Managing IT

to Support Your Mobile Workforce

nsi | Total IT Support

Helping our Clients Succeed since 1985

Table of Contents

nsi Total IT Support
Helping our Clients Succeed since 1985

Executive Overview

The days of the nine-to-five office worker are behind us. People will still be commuting to the office, but more workers find themselves on the clock evenings and weekends, and more "virtual" workplaces are evolving as more employees harness mobile technology to stay connected to the office.

Forty-five percent of all U.S. workers do some work from home or while traveling. While there are three million bona fide telecommuters according to the U.S. Census Bureau, the majority of workers are using mobile technology to take the office with them, checking email while commuting or at home, and accessing office information using their own smartphones, laptops, and tablets.

The mobile workforce has become a reality for businesses of all sizes because employees like the versatility of being able to connect from anywhere, and because of the improved productivity companies get from their mobile workers. Your challenge as a business owner is implementing a strategy to manage the mobile workforce. You want to maximize productivity while minimizing cost and risk. This eBook will help you understand the different approaches to managing the mobile workforce, including what options are available and how to assess potential security challenges and risk.

Mobile Keeps Marching On

So how mobile is today's workforce? In an increasingly global economy, the ability to conduct business from anywhere is not only appealing but also an absolute necessity.

Consider what happens when one of your sales reps meets with a customer and he or she needs to check a contract, access inventory data, or verify a production schedule. If they can answer those types of questions on the spot, they increase the likelihood of closing a deal.

Or what if you run a service company? Can you maintain superior client service without access to e-mail and business-critical documents when you need them? If you aren't connected you aren't competitive, which is why more businesses are mobilizing their employees, either equipping them with mobile workstations or enabling them to access company assets using their own smartphones and laptops.

Employees Want Their Handheld Devices

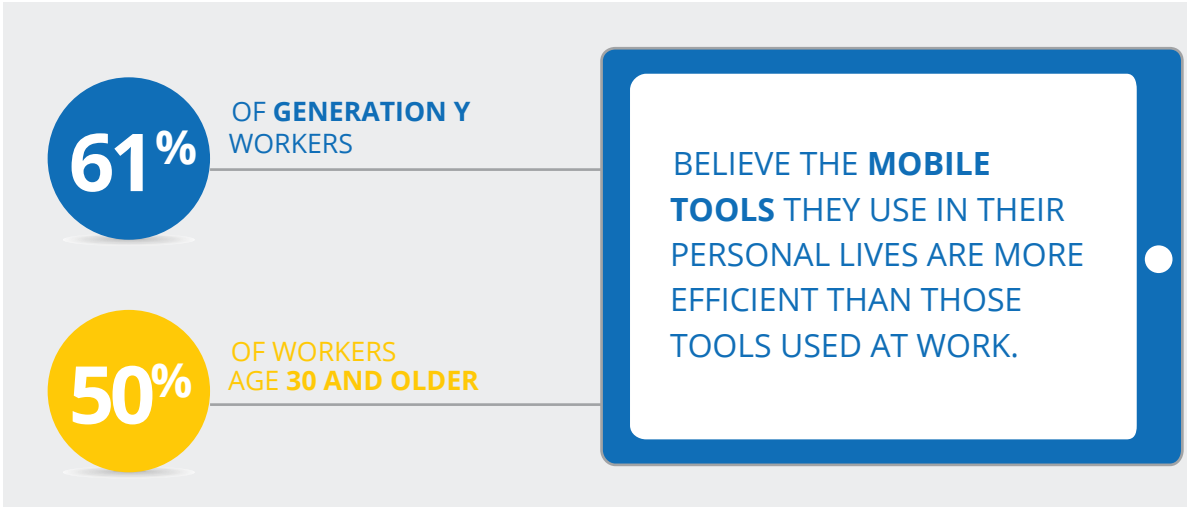
The mobile workforce is continuing to grow because consumers have become hooked on their handheld devices:

32 PERCENT OF EMPLOYEES WORLDWIDE USE MORE THAN ONE MOBILE DEVICE DURING THEIR WORKDAY.

THREE OUT OF FIVE EMPLOYEES NOW AGREE THAT THEY DON'T HAVE TO BE IN THE OFFICE TO GET THINGS DONE.

