Leveraging Mobile & Remote Computing Technology

Options and considerations for optimizing the use of technology for your business model.

DECISION-MAKERS’ GUIDE
# TABLE OF CONTENTS

1. Introduction ........................................................................................................................................ 3  
   Objectives of this Discussion Paper ................................................................................................. 3

2. Mobile and Remote Computing Options ......................................................................................... 5 
   Network Infrastructure ........................................................................................................................ 5 
   Internally Hosted Server-Based Solutions ....................................................................................... 5 
   Remote Control Solutions ................................................................................................................ 6 
   Web-Based Applications or Software as a Service ........................................................................... 8 
   “Cloud” Storage .................................................................................................................................. 9  
   Mobile & Remote Devices ................................................................................................................ 11 
   Laptop Computers .............................................................................................................................. 11 
   Smartphones ....................................................................................................................................... 12 
   Tablets ................................................................................................................................................ 14 
   Future Devices ...................................................................................................................................... 14 
   Mobile & Remote Computing Peripherals ......................................................................................... 15 
   Portable USB Storage Devices .......................................................................................................... 15 
   Printers .............................................................................................................................................. 17 
   Scanners ........................................................................................................................................... 17 
   Software ............................................................................................................................................ 17 
   Secured Access Solutions .................................................................................................................. 17 
   Collaboration Tools .......................................................................................................................... 19 
   Communication Applications ............................................................................................................ 19 
   Social Networks ............................................................................................................................... 21 
   Policies and Security Considerations ............................................................................................... 23 
   Physical Loss ...................................................................................................................................... 23 
   Unsecured Access .............................................................................................................................. 25 
   Unsafe User Behavior ......................................................................................................................... 26

3. Mobile & Remote Computing Solutions ......................................................................................... 27 
   Employee Connectivity ...................................................................................................................... 27 
   Client Self-Service ............................................................................................................................ 29

4. Disaster Recovery & Business Continuity ....................................................................................... 32

5. Conclusion ......................................................................................................................................... 33 
   Acknowledgement ............................................................................................................................ 34
Introduction

Mobile computing, collaboration tools, remote access technologies, and communication devices have fundamentally changed the business landscape. Employees are increasingly expected to be able to access e-mail, customer and client databases, and most other critical systems through secure Internet-based connections, using portals to store and share information and virtual private networks for sensitive data. Mobile and remote computing technologies can be leveraged to achieve numerous competitive advantages in areas such as recruitment, retention, customer service, and return on investment. The list of potential benefits that can be achieved is impressive, and includes the following:

- Elimination of geographic restrictions
- On-demand access to information and systems
- Enhanced and more timely communication
- Improved customer service and reduction in customer/client response time
- Changes in customer engagement through social media
- New remote service and sales options
- Gains in worker productivity
- Reduced business start-up time and costs
- Reduced “brick and mortar” dependency and/or cost
- Changes in methods for worker collaboration
- New global workforce options
- New employment structures
- Increased worker flexibility
- Increased ability to attract and retain quality employees

Objectives of this Discussion Paper

The specific technologies that enable and support mobile and remote computing are varied, but they include mobile end-user devices such as laptops, tablet PCs, PDAs, and smartphones; wireless technologies such as Bluetooth, Wi-Fi, and WiMax; and re-
mote access technologies such as Windows Terminal Services and Citrix Presentation Server. This discussion provides an overview of widely used mobile and remote computing options, presents the costs and benefits of the different options, highlights key risks, promotes best practices, and includes links to valuable resources.

Choosing the right mobile and remote computing options for your business involves a series of critical decisions regarding infrastructure, security, software, device deployment, document management, and much more. Instead of allowing the technology to drive the process, organizations should determine their business objectives, review their existing IT infrastructure, and determine which mobile and remote computing technologies would be most appropriate given their stated objectives, business needs, available resources, and budget.

Once an organization has determined the objectives for their mobile and remote computing (MRC) capabilities, and evaluated its existing environment and available resources, the considerations become more tactical. To select and implement an effective mobile and remote computing solution, management must make a number of decisions related to two general categories:

- Network infrastructure, including software, hardware, and end-user devices
- IT policy and security

While decisions related to the selection of the remote access solution, supporting devices, and software are important, the development, implementation, and enforcement of comprehensive IT policies to support these technologies are equally important. Technology, in and of itself, is of little value without an overarching operating model that defines how the system will be monitored and used so as to minimize risk, maximize productivity gains, and prevent misuse or abuse.

“Technology, in and of itself, is of little value without an overarching operating model that defines how the system will be monitored and used so as to minimize risk, maximize productivity gains, and prevent misuse or abuse.”
Network Infrastructure

Network infrastructure is key to implementing an effective mobile and remote computing environment. Many technologies are required to make mobile and remote computing happen, including software, hardware, and end-user devices. The precise configuration you choose depends on the remote desktop solution chosen. Available options fall into one of four general categories: internally hosted server-based solutions, remote control solutions and Web-based applications, software as a service (SaaS), and cloud storage.

Internally Hosted Server-Based Solutions

Server-based solutions involve server-client relationships and software configurations that support the deployment of critical business applications remotely over the Internet and/or an internal network. In the server-client model, applications reside on and are run off a server as opposed to the user’s personal computer or computer device. In this arrangement, the server provides all the computing power necessary to run the application, while the client or local computer device provides an interface for interacting with the network-hosted application. Users only need client software installed on their local desktop or laptop computer. The internally hosted server-client solution is the most popular enterprise-level solution, and XenApp or Remote Desktop Services are two notable products.

The advantage of internally hosted server-client solutions is that they allow users to run applications without having them installed on their desktop or laptop. Clients can be configured to run all available applications or just a few. It is common practice for businesses to deploy Microsoft Office applications and other productivity software to run locally, so end users remain productive even in instances where connectivity is limited or unavailable. Adoption of an internally hosted server-client solution can also lead to a reduction in IT support cost associated with the deployment of software updates and upgrades because deployment is centralized and automatically pushed to
users, eliminating the need for IT to manually update each user’s computer.

On the downside, the software licensing, server hardware and maintenance and support can be expensive for internally hosted server-client solutions. While centralization should help offset some of these costs over time through reduced user support costs (less support needed for staff in the field) and potentially lower end-user computing costs (users don’t require the most powerful computers), the internally hosted server-client model is the most expensive, requiring substantial investment on the front end. Another disadvantage of this approach is that network-enabled computers and devices become gateways to the organization’s network resources that, if lost or stolen, could be used by unauthorized parties to gain access. Also, as with any remote desktop solution, internally hosted server-client configurations require users to have an Internet connection to run applications remotely.

