



Wireless Device Management:
Controlling The Wireless Enterprise
And Reducing Total Cost of Ownership

Today's Wireless Environment

The technology platform of today's enterprise has a rapidly growing component: wireless systems. From field operations, to logistics and supply chain, a host of crucial business activities and applications are now conducted, even driven, by wireless mobile devices.

Wireless technology makes today's global supply chain enterprise more flexible and better able to respond to changing markets and aggressive competition. In the past decade, these devices and their applications have transformed supply chain management – making it leaner, more productive and more in tune with customer preferences and expectations.

However, the fundamental value of wireless devices – their mobility, which translates into ease of use and efficiency – is also their greatest challenge from an IT management perspective. Many businesses now recognize that comprehensive management of their wireless device infrastructure is a crucial component of a total IT enterprise management solution.

The Challenge of Mobility

A mobile device is not locked down – it's an enterprise asset that is potentially always on the move. It contains valuable software and firmware that needs to be configured, tracked and managed as your business grows, in lockstep with the other components of your enterprise IT environment.

As an active digital device, it is a point of entry, and thus a point of vulnerability for the wireless-enabled enterprise. In this Web-

based digital age, network security remains a paramount concern.

Recently, a major US auto manufacturer had their global network compromised via a wireless link into one of their facilities located in Europe. Additionally, a major US electronics chain learned that people in their parking lot were plucking customer's credit card information from their wireless network. These types of breaches, sniffing and network hi-jacking have raised the overall awareness around Wireless Security and caused the initiation of several wireless compliance-based standards.

And, given today's business environment, enterprise mergers and acquisitions are a constant fact of business life. Potentially, that means managing and migrating multiple wireless platforms, with potential legacy technologies and protocols.

Managing Complexity and Change

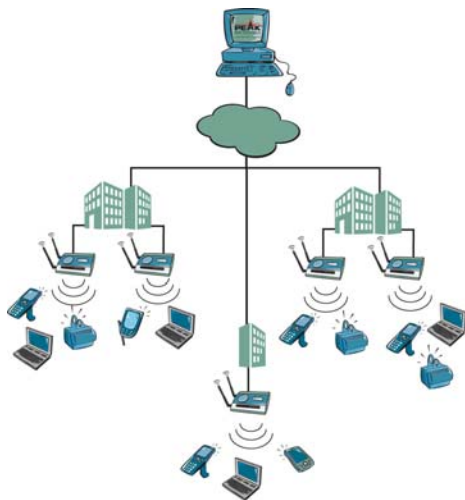
The use of wireless technology in supply chain management has exploded- far faster than expected by some. Wireless Technology is becoming pervasive and a given component of today's supply chain systems. It's a classic dilemma: Budget, time and skilled resources are not available, or have not been allocated, to manage these fast-growing platforms.

In addition, wireless platforms generate unique challenges:

- They are distributed over many remote locations, or on mobile vehicles;
- There is an evolving mix of proprietary and standard operating systems and applications;

- They involve radio frequency-specific technology, operating requirements, and protocols; and
- There are multiple compliance issues that need to be addressed with wireless information movement and distribution (such as PCI, Sarbanes-Oxley, HIPPA, etc.).

And the challenge is growing fast. Proprietary wireless protocols and operating systems have evolved to standards-based products and platforms (MS Windows, 802.11, etc.). This has stimulated much wider use of mobile technologies, with expanded applications and product offerings.



Wireless Device Management Architecture

This technology change is also contributing to much shorter product lifecycles. In the past, IT management could specify and adopt a platform, anticipating 5-10 years of use before replacement. However, conditions now have new technologies and applications being rolled out in 2-3 year cycles; it's essential to manage that kind of change strategically and proactively, to

ensure your business has the latest, most effective tools to remain competitive.

Just as with other information technologies, wireless devices should be managed as part of a plan that includes goals, milestones, and metrics.

Core Issues of Wireless Device Management

An independent research group recently estimated that the average annual total cost of ownership (TCO) for wireless devices is between \$2,500 and \$3,000 per device*, per year. Multiply that cost across any multi-site enterprise, and the impact on supply chain management and IT costs can be dramatic.

There's also a significant risk of these costs going up. Consider the experience of one major North American manufacturer: Their wireless device platform inventory listed 900 units; after three years, 250 of the devices – close to 30%! – are unaccounted for.

However, the potential savings from the proper wireless device management approach can also be dramatic: from 10% to 15% of TCO, with a potential return of \$150 to \$250 per device.