46 PERCENT OF MOBILE WORKERS FEEL THEY ARE MORE PRODUCTIVE AT THE OFFICE

AND **38 PERCENT** FEEL MORE PRODUCTIVE WORKING FROM HOME.



So workers are clearly looking to adopt the same mobile technology they use at home for use in the office. According to a survey conducted by IDC and Unisys, many IT departments are starting to provide mobile hardware to employees, but 87 percent are already providing support for personal devices.

In fact, **84% of employers** at some point tried to ban bring-your-own device (BYOD),

but **51 percent** have since repealed the ban, realizing that they couldn't stop the tide of BYOD.

But does mobile technology really improve productivity? Email access is one of the biggest productivity boosters. Fewer people who used to access their email through websites now are using mobile devices to get their work email. Research shows that 78 percent or more of smartphone users are accessing mail on their handheld devices, which means faster response time and greater productivity.

With the boom in computer tablet sales, more than 65 percent of employees are using their tablet computers for work. More than 19 million tablets were shipped in 2010 and that number is expected to grow to 276 million units by 2017. The younger the employees, the more they are using tablets.

70%

of workers under age 34 use tablets at work

as opposed to age 55 and older.

47%.

Mobile Technology Boosts Productivity

In addition to viral adoption of mobile technology by workers, more businesses are seeing the value in arming their employees mobile devices as well.

Ninety-one percent of organizations have a mobile work strategy in place. Worldwide, the amount of physical office space is shrinking while the number of employees is increasing. There are now seven desks for every 10 employees. And companies are working to embrace mobile technology to promote greater productivity:

68%

OF COMPANIES RANKED MOBILIZING BUSINESS AS THE TOP CONCERN FOR 2015 SECURING DATA RANKED SECOND

60%

OF COMPANIES HAVE SOME TYPE OF BYOD POLICY FOR PERSONAL DEVICES IN PLACE.

MORE THAN **50%** OF COMPANIES ARE BUILDING **10 OR MORE** MOBILE APPS FOR THEIR BUSINESS.

Businesses have recognized that mobile technology is the key to streamlining operations:

53% ARE MOBILIZING CORE BUSINESS PROCESSES.

49% SEE TRAINING IN PROPER USE OF MOBILE TECHNOLOGY AS CRUCIAL.

43% ARE LOOKING TO GET MORE ANALYTICS AND INSIGHT RELEVANT TO MOBILE PROGRAMS.

To remain competitive, and attract the best of the new generation for their workforce, companies need to deploy competitive business tools, and that means mobile technology. Mobile is now part of the fabric of every company, whether they are local, national, or global. And implementing a mobile program to get employees connected, increase productivity, and share business-critical data can be both an integration and a security challenge for any organization.

Supporting the Mobile Workforce

You can use various network configurations to manage your mobile workforce. There are networks designed to support occasional users, such as your team of road warriors. There also are configurations designed for remote offices, telecommuting, on-site contractors, off-site partners, and just about any type of mobile application. The primary differences are the levels of access, available resources, and most importantly, security.

You may choose to use one or multiple network configurations to support mobile users. However, your core objectives remain the same: you want to eliminate network downtime or delays in system access, and you want to harden security so mobile data access doesn't become the weak link in your network security infrastructure.

Here are some basic considerations when designing your network infrastructure to support a mobile workforce:

Every Remote Connection is a Potential Risk

When you are dealing with remote workers, telecommuters, and part-time employees, you have to provide network access while retaining control of the connection.