Remote Control Solutions

GoToMyPC and LogMeIn are examples of remote control solutions in which a direct connection is established between a locally networked PC and a remote device that allows users remote access to the applications, files, and network connections available on the locally networked computer. In the most common environment, a user will have GoToMyPC, LogMeIn, or another remote control solution installed on his or her primary work computer, providing them access to that computer from another remote computer via the remote computer’s Web browser. The remote user will see the primary desktop or laptop computer screen as if they were physically sitting in front of it.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to applications without having them installed on your desktop or laptop</td>
<td>Internet connection required for applications to run remotely</td>
</tr>
<tr>
<td>Reduced IT support costs associated with software upgrades and updates</td>
<td>Increased costs associated with software licensing and server hardware and maintenance</td>
</tr>
<tr>
<td></td>
<td>Increased security risk</td>
</tr>
</tbody>
</table>

Pros

- Access to applications without having them installed on your desktop or laptop
- Reduced IT support costs associated with software upgrades and updates

Cons

- Internet connection required for applications to run remotely
- Increased costs associated with software licensing and server hardware and maintenance
- Increased security risk
of it and are able to access and use any of the primary computer’s applications, data, and connections. In remote control situations, users gain access to internal network resources through the existing connections on the primary desktop, which serves as an intermediary between the network and the remote device. They may also access applications and files stored locally on the primary device because the remote computer or device provides an interface for interacting with the primary device.

The advantage of a remote control solution is that it is relatively inexpensive to set up and maintain. In many cases, it can be configured in less than an hour. It also does not require additional investment in server hardware. Because remote control solutions require less upfront investment and are easy to deploy and configure, they are a great mobile and remote computing option for smaller organizations with limited IT budgets and existing network infrastructure.

One disadvantage is that remote control desktop solutions require users to have two separate devices: a primary one that is directly connected to the network, and a remote device configured to control the primary one. In this scenario, organizations may be responsible for purchasing and supporting both the primary and remote computers, paying more for end-user devices – laptops and desktops – than they would in an internally hosted server-client solution. One way around this is to make a remote control solution available to users, but make the user responsible for purchasing the remote device. This makes it difficult, however, to enforce IT policies and ensure that the employee-owned remote devices conform to established security configurations that prevent unauthorized access to the remote computer. Accordingly, organizations opting for this arrangement may decide in favor of a more restrictive remote control configuration that prevents users from saving or printing network files or data locally on the remote device.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inexpensive to set up and maintain</td>
<td>Users must have two separate devices</td>
</tr>
<tr>
<td>Can be configured in less than an hour</td>
<td>Responsible for purchasing and maintaining both the primary and remote computers</td>
</tr>
<tr>
<td>No additional investment in server hardware</td>
<td>Difficult to enforce IT policies</td>
</tr>
</tbody>
</table>

---

**Pros**
- Inexpensive to set up and maintain
- Can be configured in less than an hour
- No additional investment in server hardware

**Cons**
- Users must have two separate devices
- Responsible for purchasing and maintaining both the primary and remote computers
- Difficult to enforce IT policies
Organizations should also ensure that their remote control solution is configured so that the primary computer’s keyboard is locked and that its monitor is blacked out when it is being accessed remotely. This will help prevent unauthorized access and disclosure of sensitive information within the office while the user is accessing the device remotely.

**Web-Based Applications or Software as a Service**

Another mobile and remote computing option involves the use of Web-based software services where applications are hosted by a service provider on its server, deployed over the Internet, and accessed through the user’s Web browser. This arrangement is commonly referred to as software as a service (SaaS). In the SaaS model, applications are supported by third-party vendors who lease their applications to end users, and run them remotely over the Internet through secure connections. This kind of third-party hosting generally involves specific business applications that are generally server-deployed applications such as audit, tax, and general ledger software that are not typically installed and run on the end user’s device. As the world heads toward a more centralized, Web-based computer environment, businesses are starting to move away from local deployments of common desktop software like Microsoft Office in favor of Web-based deployments of these applications. In a sign of the times, Google has offered for some time free (for individuals) Web-based word-processor and spreadsheet applications complete with online document storage. These applications permit multiple users to edit a document simultaneously without installing additional software.

The advantage of using third-party SaaS applications as opposed to internally hosted applications or software configured to run locally on the end-user device, is that SaaS products are extremely easy to deploy and usually require no hardware or support. As a result, they can be significantly less expensive. SaaS can also be implemented more quickly than internally hosted software, and organizations benefit from only having to purchase as much software as they need. They can always purchase additional licenses on an as-needed basis as the organization grows without the worry that subsequent releases will necessitate expensive hardware upgrades. Cost advantages are deepened by the fact that end-user computer costs can be kept low because the third-party’s server performs the bulk of the heavy-duty processing and user devic-
es needn’t be as powerful as when applications are hosted and run locally. Another significant advantage of SaaS is that it allows for much more accurate forecasting of IT overhead, because the software service is run on the provider’s network for a set fee, and the provider is responsible for its support, maintenance, and optimization.

A disadvantage of SaaS is that the applications tend to be less customizable due to the fact that generic configurations make it easier for providers to push updates to their clients more efficiently and help keep their cost low. Control over security and data backup is also a concern. Accordingly, organizations should perform due diligence before purchasing a service contract to ensure that the provider’s security and backup practices meet or exceed internal standards.

“Cloud” Storage

“Cloud” storage offers new opportunities to store information on servers that are widely and easily available from any Internet-enabled device, enabling a revolution in computing for many organizations. This method is a stark contrast to computing of the past, which required applications and data to be loaded manually on each device using them. After Internet users discovered that all they need in many cases is a Web browser to access information on servers, they began questioning the need to own the servers. Many firms wanted to focus on investing in core competencies in their own fields and markets, and did not want to develop expertise in storage and security practices. Many third-party firms offer virtual servers that mimic dedicated computers, requiring only Internet access on a device to access the applications and data. Amazon’s Web Services (S3), Google’s Cloud Platform, and Microsoft’s Azure options are major players in that market. Small firms can develop websites using free services such as Wordpress.com and Facebook (described below). Data and sophisticated applications are all provided by the outside parties in the cloud.