Effective wireless device management should provide an integrated process and a range of implementation options to match business requirements. There are several core issues that every management plan should address:

Device application lock-down and security

This is both an inventory and security issue. The newest generation of devices and management tools allow for preset shutdown

* Gartner Group / researchportal.com

and disabling of devices that have gone off-network or have been inactive for a period of time.

Defining these presets, so that devices can be available when needed yet controlled so as not to provide a security risk, must be based on specific operational requirements that can vary between locations and specific business applications.

Device programming and application control

Most wireless devices are task- and application- specific, so it would seem that this should be a once-and-done concern. However, there are ongoing cost and productivity issues that must be addressed through proper configuration management.

Consider what appears to be a simple issue: a malfunctioning handheld terminal. The end-user in the warehouse isn't trained or expected to solve the problem; he reports the unit is not working and gets a replacement. The faulty device is covered under a service contract – although shipping to and from the repair facility may not be covered. Often, a faulty device is shipped back and forth multiple times; the repair facility finds no problems, yet the end users are repeatedly unable to get the tool to work. Why? Because the issue isn't equipment failure – it's incompatible, faulty or outdated configuration. Yet the costs – of shipping, of unavailable tools, of increased spare device pools to cover this contingency – can all be avoided.

It means adopting an organized, rigorous approach to device management – at startup and through the device lifecycle – that either eliminates these issues or provides fast paths

for identifying and solving problems.

Remote device tracking

One of the reasons wireless device TCO is so inflated is how easy they are to lose. Until recently, this kind of inventory issue was not on an IT manager's radar; except for laptops, most IT assets were fixed in place.

Consider the experience of one major North American manufacturer: Their wireless device platform inventory listed 900 units; after three years, 250 of the devices – close to 30%! – are unaccounted for.

Fortunately, the latest generation of devices provides highly effective firmware and Web tools that make managing this issue much easier. It means that a centralized device management tool can query all the locations of a wireless network and track down the errant device – which is a lot faster and much less expensive than having someone retrace their steps throughout a facility to the last place they *remember* having it.

It's important to pay attention to this issue, and make certain that device suppliers and management system vendors have fully incorporated device discovery into their offerings; in addition, these capabilities need to match the range of operating conditions in your supply chain (mobile, single-site, etc.).

Platform asset management and reporting

This device management task is similar to standard IT management responsibilities. It includes device inventory, firmware and applications version tracking, management of updates, and security controls. There are continuing advances in software tools for this task.

It's important to ensure that you understand the scope of asset and resource reporting requirements you're likely to need, as you deploy a new wireless system or upgrade and/or integrate current platforms.

Support tools and systems

Given the unique nature and operating characteristics of wireless devices and platforms, it is very common to develop dedicated IT and Help Desk resources, distinct from the rest of your IT support platform.

The typical scope of support responsibility includes monitoring device health and remote troubleshooting, software and settings reconfiguration and updating, control and monitoring of information flow across the platform, and remote operation and control of devices.

Specialized software tools, training, and management processes are necessary. It can be very costly and counterproductive to just drop responsibility for the wireless platform onto existing support resources – especially when time, budget and trained personnel are at a premium.

The best wireless device management solutions recognize and address these essential elements. To be effective, device management must be organized and integrated into larger enterprise-wide IT processes, and scaled to your operation's size, applications requirements, and financial objectives.

Deciding on the best approach to device management, given these complex issues, calls for a sophisticated insight into how your business uses its wireless platform for strategic advantage, and what level of

investment your business can afford to ensure that it continues to offer that value.

Strategic Approaches to Implementing Device Management

There are three basic approaches to device management. Choosing the best approach is driven by factors such as the scope of wireless usage in your business, and the resources and expenditures (training, certification, diagnostic tools, etc.) you are willing to commit to manage them effectively.

Stand-alone, tool-based management:

This is the simplest approach, and one that can be implemented relatively quickly. It assumes that a device management tool can be deployed to handle all the major management tasks, with an easy-to-use interface.

This approach is best suited to operations with 1-2 locations, and a low number of devices and wireless applications to be managed. It also assumes you have the IT resources available to train and be available for this additional responsibility. There are a number of these platforms available; each has its relative advantages and limitations.

Choosing the right tool can be a challenge. It's important to remember that, in this scenario, you assume full responsibility for keeping the management platform and training up to date and properly supported to handle all help desk, configuration, inventory management, and repair issues.

Combination in-house/outsourced management:

For several operations, there are strategic and practical benefits from combining in-house resources and platforms

with third-party support. Basic, Tier One services can be handled in-house, since the training and support needs for this initial level are not very demanding.