The biggest challenge IT managers face when dealing with remote workers is an inability to oversee both ends of the network connection. The IT department has control of the company servers, anti-malware protection, corporate firewall, and other enterprise security components, but they have no control over the remote user. Mobile users could be accessing an unsecured wireless connection from a coffee shop, or they could have an infected laptop that could threaten the network. The IT staff cannot manage the configuration of a remote workstation, including the antivirus software. Nor can they control the level of security of the remote network connection. Therefore, the safest course is to assume that every remote user presents a potential security risk.

Once you start from the assumption that every remote user poses a potential threat, then you can proceed accordingly, limiting network access and ensuring that network connections are secure and protected from the host side.

Using Virtual Private Networks

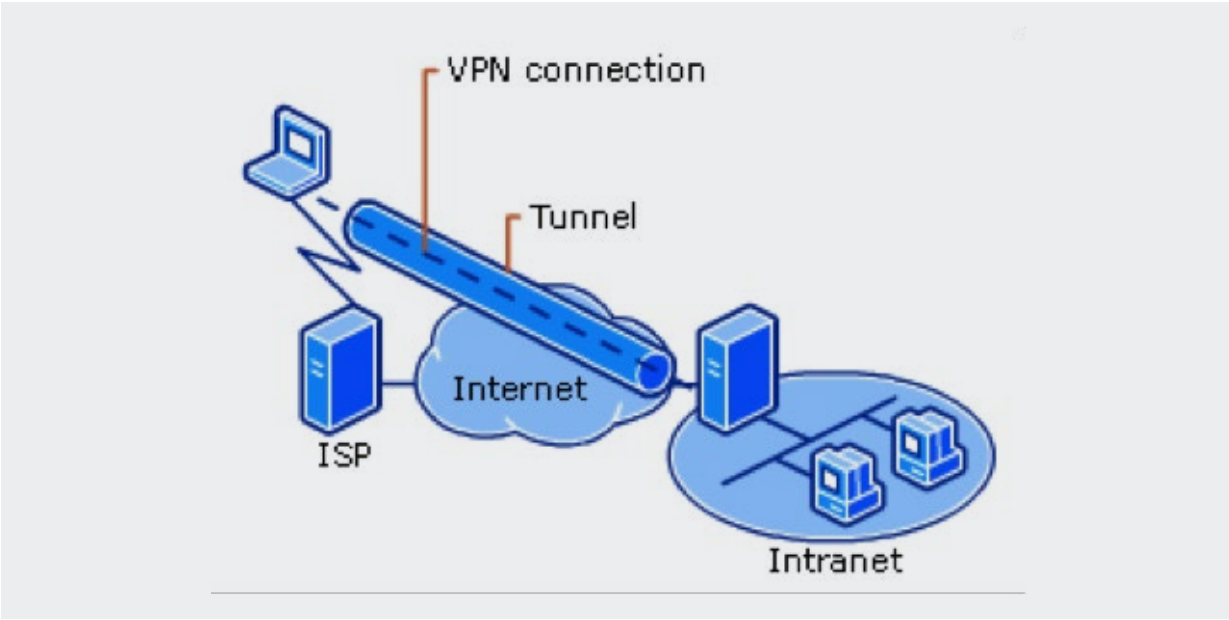
Best practice dictates that for most remote connections, you want to use a Virtual Private Network (VPN). A VPN is a means of providing a secure connection over a less secure network. The VPN provides the level of security you need to support your mobile workforce, since you can't trust the intervening network that brings the connection to the network firewall.

> A VPN is designed to provide security over a public communications infrastructure, such as the Internet. The remote client needs to be authenticated to connect to the VPN gateway in order to gain access to the network. Once the remote user is authenticated then they can access files and network resources through the VPN gateway.

Depending on your requirements, the VPN gateway can apply different protocols to establish a secure connection. For individual users, an Internet Protocol Security (IPsec) link provides a secure means of exchanging data. The advantage of IPsec is that it doesn't require a unique VPN client and it can support secure access by any user with the right authentication identifiers. For added security, some VPNs use an additional tunneling protocol such as the Point-to-Point Tunneling Protocol (PPTP). This can be an ideal approach to provide secure access to occasional users or guests.

