This may include e-mail "push" integration to handheld devices such as cell phones and PDAs.
3. Network design elements often include a service provider value-added network where both the headquarters end and remote client are supported by the provider with onsite equipment and centralized

administration and helpdesk.

4. Network design elements often include an in-house implementation and support of a headquarters VPN target machine(s) (server/application based or appliance) as well as remote client hardware/software.
5. Network design elements at the headquarters end often place the VPN target system in parallel with an existing firewall, behind the internet edge router supporting the broadband internet access circuit.
6. Network design at the headquarters end may include VPN support in conjunction with firewall support on the same hardware/software platform.
7. Network design at the headquarters end may include VPN support on an existing LAN or extranet server, although this is not recommended.
8. Remote client support may include a variety of hardware and software options depending on the device type, network access, VPN connection method (IPSec or SSL), corporate security policy, traffic content control, etc.

In basic implementations, there is generally not a corporate intranet/portal environment but rather a simplistic internet network edge build-out at the headquarters end. Bear in mind that regardless of technical complexity in support of mobile computing, an organization's acceptable use policy must be adhered to and be enforceable. This brings up a design requirement that must be included in any deployment—auditability. Network management, log analysis, session denial, and incident response must be functions with assigned resources in order to ensure a controlled and managed extended enterprise.

More complex and advanced environments supporting mobile computing generally share design elements, but vary in implementation. Depending on the business processing requirements being supported, it is often a portal-like design being deployed and maintained. What does that mean? Therein lies the complexity. In these situations, the target application systems and database systems are usually architected to support mobile computing and related transaction sets. Such systems may be web-enabled. Standard browser based access to applications may suffice or custom client applications may be employed which work with and for only specific applications and transaction sets. In these scenarios, one often finds both IPSec as well as SSL remote access capabilities, which includes functionality for basic access requirements as delineated above. Certainly, SSL remote access for simple application capability (basic deployment model) will continue to grow in popularity due to simplicity and cost effectiveness. There are potential residual data issues to be dealt with, but these are beyond the scope of this article. That being said, more complex and advanced remote access and application support includes capability for simple telecommuting and remote user support.

Advanced deployment for remote access can be characterized by the following, again given consideration for that mentioned above in the discussion of requirements analysis and risk management

1. Serves business purposes for extension of application system capability to permanent field staff.
2. Serves business purposes for web-enabling application systems for common user interface, whether in-house (campus LAN attached) or as remote client.
3. Serves business purposes for business partner application connectivity (inter-business transaction sets) as well as an application delivery mechanism for asynchronous branch office

connectivity support.

4. Network design elements often include redundant internet access circuits and routing topology (including hardware) at the headquarters end.
5. Network design elements often include tiered firewall and VPN hardware/software platforms, providing both redundancy and segmented security zones (DMZs) for respective network elements and application platforms.
6. Network design elements often include content control in the form of content switching and application traffic interrogation.
7. Network design elements often include intrusion detection/prevention systems and incident response mechanisms.
8. Network management platforms are required and are usually more sophisticated in nature, including the capability to use synthetic transactions for availability and performance monitoring.
9. Client device types range from handheld wireless machines to laptops to custom engineered application specific devices for a given line of business. This class of device type will grow and network access methods will vary.

These design elements are certainly not an exhaustive list, nor are they necessarily included in every deployment. Specific business processing requirements along with cost justifications and other considerations will determine that which gets deployed and managed for mobile computing.

It should be said that sufficient time and energy should be devoted to systems analysis and project work for application system assessment and enablement for mobile computing. How well an application system is architected, including when it was designed and implemented with then current technologies, will in part determine the extent to which it can be extended safely for mobile computing. It is not a trivial effort to extend an otherwise trusted, in-house application to the "outside" world, even when that outside exposure is via a presumed trusted network connection. All of the information systems security and risk management issues highlighted above need to be evaluated. Specific organizational issues, such as the cultural environment, need to be assessed as well. This includes the extent to which an organization values the benefits of modern information technology to meet business processing requirements.


What seems to be a "slam-dunk" positive decision in support of mobile computing actually materializes into a required evaluation of business process, corporate culture, security policy/posture, technology deployment, and application systems support. While, in some cases, the implementation of a mobile computing environment may be relatively simple and justifiable, the information security and risk management requirements must be taken as seriously as if a complex solution were pursued. Further, the implementation or expansion of a mobile computing environment includes immediate and potential cost. Immediate cost includes that related to analysis and implementation. Potential cost includes that related to ongoing support and upgrade requirements and that related to risk (including residual risk). This cost analysis must be considered in the context of business goals and objectives, as well as the resulting information technology management plan that supports the business and its ability to remain an ongoing concern.

Finally, some hard questions need defensible answers regarding mobile computing. These may include:

1. What business process and/or competitive position is enhanced by

mobile computing?

2. What is the organization's information security, risk management, and regulatory position as a whole, and as related to mobile computing?
3. What is the capability of relevant applications systems for support of mobile computing? What are the implications and costs associated with upgrade or conversion to that which supports mobile computing?
4. What is the condition of the corporate network and internet access design relative to mobile computing?
5. Does the organization maintain a data classification scheme to categorize data source/ownership, sensitivity, useful life, etc.?
6. Does the organization have the resources, including staff, to support a mobile computing environment?

Hopefully, the discussion presented in this article will provoke some thought and research into mobile computing capabilities and how your organization would benefit as a result. 

---

*Brian Nickel, CISSP, is a network design engineer and has over 20 years of varied IT experience in the healthcare and telecommunications industries.*

<sup>1</sup> Reprinted with permission. IS Auditing Guidelines 060.010.020 Mobile Computing and 060.020.120 Review of Virtual Private Networks. Copyright 2004, Information Systems Audit and Control Association® (ISACA®), Rolling Meadows, IL, 60008, USA.

<sup>2</sup> United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, Risk Management Guide for Information Technology Systems.