No matter what approach you choose – tool-based, combination, or full outsourcing – you can expect to generate savings and efficiencies in multiple areas.

More complex, Tier Two and Three responsibilities can be assumed by dedicated third-party vendors with in-depth expertise managing wireless platforms. The development of sophisticated remote operating platforms in end-user devices means it is now possible to have all major device management tasks, at all three levels of support, managed cost-effectively.

Diagnostics, troubleshooting, configuration management, updates, and inventory tracking across multiple sites is now much easier, and more full-featured, eliminating the need for live support resources at every location.

The best third-party vendors in this scenario are ones with a demonstrated competence in wireless platform management, including the understanding of protocols, regulatory issues, security management, and the key drivers associated with making sure your wireless technology provides the uptime, productivity and return on investment that you expect.

Full Outsourcing: Many companies with enterprise wireless platforms, consisting of multiple sites and a sizable number of wireless devices, are finding a major strategic advantage from completely outsourcing their device management tasks.

There are key operational and financial drivers that help justify this approach. In several situations, the mission-critical value of the wireless platform is extremely high; IT management may conclude that building and sustaining the level of competence necessary to ensure that this value is maintained is too costly and time-consuming.

From an operational perspective, counting on a dedicated outsourced resource tasked solely with managing the platform can free IT management to focus on broad, enterprise wide strategic issues that are core to their daily job functions and business. While some companies may be concerned about the risk associated with turning this vital function over to outsiders, industry experience has shown that device uptime, operator productivity, inventory control and other cost drivers can often be more effectively managed, especially for large operations, through outsourcing.

This approach also provides a level of wireless-specific expertise that can take too long, and cost too much, to develop and maintain in-house. Financial criteria may be critical: the capital investment required to specify, implement and support an extensive, multi-tier device management solution can be significant; alternatively, outsourcing the operation as an ongoing expense can be cost-justified more easily and scale to more directly match your needs and timing.

Device Management: Bottom-line Benefits

Effective, well-organized wireless device management promises significant reductions in the TCO of wireless devices and platforms. It also can help increase uptime and productivity of wireless supply chain operations, and enhance operator efficiency and user experience.

No matter what approach you choose – tool-based, combination, or full outsourcing – you can expect to generate savings and efficiencies in multiple areas. There are both immediate and long-term ways total cost of ownership will be reduced:

- **Fewer spares** – better diagnosis, remote connectivity and monitoring, automated software provisioning, all enable you to have more devices up and running, so your pool of spare/back-up devices per location can be kept to a minimum;
- **Lower shipping costs** – shipping costs between user locations and repair shops for repair/replacement purposes can be much better controlled through remote management, better software maintenance, and other proactive device management steps;
- **Reduced IT support requirements** – with remote access and outsourced support, you may be able to eliminate most site-by-site IT support demands, during wireless application start-up and on an ongoing basis;
- **Improved asset management** – with the right tools and procedures in place, device inventory loss can be much better controlled, keeping replacement costs down;
- **Reduced provisioning costs** – device application software and security

software, updated overnight remotely, makes keeping devices current and fully functional a simple, low-cost activity;

- **Lower software license fees** – by keeping spare pools to a minimum and exercising better device inventory management, fewer device software licenses are needed.

You can improve operational productivity – and as a result, ROI – with a complete, well-designed device management solution. Proactive system monitoring and standard imaging for devices will help you identify and correct defective devices faster, and can practically eliminate “no-defect-found” events that consume valuable time and keep devices out of service.

The right device management plan can help your operation run more smoothly – by enhancing the operator experience. Remote training (automated/interactive modules and live online sessions), expertly designed training tools and device documentation (with screen grabs and live screens from actual devices and subsystems) can dramatically improve operator efficiency and enhance their daily work practices.

Remote, real-time problem resolution through online systems helps operators in multiple locations feel fully supported, and makes it easier and more productive for them to report problems or issues, because they can get them quickly resolved.

About PEAK Technologies

PEAK Technologies, a Platinum Equity Company, is a systems integrator of supply chain automation and inventory management solutions delivering tangible return on investment to some of the world's largest corporations. PEAK's primary applications include solutions for warehousing, manufacturing, and distribution operations. PEAK's portfolio of solutions and services include business process consulting, enterprise resource planning (ERP) systems integration, wireless professional services, project management, printing/media solutions, and life-cycle support services. PEAK Technologies has locations throughout North America providing a comprehensive "foot print" for national, multi-site life cycle service and support.