To provide secure access to a specific application or for users that require frequent network access, VPNs can use Secure Sockets Layer (SSL) authentication, which manages authentication of network servers and remote clients, and handles encrypted communications between servers. For telecommuters or trusted remote users that connect to the network frequently, a VPN with SSL security is recommended.

Even though you need to grant authenticated network access to mobile users, that doesn't mean you want to hand them the keys to access the entire enterprise. A VPN also supports sets of discrete networks in that it operates across a shared network infrastructure but without sharing any connection points. This means you can control user access using VPN, limiting access to sensitive portions of the network.



Remote Workers vs. Occasional Workers

You want to use a different strategy to connect dedicated remote workers as opposed to part-time workers or contract employees.

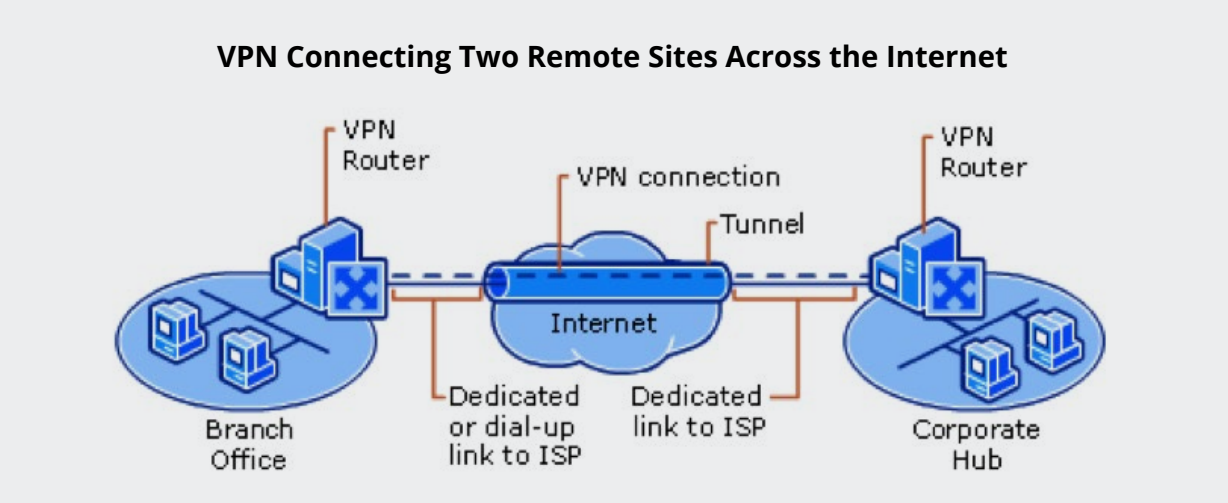
For employees that need frequent or dedicated access to specific network resources, using a VPN with SSL security should provide secure access to specific portions of the network. The VPN client software can be configured to provide access to designated servers or data. In fact, VPN clients re often used to manage access for the corporate Intranet as well, segmenting the internal network so only specific departments, such as payroll and HR, can share sensitive information. For dedicated telecommuters or remote users, the IT department will have more control over the client hardware with SSL, including VPN client configuration.

For occasional or part-time workers, VPN access using IPsec can provide controlled, secure access no matter whether the client platform is a laptop, a tablet, or a smartphone. The VPN connection authenticates the user, and the same kinds of restrictions can be applied so remote users only have access to authorized areas.

Your definition of a “mobile workforce” should include those users who come to the office occasionally to work on site. They could be full-time employees from other locations, contract workers, or guests. Using a wireless link to connect users to an isolated part of the network designated as “safe” for visitors is one way to provide access without incurring risk.