While many firms have serious concerns about storing confidential information in the cloud, one could argue that firms that specialize in cloud storage would actually provide an increase, rather than a decrease, in security because their professional survival depends on it.
the cloud, one could argue that firms that specialize in cloud storage would actually provide an increase, rather than a decrease, in security because their professional survival depends on it. Standards from regulating bodies such as Health Insurance Portability and Accountability Act (HIPAA) and have embraced cloud storage, but require reasonable precautions such as strong encryption. The Committee of Sponsoring Organizations of the Treadway Committee has published a thought leadership paper, *Enterprise Risk Management for Cloud Computing* that provides an overview of the various types of cloud computing models and their associated opportunities and risks that are an important part of any decision to store confidential client information.

SaaS, described above, is one way to make use of cloud computing beyond storage. In fact, as described in a video by Integrant, SaaS is the highest level of cloud computing, where everything is managed by the cloud vendor. Examples of items managed are networks, storage, servers, operating system, data, and applications. Two other cloud computing options are platform as a service (PaaS) and infrastructure as a service (IaaS), described next.

**Platform as a Service (PaaS)**

PaaS is a more modest form of cloud computing, where the vendor manages fewer of the resources. This approach is more commonly used by developers. Management of applications and data are taken over by the client, and the vendor takes care of everything else listed above (networks, storage, servers, and operating system). You could, for instance, request a Windows Server with a specific level of memory and features available (like a database package for managing inventories or customer files).

When the development project is complete, you can “go live” and use it for customer transactions, or contact the vendor and release some or all of those resources. Your platform is only available in a specific size while you are paying for it.

**Infrastructure as a Service (IaaS)**

IaaS is an even more modest form of cloud computing, where the vendor only provides computing hardware resources. As described above, Amazon, Google, and Microsoft provide such services. The vendor presents a place you can install an operating system along with the database and other tools, and you manage data and applications. IaaS works well in situations in which everything has been tested and fine-tuned.
on one server, and information systems personnel can replicate it on other hardware, but they do not wish to purchase the hardware because demand goes up dramatically during particular times of the business cycle. For instance, firms offering Web-based tax preparation software would scale up dramatically between January and April. It would be wasteful to have hardware sitting dormant during the rest of the year when they might only need 5 percent of the capacity of the busy season. Therefore, they release those resources and their bill diminishes greatly. The vendor then is free to rent those capabilities to other firms that have busy season in the summer, such as vacation sales agents or HVAC manufacturers. Then in the fall, retailers can make use of those resources during the holiday sales season.

Stated more simply, IaaS enables information systems managers to create new servers or dismantle them on the fly without buying, selling, handling, or even seeing the equipment.

Mobile & Remote Devices

Being connected to the office at all times has become not only the norm but increasingly the expectation. Compact end-user devices are a substantial driving force behind the mobile and remote computing trend. It began with laptops in the 1990s, accelerated with the introduction of Blackberries in 1999, and was soon followed by smartphones then tablets. Assisting in this revolution has been a large library of “apps” (smartphone applications) as well as abundant connections via Wi-Fi and 4G LTE. Fast data connections have arisen at work and home, as well as many locations in between. Taken together, these technologies allow users to squeeze productive work into even the smallest amount of downtime. As a result, users can be plugged into their organization’s resources, applications, and data as if they were in the office, regardless of where they are physically.

Laptop Computers

Laptop computers fueled the initial push towards mobile and remote computing. Their widespread availability made it possible for users to bring critical applications and data with them anywhere, either through productivity software installed and run locally or via remote interaction with SaaS or applications hosted internally. Laptop computers make mobile and remote computing practical because they can be used as a mobile or remote worker’s
primary device, regardless of whether or not they are in the office. Laptops should be selected based on the needs of the end user. Those whose job functions require them to do a lot of typing benefit from laptops because of their built-in keyboards. Newer, thin, and lightweight models with solid-state drives (SSD) rather than spinning hard drives (HD) have recently become the desired choice for highly mobile workers. Although they often have slightly slower processors, tiny “sub-notebook” and “netbook” computers with smaller screens, keyboards, and prices, are excellent choices for those who wish to avoid stress on their shoulders, necks, and bank accounts. As more data can be found in the cloud, HD or SSD storage needs have been reduced substantially. Organizations can choose options such as drive encryption, laptop loss management software, and biometric capabilities such as built-in fingerprint scanners to provide additional layers of security. Laptops also provide unsung benefits such as battery power in case of a power outage, supporting continuity planning at the office.

Many companies began issuing standard laptops to enable staff members to familiarize themselves with the devices, enabling them to quickly set up, fix, or replace devices when a problem occurs, reducing support costs as well as user downtime. Standardized laptop options also allow organizations to order in bulk and realize substantial cost savings. After the price of laptops came down substantially, they became fixtures for managers and executives, and sales of laptop computers surpassed desktops in 2008. As operating systems improved Wi-Fi connections via simpler setup, greater reliability, and faster speed, some firms have relaxed their rules about supporting various models.

Smartphones

The development, availability, and affordability of ultra-mobile, hand-held Blackberries kicked off an avalanche of smartphones that buried PDAs (such as Palm Pilots,) that preceded them. Releases from other manufacturers became stiff competition for Blackberry, which has since seen single-digit market shares, below Google’s Android, Apple’s iPhone, and Microsoft’s Windows Phone 8/10, in descending order of market size. Apple’s iPhone popularized smartphones and enjoys a loyal, passionate following and the largest library of applications. Google’s Android software is provided on an open-source basis, and applications are not as carefully vetted for safety or functionality, unlike those available for the iPhone. At the
same time, opportunities for larger or multiple screens, more extensive multitasking, more battery options, storage expandability, exclusive Google applications, and application “widgets” have attracted millions to the Android platform. Lenovo’s purchase of Motorola’s smartphone operations makes for a formidable opponent, while Apple continues to sell millions of new iPhone models within days of each release. Microsoft’s late entry into the smartphone market has found limited success to date, but the unified “tiled” interface among all devices and free cloud storage appear to be elements of an investment in future devices.

No matter what the platform, users can truly stay connected anytime, anywhere. These devices feature persistent connectivity via cellular broadband services such as 4G LTE, and offer remote users real-time access to e-mail, calendars, address books, tasks, notes and the Internet. Cell phones can also be used to view (and even edit) Microsoft Office documents as well as view PDFs and other files. The devices can run a number of useful applications, including free Voice over IP (VoIP) and navigation software, which can be used to find directions and view maps. Handheld devices are intuitively designed for viewing text, and may be the only device necessary for those whose primary concern is being able to send and receive e-mail. Typing presents some challenges on these small devices, and options such as slide-out physical keyboards, Swype for virtual keyboards, Bluetooth keyboards, and voice recognition are used by millions of users on the road. For those who need the more robust computing that a laptop provides, some handheld devices can double as broadband modems that provide persistent Internet connectivity through LTE networks.

