Strategies for the connected workplace

Making the most out of mobile devices while protecting your enterprise

verizon

Business needs and goals

Enterprises are realizing a new vision where constant connectivity and communication plays a major role in every aspect of daily business. The use—and usefulness—of mobile devices in the workplace is increasing exponentially.

Mobile initiatives can help enhance your:

- Process
- Satisfaction
- Agility
- Communication
- Productivity
- Interaction

Done right, mobile initiatives deliver an excellent return on investment. Companies that embrace mobility can:

- Increase communication and collaboration.
- Boost productivity and reduce response time.
- Elevate employee satisfaction.
- Interact quickly with customers, improving customer satisfaction.
- Streamline business processes.
- Adapt quickly to the next wave of technology.

There are challenges, though, including:

- Maintaining security in a mobile environment.
- Understanding how mobile devices impact IT environments and company workflows.
- Training IT to troubleshoot devices remotely
- Adopting backup and repair/ replacement strategies.

How can you successfully integrate mobility into your business?

By partnering with a trusted technology provider that can help you work through the following five steps to create a mobility strategy.

1. Business needs and goals
2. Security and mobile device management
3. Deployment
4. Support
5. Positioning for the future

Business needs and goals

The best mobility strategy is one based on your unique business needs. Answering these questions will help define your plan.

What would you like to accomplish?

Do you need to:

- Access sensitive or proprietary information from the field?
- Quickly respond to changing conditions or customer needs?
- Use customer relationship management (CRM) or sales force automation (SFA) systems remotely?
- Capture signatures or accept payments offsite?
- Stimulate communication and collaboration
- Get data from machine-to-machine (M2M) connections?

Understanding these goals will help you determine device and security needs.

Operating system support
There are several manufacturers and operating systems to choose from—Apple® iOS, Android,™ BlackBerry® or Microsoft® Windows.® It may not be realistic to try to limit operating systems you support, particularly if you adopt a policy allowing employee-owned devices.

If you open the door to all operating systems by letting employees use their personal devices on the job, you can reduce training time and spend less money purchasing devices. However, the complexity of managing multiple device types may require you to put more resources into security and tech support.

Device decisions
There are many ways to work on the go, ranging from toting a full-size notebook to chatting on a slender smartphone.

What works best for your employees?

To ensure that everyone has the apps they need to incorporate their personal phones into the workplace, you can also set up a business app storefront mirroring those in the consumer space.

Tablets and mini tablets are best for employees who:
- Create or edit content, including video.
- Stage or participate in video conferences.
- Create or participate in presentations.
- Access desktops or internal applications.
- Take lots of notes.
- Need to capture data and/or signatures.

Smartphones are most practical for employees who:
- Need to talk and/or text frequently.
- Need a portable GPS for turn-by-turn navigation.
- Need a more compact device.
- Need a versatile device capable of doing anything from making phone calls to running business applications.

Relatively new on the scene are hybrid devices that combine the capabilities of a smartphone and mini tablet. Hybrids might be a good option for employees who:
- Need a screen larger than a smartphone's, but don't want to carry two devices.

How will you connect to a wireless network?

4G LTE–capable devices maximize speed and functionality, and eliminate the hassle and expense of carrying additional hardware. They also keep your data secure. 4G LTE provides enhanced security on multiple levels, including secure storage of credentials and data on SIM cards; mutual authentication between the 4G LTE SIM and the network; 128-bit root keys instead of 64-bit keys; creation of session-specific encryption keys for signaling and subscriber data; and additional algorithms to check data integrity.

With 4G LTE–enabled notebooks, smartphones, tablets and hybrids, you can:
- Eliminate the risk of sending corporate data through unsecured public Wi-Fi networks.
- Access business systems immediately, reducing response time.
- Increase productivity.
- Improve return on investment.

Another option is to use a portable Wi-Fi hotspot. These are particularly handy if you want to connect multiple devices, for groups of employees traveling together or working offsite. And they are preferable to public Wi-Fi networks, because you control the security of the hotspot and access to it.

Employees should be encouraged to connect only to known, secure Wi-Fi networks, so your company data—and reputation—stay secure.