Connecting Remote Offices

A site-to-site VPN is an ideal way to connect a remote location or office as well. The site-to-site VPN uses a gateway that connects one network or data center to another. End-nodes don't require a VPN client because the gateway handles the connection. In essence, a site-to-site VPN is a secure connection over a public connection between two VPN gateways. Most site-to-site VPNs use IPsec for authentication.



Unlike granting individual remote users access, when connecting remote offices you are authenticating access for the entire network at each end, so additional access controls and authentication have to be applied. Once a user is authenticated to access the local area network, the same authentication rules would apply to the VPN connection as well; to the user, the VPN looks like just another LAN resource.

> Networks are increasingly using cloud resources to provide a secure link between a VPN gateway hosted in the cloud, and a VPN gateway on the network. This makes it easier to connect any remote office location and in some cases remote service providers.

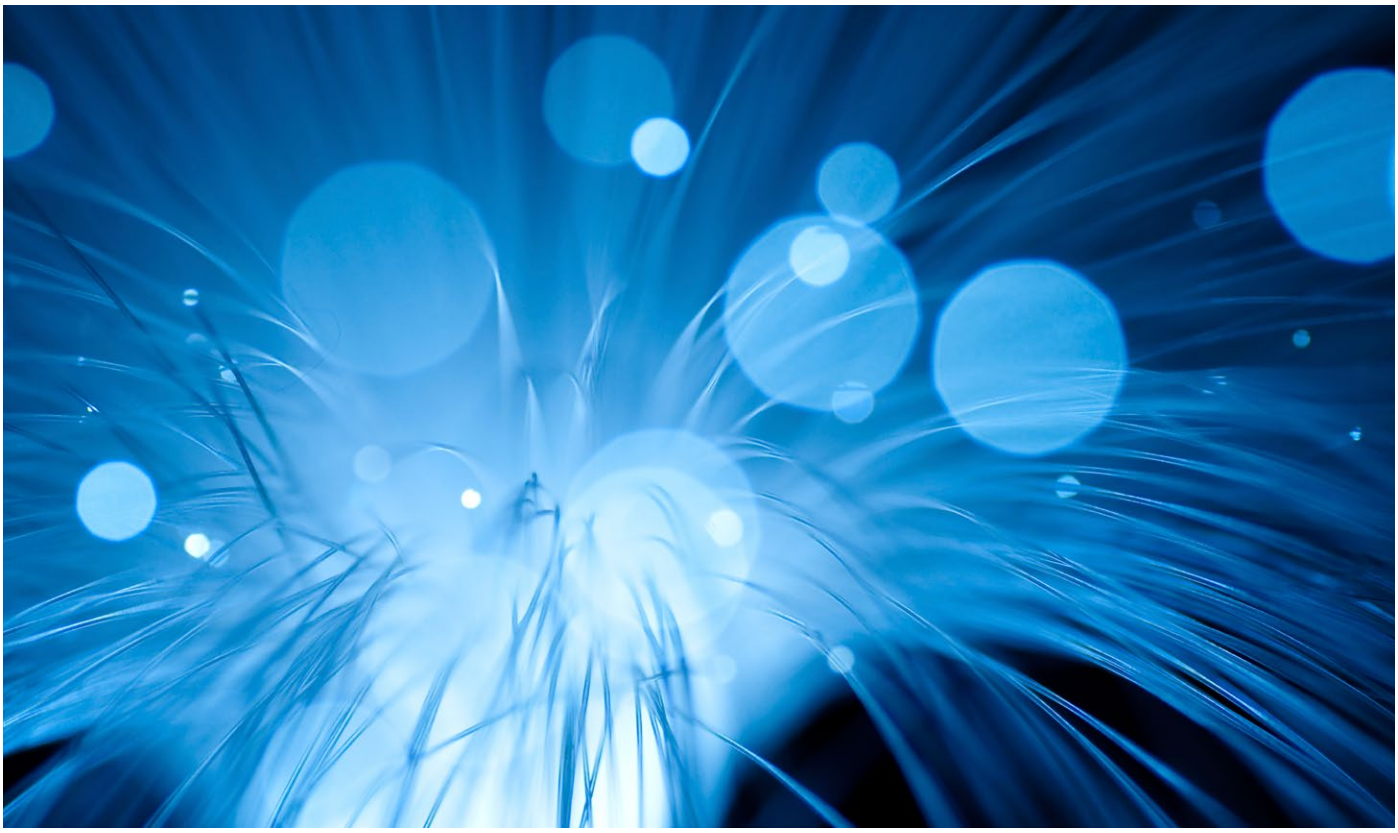
Remote Desktop Connections

Remote computer connections based on the Remote Desktop Protocol (RDP) are one means to support remote workers. Every Windows machine has an RDP client, which can be connected to a Windows server running RDP on the network. Using RDP, you can create a Remote Desktop Connection with a computer workstation across the corporate network, a dedicated wide area network connection, or a connection such as the Internet.

Rather than sharing just file data, RDP creates a shared desktop. The remote client can connect to their work computer, for example, and access applications, files, and network resources such as local printers from the remote computer just as if they were sitting at their office desk. The RDP connection presents the same interface and applications as they would see on their LAN workstation.

To establish an RDP connection requires the proper permissions for connection and authentication, including a password. Sending and receiving data through an RDP connection is similar to a conventional network. The application or service data is read, encrypted, and delivered as data over the network, and then sent to the address for the remote client. Data from the client works in reverse, sending packet data that is decrypted by the RDP server for use by the designated application.

RDP can be a valuable tool when you need to access proprietary software or software with controlled user licenses. The connection is secure and reads licensing information so it can provide access to registered server applications as if the connection was on the local network. It's also a good way to ensure that the data remains on the network server and is not transmitted outside the system, since the RDP protocol allows remote users to manipulate data across the network without having to transfer it.



Authentication and BYOD