While these devices provide productivity benefits, they also pose new risks to organizations and their clients. The creation of a mobile device security policy and procedures manual can outline the practices necessary to protect company and client information housed on mobile devices. Enforcing minimal security settings, such as password protection, remote wiping of data, and idle timeout can mitigate the risk of losing sensitive data.
losing sensitive data.

**Tablets**

Tablet computers were introduced as far back as 1993 with the Apple Newton. A tablet version of Windows also was released more than a decade ago, in 2002. The Newton did not catch on, and the Windows convertible tablet/notebook took some time to grow as well.

In fact, the market for tablets was miniscule until Apple’s iPad, released in 2010, made use of natural gestures and popularized this platform. Though an Archos Android tablet appeared in 2009, Apple’s iPad made immediate use of apps in its App Store, providing a substantial and vetted set of capabilities. As with iPhones, the experience is tightly controlled and highly reliable. The overwhelming majority of tablets are made by Apple.

Bridging between tablets and notebooks are several offerings by a variety of manufacturers that have detaching or folding keyboards. Indeed, an iPad with a keyboard or a Surface can be easily mistaken for a traditional laptop computer. Because data entry with a virtual keyboard is rather limited, many analysts consider tablets as consumption rather than composition devices. However, the advent of full-touch Bluetooth keyboards built into device cases has provided some composition advances, as has dictation.

**Future Devices**

Wearable devices and bendable screens are on the horizon. Google Glass, for example, provided a pair of glasses that allowed data to be superimposed over images seen by the eyes, often called “augmented reality.” In its trial period, select users found it easy to record video without holding an obvious device up to the eye, give voice commands to check e-mail, or browse the Web. Privacy concerns have been expressed by many analysts, as coupling the unique physical features of human faces with large databases could jeopardize our anonymity as we move from place to place.

Samsung’s “Youm” project provides flexible displays that can be bent, rolled, or even folded, allowing for large screen options to be provided with small devices such as smartphones. They also allow screens to “wrap” around to the side of the device, such as the “Galaxy 6 Edge” that became available in 2015.
The sizes of flexible screens are moving upward. On Jan. 5, 2016, LG announced thin televisions that were demonstrated at the 2016 Consumer Electronics Show in Las Vegas, that bend and even roll up. They will become larger and gain higher resolution over time. A prototype LG 55-inch, 1 millimeter thick “wallpaper” screen was shown in May 2015, but production has not yet begun.

Mobile & Remote Computing Peripherals

When it comes time to outfit the mobile and remote workforce with additional devices, tools, and add-ons to help make them more productive in the field, there are many options to consider. Three categories of peripherals that warrant attention are portable USB storage devices, printers, and scanners.

Portable USB Storage Devices

Portable storage devices such as USB “flash” or “thumb” drives, external hard drives, and even portable media players like the iPod—provide a convenient way for mobile and remote workers to store their data and easily transfer digital documents from one device to another. USB drives are highly portable with hefty storage capacities. Thumb drives that store 1 TB and above are available from some suppliers for less than $50. As a novelty, thumb drives have been built into items such as keychains, pens, and business cards. Their compact nature, coupled with the fact that they can be used with any computer or tablet that possesses a USB port, makes them an essential accessory for the mobile and remote worker.

In addition to their common usage as portable repositories of digital data, USB drives may also be used to store and deploy portable applications so that users can access their own applications on any computer with a USB port. So far, the most common type of applications deployed in this manner are e-mail clients and Web browsers, but portable versions of office productivity software applications also exist. The advantage of USB drives and USB-deployed applications is that they enable users to access their applications without having to carry their laptops around. Also, because applications are run from the removable USB drive, it is less likely that users will leave sensitive information on the hard drive of any foreign devices they might use as they might with remote access solutions.

Convenience notwithstanding, there are a number of security concerns associated with portable USB devices. Because they are so compact and so portable, they tend to
be easily misplaced, stolen, or left behind. This makes encryption of USB storage devices absolutely essential, especially when such devices contain sensitive information. There are a number of quality encryption products on the market that can be used to create encrypted directories on digital storage media, including USB drives, optical hard drives, and CD- or DVD-ROMs.

Another security issue related to portable USB storage devices has to do with the fact that they are frequently used on computers that do not fall under the organization’s security perimeter. When a USB storage device is plugged into a computer it becomes vulnerable to viruses and other malicious software or code that might be lurking on that device. For this reason, users should be selective about the computers with which they use their USB devices. At a minimum, users should check to make sure that the computers with which they use their portable storage devices have active and up-to-date anti-virus software. It is best to avoid public computer kiosks altogether.

It might be surprising that even USB devices such as printers, keyboards, and scanners can present security risks via a so-called “BADUSB,” which permits an outsider to install a virus or install a key logger that reveals all keys pressed by the user (including passwords). These devices, however, cannot be abandoned because of the obvious and strong positives associated with them, described next.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to transfer files from one device to another</td>
<td>Easily misplaced or stolen</td>
</tr>
<tr>
<td>Compatible with any computer or tablet that has a USB port</td>
<td>Frequently used on computers that do not fall under the organization’s security perimeter</td>
</tr>
<tr>
<td>Low cost, high storage capacity</td>
<td>Vulnerable to viruses and other malicious software</td>
</tr>
<tr>
<td>Compact and portable</td>
<td></td>
</tr>
<tr>
<td>Reduced likelihood that workers will sensitive information on a hard drive</td>
<td></td>
</tr>
</tbody>
</table>
Printers

The need for (safe) printers should be considered when outfitting mobile and remote users. However, this market has declined in recent years with the advent of PDF files, hotel business centers, and user-friendly photocopying/printing shops. If the printed matter is not needed immediately in hand, many printer models allow printing from anywhere in the world just by sending an e-mail to the device.

Scanners

Scanners allow mobile and remote computing users to digitally capture, file, and store paper-based information digitally. Mobile workers often generate their own PDF documents directly from Microsoft Office (versions from 2010 to the present), and the need for scanners on site has diminished greatly. Some auditors might need to convert paper documents into electronic files, and might opt to bring along their own portable scanners. Two work-arounds for remote users who need to digitally capture paper documents, but lack access to a scanner, include faxing documents to their fax client software and then to save the resulting image file to their laptop as appropriate, and photographing the documents using a reasonably good quality smartphone or tablet camera. These methods effectively turn available hardware into makeshift scanners.