You also want to make sure your carrier provides coverage everywhere you do business, including overseas.

Consider what kind of apps your employees will need.

Do your employees need access to business-specific apps? If they do, will off-the-shelf solutions work, or do you need to develop your own?

Off-the-shelf apps have a standardized feature set and are generally more affordable than custom apps. Or you can develop your own proprietary apps. Tools such as mobile enterprise application platforms (MEAPs) can reduce the time, cost and effort of creating apps—or you can work with a vendor that offers mobile application architecture and design.

Security and mobile device management

Integrating new devices and new operating systems requires taking a fresh look at your policies and processes. Strong security is critical for mobile devices, which are easily lost or stolen, because you lose not only the device, but the data on it, too. A vendor offering mobility management services, which include mobile security, can help you develop and manage policies and processes.

Data security

In this approach, mobile device storage is encrypted to help protect data in case the device is lost or stolen. Depending on the device, the internal storage, the application data or even additional storage (such as a Secure Digital [SD] card) can be encrypted.

Device security

Another option is to secure the entire device through enforcement of a Microsoft® Exchange ActiveSync® policy or through a mobile device management solution. This allows your IT department to wipe the device remotely if it's lost or stolen.

Identity and access security

Enterprises can also channel users through a virtual private network (VPN) or Private IP and/or set up an authentication process to ensure that only authorized users can access corporate networks, systems and information. This can prevent fraudulent access and use of data that could potentially impact your business, partners and customers. Further controls can be put in place to automate user account provisioning and workflow, so that employees can access only the applications and information appropriate for their job profile and responsibility level.

Employee-owned device policies create their own unique security challenges. To secure enterprise data on employee-owned devices, you can use dual-persona software, which partitions personal and business applications. That means IT administrators can enforce enterprise-level security on the business side, and perform remote lock and wipe if the device is lost or the employee leaves the company.

Security policies should also include a strategy for backing up data. If your employees use mobile apps that store data locally, that data could be lost if the device fails. A more reliable strategy is to transfer data and applications to and from a secure cloud-based system.

Deployment

Deploying mobile devices requires a different strategy than traditional workstations. Mobile devices may need additional management systems, such as a mobile device management platform, or additional support processes.

Take steps for a successful deployment:

1. Plan
2. Configure
3. Distribute
4. Train

To decide how to proceed, ask yourself a couple of questions: How do you want to configure the devices? Should configuration take place before or after users receive them? With over-the-air (OTA) capabilities, you can remotely update applications, configuration settings and operating systems on myriad devices, whenever needed.

Configuration requirements may include:[1]

- Mobile device management (MDM) software
- Exchange ActiveSync
- Company-used applications
- Wi-Fi
- VPN

You also need to think about logistics: How will you get the devices to users who might be spread across multiple locations? Will they be new users, or are you simply upgrading existing equipment?

Also, if you need to keep track of what kind of mobile devices you have, who they're assigned to and for how long, you may want to make an asset-tracking system part of the deployment process.

To prepare for mobilization, IT departments should create policies for acceptable use and make sure users understand them. If your policy is to remotely wipe a device when it's lost—or when an employee leaves the job—users need to know that before they put personal pictures, music and so forth on it.

Don't underestimate the importance of training during the deployment phase. Some users may not be familiar with touch-based interfaces, or know how to make the best use of mobile business applications. Training on the front end can pay off in less tech support time later—and help your company more quickly reap the benefits of mobility.

Support

Providing tech support to mobile device users can be challenging for traditional IT departments.

Mobile device users may configure their phone or tablet to suit their tastes, and may have personal music, pictures and apps on it. That means IT has to navigate those customizations while troubleshooting, so it can take longer to help users through issues.

We're just beginning to explore all of the ways we can use wireless technology to evolve business models, generate growth and solve business and societal challenges. Taking the time to plan for a successful integration—and partnering with the right vendor—will empower you to leverage the newest technology to meet your core business goals and objectives and position yourself for future success.