Inevitably, you are going to have to deal with employees who want to use their own smartphones, tablets, and laptops for work. You can give them credentials for a VPN connection so their remote device can access network resources using a secure connection; however, you should consider stronger security measures when supporting BYOD.

Multi-factor authentication methods harden security while still promoting BYOD security. Consider adopting measures beyond simple password access. One-time passwords are one approach, and you can use alternative notification strategies such as delivering a text message for authentication. Once connected, using a secure SSL VPN connection provides security to any authenticated users, since you don't need client software.

You might also consider adopting Single Sign On (SSO). Rather than forcing employees to log in to specific servers and applications, you can use an SSO tool as part of SSL VPN configuration so authenticated users have a single password to grant secure access to both authorized network and cloud resources.

Using soft security tokens is a means of further securing BYOD data. A soft token interacts with the mobile device, such as a smartphone, to apply two-factor authentication. This is an easy way to add another layer of security, and it can be easily managed and updated since it's all in software.

The challenge with BYOD is that the company never has complete control of the user's device. Limiting access to sensitive data or making sure that data can be viewed but cannot be transferred will help keep data safe. And remember that smartphones and laptops can be lost or stolen, so insist that your BYOD users have some tool that allows you to remotely lock the device and wipe its memory.

Strict corporate policies must be in place and enforced for all remote users. Any **BYOD policy**, for example, should insist upon auto-locking capability with a PIN, encryption, and remote wipe in case of theft. It also should cover the types of data that can be stored remotely, and acceptable backup procedures. Highly regulated industries, such as healthcare and financial services, have strict security regulations so it's essential to make sure your policies comply with regulations and they are enforced.

Maintain Strict Provisioning and Decommissioning Procedures

The biggest threat to network security is human error, and one of the biggest holes in network systems is users who are no longer with the company and forgotten passwords.

When you bring on a new employee or remote users, you need to have a well-defined and well-documented procedure in place to provision that user's remote system, including establishing access to specific portions of the enterprise and authentication protocols. When any new employee joins the company, Human Resources has a checklist of things that must be completed, such as tax information, payroll, employee manual, email, etc. There should be a similar detailed checklist to ensure employees have the necessary network and remote access.