Software

In addition to the remote desktop solutions noted above, there are additional software technologies that facilitate an effective and secure mobile and remote computing environment. These include secured access solutions, communication applications, and collaboration tools that allow users to share information and communicate both efficiently and securely.

Secured Access Solutions

There is no refuting that mobile and remote computing involves increased security risks. The extension of security end points beyond the protection of an organization’s internal security perimeter makes it easier for security gaps to develop. There are, however, a number of software solutions that can be implemented to shore up mobile security end points, enabling organizations to boost employee productivity while reducing the organization’s risk exposure to an acceptable level. Virtual Private Network (VPN) and Secure Socket Layer (SSL) or Transport Layer Security (TLS) technologies
represent popular and effective methods to keep remote connections and communication secure.

VPNs are a class of software technologies that create an encrypted Internet connection between a remote device and an organization’s private network, enabling remote users to securely access internal network resources residing within an organization’s firewall. In effect, VPNs establish a closed communications network tunneled through a larger network, such as the Internet. This ensures that remote workers have access to everything that would be available to them within the company’s walls, including internally hosted applications and data, intranets, e-mail, and printers, while preventing unauthorized users from tapping into the connection to intercept transmitted information or gain access to the network. All organizations enabling remote connection to internally hosted network resources via the Internet should employ VPN technology.

TLS and its predecessor SSL are Web security protocols that employ encryption to provide secure client-server communication over the Internet for things such as Web browsing, e-mail, Internet faxing, and instant messaging. Their use significantly reduces the likelihood of eavesdropping, tampering, and message forgery. Organizations establish SSL or TLS encryption on websites where secure data is transmitted. Websites employing the SSL or TLS protocols are noticeably different from other websites in that their Web addresses begin with “https” rather than “http.” Most Internet users will recognize SSL or TLS on websites that handle credit card transactions, but the technology can be extended to accommodate the communication of any sensitive data over the web. The cost of deploying VPN and SSL or TLS technologies vary, depending on the size of the organization, the number of remote users, and the number of applications the organization wishes to secure. The Internet Engineering Task Force (IETF) identifies SSL as the standard for transmitting data.

File Transfer Protocol (FTP) is another option for secure transmission of sensitive information by remote workers via the Internet. FTP is an open standard that allows documents to be securely transferred between two computers, an FTP server and an FTP client, via a network such as the Internet. Remote users use the FTP client (included within most web browsers) to download and upload files to the FTP server. FTP implementations should employ SSL or TLS technology, but are otherwise relatively easy and inexpensive to implement. They may be supported internally or purchased...
and hosted as a subscription from a third-party provider.

**Collaboration Tools**

While FTP sites store files and support secure transfer of relatively large files over the Internet, collaboration tools such as intranets, wikis, and portals (including Microsoft Sharepoint) make it easier to structure and share information, substantially reducing the amount of time users spend searching for files, documents, or other information. Intranets employ basic website technology and enhanced security to create online environments where internal users can share sensitive information across the organization. An intranet is essentially a miniature version of the Internet, but it is closed to facilitate the exchange of information among a community of internal users. Information, documents, and files are posted to sites within the intranet that can be accessed by other intranet users via their web browsers.

Portals such as Microsoft’s SharePoint technologies offer out-of-the-box intranet frameworks that can be implemented quickly to deliver additional functionality that enhances collaboration among intranet users. Portal users are not only able to access and retrieve information, but they can also add, remove, and edit content on pages.

**Communication Applications**

Communication is key in any work environment, especially in mobile and remote environments where team members are often in disparate locations and unable to engage in face-to-face interaction. For a mobile or remote environment to be effective, workers need to be able to interact with their co-workers with the same ease and frequency as if they were physically together in the office. There are a number of technology solutions available that can help facilitate this level of communication between remote workers and others within the organization.

Webmail secured with SSL or TLS technology ensures that all remote users have reliable, secure access to e-mail, even if their device lacks a formally configured connection. Because webmail is hosted on the Web, users are able to access their e-mail from any computer with an Internet connection and a Web browser. Larger organizations tend to use VPNs to facilitate access to an internally hosted e-mail server, so for them webmail is a secondary access option for e-mail. However, there are a number of organizations – usually smaller in scale who rely on webmail as their only option for remote e-mail access. The advantage of webmail is that it can help reduce technology
overhead by outsourcing end-user support and e-mail server maintenance.

Instant messaging (IM) is another valuable communication software tool. Once thought of as a fluff technology for tech-savvy Gen Xers and millennials, and a mainstay of AOL Inc. (AOL), IM has matured into a viable business application, enjoying widespread adoption across organizations of all sizes. Today’s IM world has many options for users. Androids, iPhones, and Window phones have built-in SMS (short message system) applications, and many other widely used third-party applications, such as Facebook Messenger and Skype, are also available. Users also obtain free applications that can go well beyond text messages, such as the popular trio WeChat, WhatsApp, and Snapchat. The beauty of IM is that it lets employees communicate back and forth as quickly as if they were having a real-time conversation, providing an easy way to ask a quick question and get a quick response without the need to pick up the phone or type an e-mail. IM also allows individuals to communicate when a vocal conversation may not be appropriate, such as during teleconferences or virtual presentations.

As with e-mail, IM should be hosted inside an organization’s firewall or purchased as a subscription from a secure third-party vendor who uses SSL or TLS encryption. IM is similarly bound by rules and regulations governing document retention, such as the Federal Rules of Civil Procedure, so organizations will need to establish and enforce formal IM retention policies and clearly understand those of their third-party provider.

Voice over Internet Protocol (VoIP) represents another critical software service that organizations implementing mobile and remote computing initiatives might want to consider. VoIP allows users located anywhere in the world to send and receive phone calls from their mobile workstation or hand held device as if they were in the office. VoIP is significantly cheaper than traditional telephone service. There are still some noticeable differences in quality between traditional phone service and VoIP, which may be exacerbated by bandwidth problems, reduced transmission speed, and heavy traffic. As time passes and technology progresses, however, this quality difference

"The beauty of IM is that it lets employees communicate back and forth as quickly as if they were having a real-time conversation, providing an easy way to ask a quick question and get a quick response without the need to pick up the phone or type an e-mail."
should become less of an issue.

One exciting development in the area of communication software is the emergence of unified communication solutions that enable users to send and receive voice, fax, e-mail, instant messages, images, video, and VoIP. With many you can launch Web conferencing from a single interface by phone, PC, or Internet-enabled device. Unified communication solutions consolidate all of a user’s digital communications on one convenient dashboard.