Also, because the devices are, by definition, generally used outside the office, support staff often have to work remotely, which can also slow down troubleshooting. In addition, if you have a policy allowing employee-owned devices, the support person may not be familiar with the interface of a particular phone.

You also need to set expectations for what a device is capable of and what is considered responsible use. The device and infrastructure can only do what is within their feature set. Sometimes employees may think a device is broken when they are simply not using it correctly.

Another consideration is device replacement and repair.
Productivity suffers if a device is lost or quits working. To minimize downtime, it's a good idea to partner with a carrier that will:

- Help you locate lost devices.
- Rapidly deliver a replacement device, anywhere in the world.

Positioning for the future

It's important for enterprises to keep a finger on the pulse of technology innovation and integration, and to keep moving forward.

As information technology reaches the next stage, the way we view and accomplish work is undergoing a fundamental change. More people are working from home or from the road, and that's a trend that can easily fragment a workforce.

Developing a strong mobile device strategy now will create the foundation for long-term success. Because a mobility platform does more than untether people—it brings your business together. It empowers employees to communicate and collaborate and access the information they need, turning business into an action—not just a place.

Let Verizon help you harness the power of mobility

Verizon can help your enterprise leverage mobile communications to securely and cost-effectively power productivity and boost communication and collaboration.

No matter where your business falls in the mobility spectrum, we can help, whether it's driving a new mobility initiative or making the most of your existing program and assets. We have the devices, plans, coverage, services and partners to help you accomplish your goals.

Explore mobility offerings from Verizon.

Mobility solutions
Verizon can assist with planning, design, implementation and operation and management of mobility solutions.

Mobility management
This service helps you understand and manage your mobile inventory, spend, logistics and apps, and protect company data with secure managed connections for remote workers.

Wireless devices
Verizon makes it easy to find the right devices, whether you need tablets, smartphones, basic phones, mobile hotspots/Verizon Jetpack® devices or USB modems.

Voice and messaging
Voice and messaging services from Verizon give your team the quality and functionality they need to respond faster and keep your business moving. With services like messaging, Group Communications and Push to Talk, your entire team can communicate simultaneously.

Mobile application
Whether you need to organize your sales force, monitor vehicle usage or convert to a mobile office, Verizon can get you there with applications that help you close more deals, control costs and increase productivity.

Mobile broadband
With Verizon Mobile Broadband, you can securely log on via VPN from more places—for instance, from inside a taxi, in an airport terminal or even at a job site at the end of a dusty road.

Global communications
Verizon's global solutions—supported by our global partners—give you the power to support your workforce virtually anywhere business takes them.

Private network
Verizon Private Network offers your organization its very own reliable and secure wireless extension to your IP network.

Verizon was the number-one-ranked telecom company in Fortune® magazine's 2012 list of the world's most admired companies, including first-place rankings for innovation and quality of products and services.

The right technology to set you apart

At Verizon, we've made substantial and deliberate investments to bring together the assets that will help you reap the benefits of technology convergence.

The intersection of cloud, mobility and security is driving a massive revolution in business and government IT. Our strategic acquisitions and investments have allowed us to build out our core competencies. We've expanded our global IP networks and our 4G LTE network in the U.S., and our security practices, with Cybertrust. Most recently we've expanded in the critical areas of cloud, IT and machine to machine with Terremark, Cloudswitch and nPhase.

To deliver that value, Verizon has created an innovative portfolio of platform technologies, the foundation to building solutions that help overcome today's challenges to your industry, your business and your customers.

Our broad portfolio of device vendors allows us to objectively recommend the equipment that best fits the needs of your business. The Verizon Partner Program includes over 150 companies that help us tailor industry solutions that meet the unique needs of your business and customers. Working with world-class technology and application vendors enables us to create and deliver end-to-end business, communications and industry solutions.

Verizon leverages its investments, partners and highly experienced workforce to create complete turnkey, configurable solutions that span the globe; together, we're solving industry-specific challenges and inspiring the big ideas of tomorrow.

1. The availability of these features requires a combination of device and management software.

Learn more.

For more information, contact your Verizon Wireless business specialist or visit us at **verizonwireless.com/contactarep**