Identity and access management (IAM) can be used to initiate, record, and manage user identities, including permissions and access rights. The benefit of adopting IAM is that it's automated, which means you can establish a single set of access protocols and the system automatically enforces policies and procedures, making sure individuals and services are properly authenticated, authorized, and audited. This includes establishing authentication for mobile users and BYOD hardware.

> As part of your security strategy, you should be auditing network usage on a regular basis. You want to ensure that your mobile users don't have access to sections of the network where they don't belong, or that unauthorized users are entering the system.

When an employee leaves the company, it's even more important to have a detailed checklist to deauthorize workers. Disgruntled workers are often able to access the company network and wreak havoc because no one bothered to disable their credentials. Make sure you maintain a detailed checklist to delete credentials from applications, servers, the VPN gateway, active directories, Intranet logins, and so forth. Be sure to retrieve any mobile devices such as laptops and smartphones as part of the exit interview, i.e. before they leave the building. Also, be sure to change any common passwords or PINs.

The Technical Requirements for the Mobile Workforce

These are just some of the considerations for managing a mobile workforce. Now you have to consider the best technology and remote access architecture to meet the unique needs of your mobile workforce. Here are some basic considerations when considering technical requirements:

Enterprise Gateway or SaaS

Larger enterprise networks typically maintain a standalone VPN gateway or secure remote access appliance as part of their mobile computing infrastructure. Although this requires more IT management time and administration to install, configure, and maintain, it also provides greater control, including the ability to use stronger security measures.

A Software-as-a-Service or Web-based VPN gateway is also an option. Unlike VPN gateways that protect direct access to your network, a Web-based VPN provides a secure connection to the Internet, which can be extremely valuable to eliminate problems with eavesdroppers at public Wi-Fi hot spots. Using a hosted VPN service eliminates having online advertisers track you or other privacy issues when using Wi-Fi in public places. There are security concerns with some hosted VPN services, but if you are already using cloud services, a SaaS VPN solution can be a cost-effective solution.

Wireless Networking

As part of your mobile worker infrastructure, you will want to be able to support employees who occasionally come to the office. The easiest solution is setting up a wireless network. Wireless bandwidth is shared, so if you have a wireless network in-house to support employees and drop-in or mobile workers, make sure you have sufficient wireless capacity. That will probably mean multiple wireless access points.

The latest wireless standards will help here. The 802.11ac standard has been developed specifically to handle more users. Manufacturers claim that the 802.11ac wireless standard is three times faster than the previous standard, 802.11n, but more importantly, it can handle more connections. Although manufacturers are currently making 802.11ac wireless routers with four antennas, the specification can certainly handle eight connections, each running at 400 Mbps.

An IT professional can optimize your office wireless network, making sure you have enough wireless access points in the right locations.

Back-Office Integration

The reason to go mobile is to promote worker productivity. You want to give employees access to back office systems and applications that make them more productive in the field, but you don't want to sacrifice back-office efficiency for mobility. For example, using remote access to capture sales data in a spreadsheet isn't useful if that data then has to be manually entered into an Enterprise Resource Planning (ERP) system.

When considering your mobile workforce, consider your current back office applications and how many of them will elegantly support mobile users. Many vendors offer their own mobility platforms. Salesforce, for example, has an entire app exchange that offers mobility solutions for its Customer Relationship Management (CRM) platform.

Also, be sure that you have the tools and resources needed to connect your field workforce with back-office business systems. For example, is true two-way communications? Some interfaces will be intuitive and offer drag-and-drop integration, while others will require custom software development and maintenance. Determine how difficult it will be to extend your enterprise software for productive use by your mobile workforce.