Social Networks

Perhaps no computing application has had as rapid a rise as social networks, particularly three highly publicized networks: Facebook, Twitter, and Instagram. According to Statista, in November 2015 Facebook’s active user base reached 1.55 billion, representing about 20 percent of the world’s population. The same source reports that Twitter had 316 million active users at the same time, which trailed Instagram’s 400 million active users. Facebook’s appeal is the colorful graphics and lively “news feed” that shows postings in real time; Twitter’s appeal is in simple postings with on-the-fly, user-defined searchable key words and phrases (called hash tags). Instagram’s appeal stems partly from a clean user interface and partly from the abundance of smartphones with reasonable quality cameras.

One photo-centered social network, Snapchat, provides no archive of the photos.

Leading Social Networks Worldwide as of April 2016, ranked by number of active users (in millions)

<table>
<thead>
<tr>
<th>Social Network</th>
<th>Active Users (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>1,590</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>1,000</td>
</tr>
<tr>
<td>Facebook Messenger</td>
<td>900</td>
</tr>
<tr>
<td>Tumblr</td>
<td>555</td>
</tr>
<tr>
<td>Instagram</td>
<td>400</td>
</tr>
<tr>
<td>Twitter</td>
<td>320</td>
</tr>
</tbody>
</table>

Source: Statista
In fact, each photo disappears 10 seconds after the user clicks to view it.

There are three significant implications of social networks for organizations. First, firms must make decisions about how to represent themselves on such networks. Many firms represent themselves by opening Facebook pages and starting Twitter and Instagram feeds. Some firms use Facebook as their home page, finding it easier than learning complex Web development tools to provide updates, coupons, and photos. One benefit is to appear “trendy,” and another is to spawn “followers” who receive updates in a news feed. “Tweets” on Twitter keep users in touch with your activities as well, and software can search through the keyword hash tags to provide real-time data and sophisticated historical analysis. Some software is available to turn Twitter posts into Facebook postings automatically, serving both functions. Other software analyzes user sentiment, tracking Facebook “likes” and Twitter “retweets.”

Second, firms must monitor discussions online and decide how to handle misinformation or damaging information that might appear. When firms interact with the public, they need to be aware of postings and tweets that can be made about them by users who are either happy or angry. Firms need to protect their operations by acting on negative information, either by correcting problems that are real, or by removing or correcting misinformation that might be found. A firm cannot act on the information without monitoring what is being said on social networks.

Third, firms must monitor users. The wide availability of portable devices and the appeal of social networks has spawned a new malady that researchers call “Facebook Addiction”. Firms that block such networks from their employees during working hours need to understand that there is little control over such access by mobile and remote workers. Policies that never before were needed must be formulated to accomplish reasonable parameters in this rapidly evolving area.

Finally, with Snapchat, organizations should be concerned about abuses and self-destructive posts. Will users send corporate secrets to others? Will employees send embarrassing or obscene photos? If someone takes a screen shot or photograph of those limited-life posts with another camera, then the content no longer will completely self-destruct, and employees could subject the firm to some risk. Policies and security considerations are discussed in the next section.
Policies and Security Considerations

With all of the compelling benefits associated with mobile and remote computing, it is easy to view it purely as a win-win situation. In reality, the deployment of mobile devices and the facilitation of remote access exposes an organization to a much greater degree of risk than traditional non-mobile, non-remote IT environment. Because security end points in the mobile and remote computing environment extend beyond the safety of the hardwired network and its firewall, there is greater opportunity for security breaches to occur, making a comprehensive security policy that incorporates training and enforcement absolutely essential. For one thing, handheld mobile devices are much more likely to be stolen, lost, or misplaced by virtue of their compact size and portability. Mobile and remote devices also come in contact with viruses, bots, and other malware more frequently due to increased reliance on public networks and unfamiliar computer devices (printers, kiosks, etc.). To successfully manage the increased risk, formal policies outlining the proper use of organization resources need to be established. These policies should address the three general areas of risk associated with mobile and remote computing: physical loss, unauthorized access, and unsafe user behavior.

Physical Loss

The same qualities – size and portability – that make mobile devices so convenient also make them much more likely to be lost, stolen, or misplaced. Physical loss is inevitable. Since these devices are network-enabled, a lost device exposes the organization to significant risk. Mobile devices are gateways to an organization’s network and any information residing there. It is extremely important to plan for the likelihood of loss or theft, and consider policies that minimize the potential for damage by addressing security at the device level, application level, and data level.

Organizations can provide device-level protections against physical loss by ensuring that mobile computing devices such as laptops are physically secured via cable locks or similar measures when used remotely or in the office. Users should also employ the “Lock Computer” functionality built into Windows by typing Windows-L (holding down the Windows key and pressing L) when leaving devices unattended, even for a few minutes. All computer devices – including laptops and handheld devices – should be password protected via strong passwords – and the longer the password, the better.
Strong passwords involve some combination of capital, lowercase, numeric, and special characters to make them more difficult to crack. Given that many have begun proclaiming that passwords have outlived their usefulness, organizations should consider multifactor authentication schemes that require users to provide: Something the user knows (passphrases or answers to questions); something the user has (tokens, such as magnetic badges); or a permanent personal feature of the user (biometrics, including fingerprint, voice, or retinal scans). Many laptops ship with optional fingerprint scanners, making implementation of multifactor authentication as simple as purchasing a specific laptop model.

To provide protection at the application level, organizations need to make sure that application access is also password protected via strong passwords. In the case of a VPN, it is advisable that a separate and distinct strong password be required to grant access. This makes it that much more difficult for unauthorized users to gain access to critical network resources.

Data-level protection involves the use of encryption to “scramble” data so it is unreadable to unauthorized users who lack a decryption key or password. There are a number of encryption software products on the market that allow encrypted directories to be created on hard drives, USB drives, CD- or DVD-ROMs, and other media, as well as encryption products for e-mail and e-mail attachments. Encryption ensures that sensitive data stored on a lost or stolen device will not be disclosed to unauthorized users. Organizations should look for products that employ 128-bit encryption or higher. The risk of losing sensitive data can also be mitigated by ensuring that devices can be remotely wiped clean, making the data irretrievable to unintended parties.
Unsecured Access

Does your organization abide by the following general guidelines?

☐ Always use Ethernet over wireless when available. It is inherently more secure.
☐ Install and use acceptable firewall software.
☐ Deploy anti-virus and anti-spyware software on all organization computers and computer devices.
☐ Always use a VPN when connecting to network resources remotely.
☐ Be sure to deploy the latest security patches simultaneously to all computers and devices as they become available.
☐ Use digital signatures and certificates when transmitting data via e-mail.
☐ Encrypt documents that contain sensitive data before e-mailing them.
☐ Ensure that Web-based applications are hosted using TLS or SSL websites (HTTPS).

In addition to these general guidelines, the following Wi-Fi best practices should also be communicated and enforced:

☐ Use broadband wireless rather than Wi-Fi, reserving Wi-Fi for Internet browsing only.
☐ Turn-off all wireless capabilities (Wi-Fi 802.11a/b/g/n, Bluetooth, Infrared, and wireless broadband) when not in use.
☐ Disable all ad hoc/peer-to-peer connections when in the field.
☐ Avoid large hotspots (i.e., hotels and airports) where it is unclear who is online.

For organizations that are required to maintain Payment Card Industry (PCI) compliance, a lack of education and awareness around payment security, coupled with poor implementation and maintenance of PCI standards, gives rise to many of the security breaches happening today. The fallout of a data breach can be significant, including fines and penalties, termination of your ability to accept payment cards, fraud
losses, settlements, and judgments. The PCI Data Security Standard (DSS) focuses on six goals.

1. Build and maintain a secure network.
2. Protect cardholder data.
3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Regularly monitor and test networks.

Unsafe User Behavior

An effective mobile and remote computing security strategy needs to address unsafe user behavior. This category of risk represents the great unknown, because there is no guarantee that users will observe the organization’s formal policies when out of the office. Education and training is key. Established policies must be formally communicated and reiterated in frequent training sessions, as well as documented and disseminated in writing so that they become habit and a part of the organization’s culture and expectations for performance. The need for management to achieve user buy-in cannot be over-emphasized. An organization may have a brilliant and exhaustively comprehensive policy document in place, but if nobody reads it or follows the policies it contains, it won’t serve its purpose.

Compliance with internal policies needs to be monitored and enforced. There are a number of managed security and enforcement solutions available. While some employees may complain that usage monitoring is invasive and unwarranted, the threat posed by a security breach, network attack, and theft or disclosure of sensitive information is too great to take a hands-off approach to enforcement. An organization needs to be sure it communicates to employees that the ultimate objective of monitoring and enforcement is to keep the enterprise secure and to minimize threats that negatively impact its viability. Before implementing monitoring and enforcement policies and procedures, an attorney should be consulted to ensure that the organization’s strategy is in compliance with local, state, and federal privacy laws.
Every organization has unique needs, established operating models, and its own personality. Accordingly, the use of mobile and remote computing technologies and the precise configuration chosen will vary from organization to organization. There are, however, a number of common objectives that organizations hope to achieve through the expansion of mobile and remote computing capabilities, including the following:

- Flexible work arrangements and home-based workers
- A well-connected mobile workforce
- Temporary worker accommodations
- Disaster recovery and business continuity
- Client self-service

Now that we have established a better understanding of the MRC solutions available, and have explored some of the security issues and policy considerations related to mobile & remote computing, let’s take a look at the common business objectives that might prompt an organization to pursue a mobile & remote computing initiative and viable solutions for achieving each.

**Employee Connectivity**

For the remote worker, no matter which kind outlined above, a reliable and secure network connection is key. There are numerous options for connectivity, depending on the remote location.

**Broadband connection** – Organizations should opt for a broadband connection (cable, cellular, fiber optic, or high speed DSL) with enough bandwidth to run applications from the organization’s servers, download files stored on the network, and back-up home office data to prevent lost productivity in the event of a computer error or damage to the remote device.

**Wireless cards** – For periodic access to the organization’s network, consider broad-
band cards employing EVDO, EDGE, or 3G wireless technology. Cellular broadband is offered by all the major cell phone carriers, and affords mobile workers network access wherever there is cellular service. If a high-speed data network is not available, the cards are generally backward compatible, enabling them to run on older cell systems at slower speeds. Furthermore, because they are private networks with fewer users and employ encryption to prevent unauthorized access, cellular broadband networks are inherently more secure than public Wi-Fi.

**Public Wi-Fi** – Connectivity through public infrastructure such as Wi-Fi networks at airports, hotels, or coffee bars is not only unpredictable, but it also contains inherent security risks. One journalist accompanied a hacker to a café, and in 20 minutes the hacker showed how he could find out where all the other users were born, where they went to school, and their last five Google queries, among other things. The hacker carried a small box into the coffee shop that became a so-called “evil twin.” The box broadcast a “friendly” Wi-Fi network ID (such as the coffee shop’s name, which looked more believable than the odd address the coffee shop actually used). He became the network, examining all of the transmissions between the users and the evil twin box. It is entirely reasonable to develop a policy that forbids the use of public Wi-Fi, and requires users to connect through a trusted mobile phone.

**Handheld Device** – There are a number of handheld devices that offer connectivity to internal networks for remote e-mail access and simple viewing of digital documents. PDAs, smartphones, and blackberries run across the same EVDO and 4G-enabled networks mentioned above, and some can even act as a broadband modem, extending trusted, quick, and dependable mobile connectivity to laptops and other devices.

Establishing an Internet connection is only the first step, however. Once a connection has been established and a service provider has been chosen, a remote connection to an organization’s network must be established and secured. This is typically achieved through the deployment of a VPN, which enables remote users to connect to internal resources by tunneling through the Internet and the organization’s firewall via an encrypted pathway.

The infrastructure needed to support remote work once connectivity is established depends on the application. SaaS and other Web-deployed applications tend to require less in the way of infrastructure – only a Web browser which serves as the cli-
ent – while other internally hosted applications may require a client component to be installed locally on the remote user’s PC. For example, local applications accessed via Citrix (or other infrastructure software) tend to lag; it may take a while for the results of a mouse click to be visible.

**Remote Control Solutions** — Remote control solutions, such as Windows Remote Desktop, LogMeIn, or GoToMyPC, enable employees to access and control an office PC remotely. As with other mobile and remote computing solutions, it is best to use the encrypted communication pathway afforded by VPN to facilitate and secure the connection to the home office. When more limited access is sufficient, Web-deployed applications or SaaS accessed through a SSL or TLS-secured website can be a good solution.