Off-the-Shelf versus Customizable Solutions

The age-old question that all network managers face is whether it's more effective to build a solution or buy someone else's product. It takes longer to build your own application, and after you build it, you have to manage it. If you buy an off-the-shelf solution then you may be limited to the features and functions that the vendor offers, which may or may not meet your needs.

When it comes to supporting your mobile workforce, it's difficult to anticipate future needs. Mobile and wireless standards change. New mobile hardware platforms emerge and fall from favor almost overnight. The company's back office needs also evolve, which can present new challenges when it comes to connecting mobile users. Your best strategy is to find a solution that meets your needs today and has the flexibility to grow with your needs.

In some cases, you may want to build your own customizable interface for a business-critical back office application. Developing a mobile app isn't that expensive and there are services that will do it for you. However, remember that you will have to maintain that app as technology evolves. Consider standardizing on a single mobile platform, such as Android or iOS, and be sure to use standardized development tools so you can upgrade the software as needed.

Managing Mobile Workflow

In addition to mobile compatibility, consider what impact mobile applications are going to have on workflow configuration. Part of customization has to be having the flexibility to determine where incoming data is routed and how it flows to other systems. For example, do you have to create custom field forms? Are there additional integration steps required for mobile users?

Your goal is to make workflow seamless for mobile users, but you may not be able to offer the same workflow experience. Consider how the exchange of data with mobile users will affect orchestration of data and systematic business processes.

Offline versus Online

There are times that mobile workers may not have access to a network connection, or perhaps they just prefer to prepare the day's work and then submit it all at once as a batch process. Can your mobile system handle offline as well as online users?

Mobile workforce software has to be able to handle data conflict detection, synchronization, and version management. For example, what happens if a remote worker tries to overwrite a file with an outdated document? Be sure your mobile systems can handle version management and data conflicts so data isn't misaligned or duplicated.

Proprietary Hardware, Standard Devices, and BYOD

Some mobile applications call for proprietary hardware, such as bar code readers or customized tablets. Retail, for example, often calls for proprietary hardware that incorporates credit card readers, scanners, and other features, although increasingly retail software is running on off-the-shelf hardware such as an Apple iPad. Consider the best and most cost-effective solution for your mobile users.

For example, can remote users gain access using any network browser, such as Explorer, Chrome, or Firefox? What about handheld devices? Does the software support both iOS and Android? Are there hardware limitations such as memory requirements, screen resolution, GPS requirements, a built-in camera, etc.? These factors will determine if you need proprietary hardware or specialty devices.

As part of your BYOD policies and procedures, be sure to limit access to those devices that are compatible with the enterprise mobile applications, otherwise, your IT team may be troubleshooting incompatible devices.

System Security

You can't be too cautious when it comes to security. You may have the best firewall and antivirus protection on the market, but any network security system is only as strong as its weakest link. Make sure your mobile applications aren't that weak link.

Understand how the software vendors support data security. Do they use encryption? Is there a risk to data being stored on a remote mobile device? How compatible is the software with your other security products, such as the firewall or cloud-based VPN platform?

You don't want to compromise security for the sake of convenience. Make sure your mobile solutions integrate smoothly with your network security systems.

About NSI Total IT Support

NSI provides end-to-end networking and IT support to organizations of any size. NSI offers customized integration, network design, and system management services to meet any need and any budget.

- NSI's TotalCare Managed Services Team is available to monitor and manage the overall health of your computer network, using advanced asset management tools to ensure that your network is operating at peak performance.
- NSI also offers TotalCare Data Backup and Recovery services to ensure that business-critical data is safe and secure.
- NSI TotalCare Managed Services for Print is available to save you time and money by maintaining your office printers for you, including maintenance, troubleshooting, and printing supplies.
- If you need hosted services, NSI also offers affordable onsite, offsite, and cloud hosted solutions to minimize risk of system failure while maximizing computer resources.
- NSI also offers comprehensive help desk and support services to keep your business-critical systems up and running.

For more information about NSI, visit www.nsiserv.com.