**Client Self-Service**

In the information-now world in which we live and work, customers and clients expect quick and convenient access to the information they need, when they need it. Many are quite comfortable with electronic communication, and often prefer e-mail and Web interaction to face-to-face meetings. Efficient communication saves them valuable time and money, and having the ability to access the information they are looking for on demand rather than having to establish an appointment keeps them focused on the day-to-day operations of their business. Despite its convenience, e-mail is not always the best option for communicating and exchanging information with customers or clients. For instance, e-mail transmitted via the Internet is inherently less secure than messages sent over a private internal network, and may be vulnerable to interception and disclosure. E-mail communication is further limited by the fact that available bandwidth and e-mail server configurations impose limits on message size. This can make it difficult to send large files via e-mail.

Portals (or extranets) offer an ideal solution for addressing the needs of clients and the limitations of e-mail. They use the same Internet technology employed by intranets and the Web to create secured Web pages that deliver self-service functionality to customers and clients, allowing them to download digital files and access the information they want when they want it, regardless of business hours. A properly configured client portal features password protection to help ensure that only authorized users can gain access, and can easily accommodate large files. Portals can
be customized so that each authenticated user is only able to access the pages, documents, and information intended for them. Portals also support establishing profiles and other personalization techniques that modify content and presentation based on permissions and personal preferences. With a portal, all of a customer’s or client’s information can be stored in one place, forming a central repository. On the user side, a Web browser is all that is required.

For larger organizations, in-house portal development is possible, but it would require a robust IT department with deep programming skills. Smaller organizations may have to outsource portal development, or purchase packaged portal software or a subscription to SaaS portal solutions.

Portals can be hosted internally or with a third-party Internet service provider (ISP). In general, outsourced hosting is preferable for organizations with little room for error. If even a brief outage is unacceptable, engaging an ISP that will agree to a rigid service-level agreement is prudent. SaaS portal solutions tend to include hosting.
The following table provides tactical advice for addressing the three key risk areas related to Mobile and Remote Computing (MRC):

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Tactical Advice</th>
</tr>
</thead>
</table>
| Physical Security | • Implement biometric verification to facilitate multilayer authentication  
                   • Physically secure mobile devices with cable locks if possible  
                   • Monitor for unsafe user behavior  
                   • Mandate password authentication via strong passwords at both the device and application levels |
| Data Security    | • Sensitive data should only be stored on encrypted devices  
                   • Devices should be setup to allow for remote wiping of data  
                   • USB flash drives and other USB storage devices should provide encryption |
| Unsecured Access | • Use Ethernet or broadband wireless rather than Wi-Fi when available  
                   • Install and use a firewall  
                   • Require up-to-date anti-virus/anti-spyware  
                   • Always use an IPSec, SSL, or TLS VPN to attach to network or home office resources  
                   • Host Web-based company applications such as e-mail using SSL or TLS (HTTPS)  
                   • Require employees to turn off all unprotected shares  
                   • Use SSL or TLS websites when sending/entering sensitive data (i.e. credit cards numbers)  
                   • Digitally sign data to make it difficult for hackers to change data during transport  
                   • Encrypt documents that contain sensitive data that will be sent over the Internet |
Disaster Recovery & Business Continuity

Business disruptions can occur for a number of reasons, ranging from relatively benign such as a burst pipe to more catastrophic events like Hurricane Katrina. There are plenty of scenarios in between that can disrupt an organization. They may not yield catchy headlines, but they can devastate an organization in a matter of hours.

Mobile and remote computing is an important component of many disaster recovery/business continuity plans. It enables workers to continue to perform their jobs even when access to the physical office is unavailable. The key is leverage. As organizations roll out mobile technologies, it is important to review how they integrate with existing plans, especially if disaster recovery planning is compliance-mandated (e.g., Sarbanes-Oxley or HIPAA).

Data backup and network redundancy are crucial if mobile and remote computing is to be effective in facilitating business continuity. Simply providing laptops to employees won’t be sufficient if they cannot access the data and applications they need to do their jobs. Locally stored data should be backed up off-site regularly, preferably through automated processes that do not require conscious involvement on the part of end-users. Making the additional effort to synchronize data to servers in different locations means the remote worker may see little or no disruption.

As for access to critical business applications, either an internally hosted solution reproduced offsite or third-party Web-hosted SaaS products should be considered. In the case of SaaS, PaaS, and IaaS, the level of backup and system redundancy offered by the major providers far exceeds that which even the largest and most sophisticated organizations can achieve economically. Because remote control-based solutions rely on office-bound computers to serve as intermediaries between the network and the remote devices, they are not the best option for organizations looking to achieve substantial business continuity and disaster recovery advantage from their mobile and remote computing solutions. If an event causes a disruption at the home office, chances are that the primary device will be disrupted as well.

Technical and cost issues need to be considered when attempting to integrate
mobile and remote computing technologies into a disaster/business continuity plan. Organizations need to make sure when calculating the return on investment for these options that they include the cost of not having access to their data for one or two days, one month, or several months. Laptops may be more expensive than desktops, but if you can’t access your desktops, they are of little use.

**Conclusion**

Determining your objectives and addressing risk are critical when defining your organization’s mobile and remote computing strategy. While there are many benefits of implementing mobile and remote computing technologies, they also pose new challenges, not all of which are technical. They often have operational, personnel, and procedural implications that can change the face of your business. To create an effective plan, begin by identifying the specific technologies that can help you reach your organization’s goals and the amount of risk that the organization is willing to assume.

Risk in itself is not necessarily a problem, as long as you are ready to mitigate these risks throughout the implementation process. Careful planning helps organizations identify what could go wrong before they are faced with problems that could cost significant time or money. Planning starts with understanding how mobile and remote computing technologies can deliver a competitive advantage, and continues with the selection and implementation of specific solutions, along with appropriately documented policies and procedures tailored to address the unique risks inherent in the solution and the organization’s culture.

Begin by reading additional resources about the specific mobile and remote computing solutions from which you think your organization can benefit. Then, work with your IT provider or consider engaging the services of a qualified technology consultant, like a Certified Information Technology Professional (CITP), who can guide you through the issues. Together, you can develop a budget and scalable plan that delivers
the return on investment you need.

Acknowledgement

Much of the content and structure of the discussion paper was derived from the AICPA Information Technology Section’s 2007 discussion paper, Leveraging Mobile & Remote Computing: A Decision-Maker’s Guide.

The following members of the PICPA IT Assurance Emerging Issues Subcommittee contributed to the update of this discussion paper: Adanma Akujieze, Matthew Bogusch, Scott Carver, Mark Dolson, Robert Feltovich, Dennis Galletta, Thomas Huff, Immanuel Karuppumanil, Robert Listerman, Michael McAllister, Samuel Monastra, Michael Reinmund, Bernard Thompson.