



**Practical IT Research that Drives Measurable Results**

Understand and Develop a Mobile Management Strategy

Rein in the Mobile Fleet to Ensure Enterprise Security, Productivity, and Appropriate Use of Network Resources

# Introduction

- Mobile device usage is outpacing traditional forms of computing such as desktop and laptop devices, surpassing them by 2013.
- Info-Tech research shows up to 30% of mobile devices are lost or stolen along with their corporate data and intellectual property.
- Info-Tech estimates that deployment and ownership of a mobile device costs a minimum of \$2740 over three years, excluding long distance and roaming charges.
- Management tools and policies are still in the development phase and don't necessarily integrate well with other enterprise system management tools.
- This solution set will help your enterprise create strategies and policies to manage mobile device growth, risk and costs in the most effective way.

Understand Mobile  
Device Management

Mobile Device  
Management  
Solutions

Real World Examples

Arrive at a Strategy

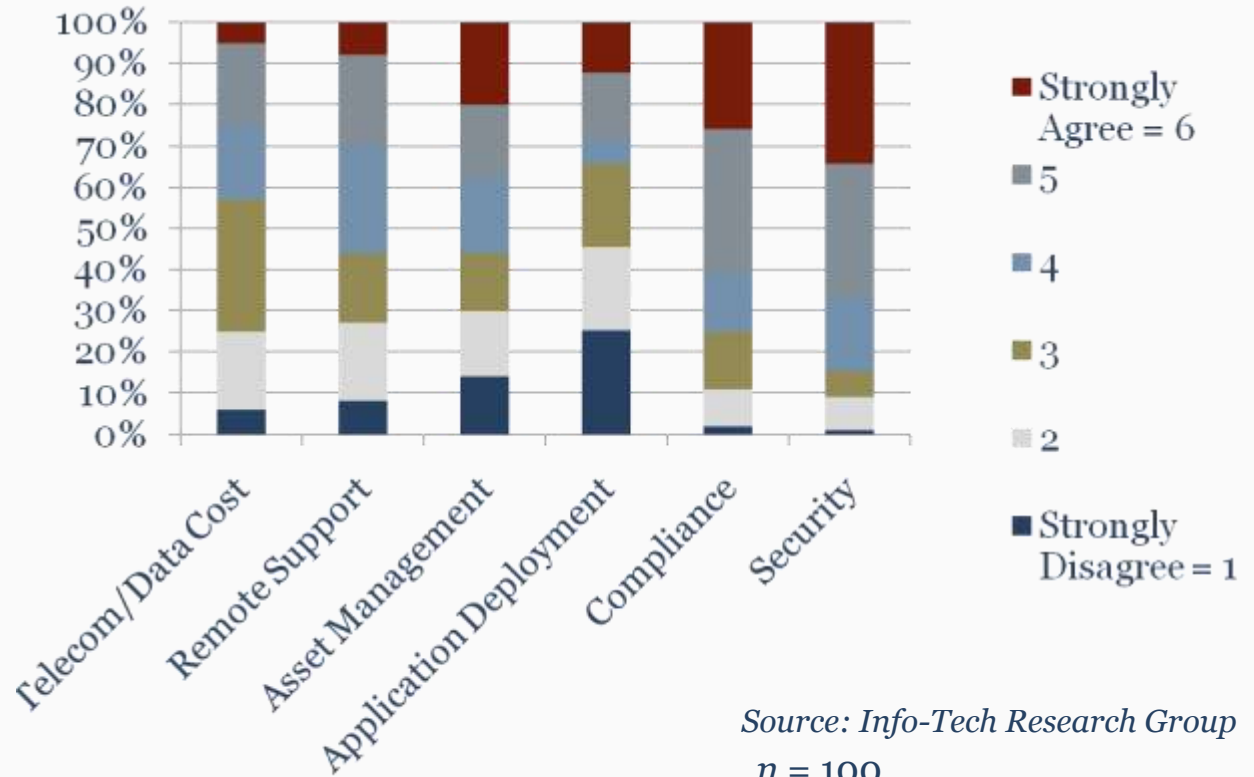
# Executive Summary

- IT leader interviews revealed that the real benefit of mobile devices is in deploying key enterprise applications as part of an overall mobile strategy
- 58% of IT leaders are dissatisfied with their mobile device management success, particularly security
- Mobile device management creates cost savings that grow with the fleet
- Saving big on mobile device voice and data costs, the biggest mobile device expense, is as simple as switching to an individual liability policy
- Mobile device security must be rigorously managed. Just because you can't see them doesn't mean the security breach won't hurt.
- Mobile device data backup and recovery is not a requirement with always on connectivity and synchronization
- Management functionality included in the email delivery platform (i.e. Blackberry Enterprise Server (BES) or Microsoft Exchange ActiveSync) is “good enough” for most enterprises
- Outsourcing mobile device management is off the table for enterprises with less than 500 devices
- Design and communicate mobile device support processes or face dissatisfied users, some of which will be senior management

# 58% of IT Leaders are Dissatisfied with their Mobile Device Telecom Cost Management

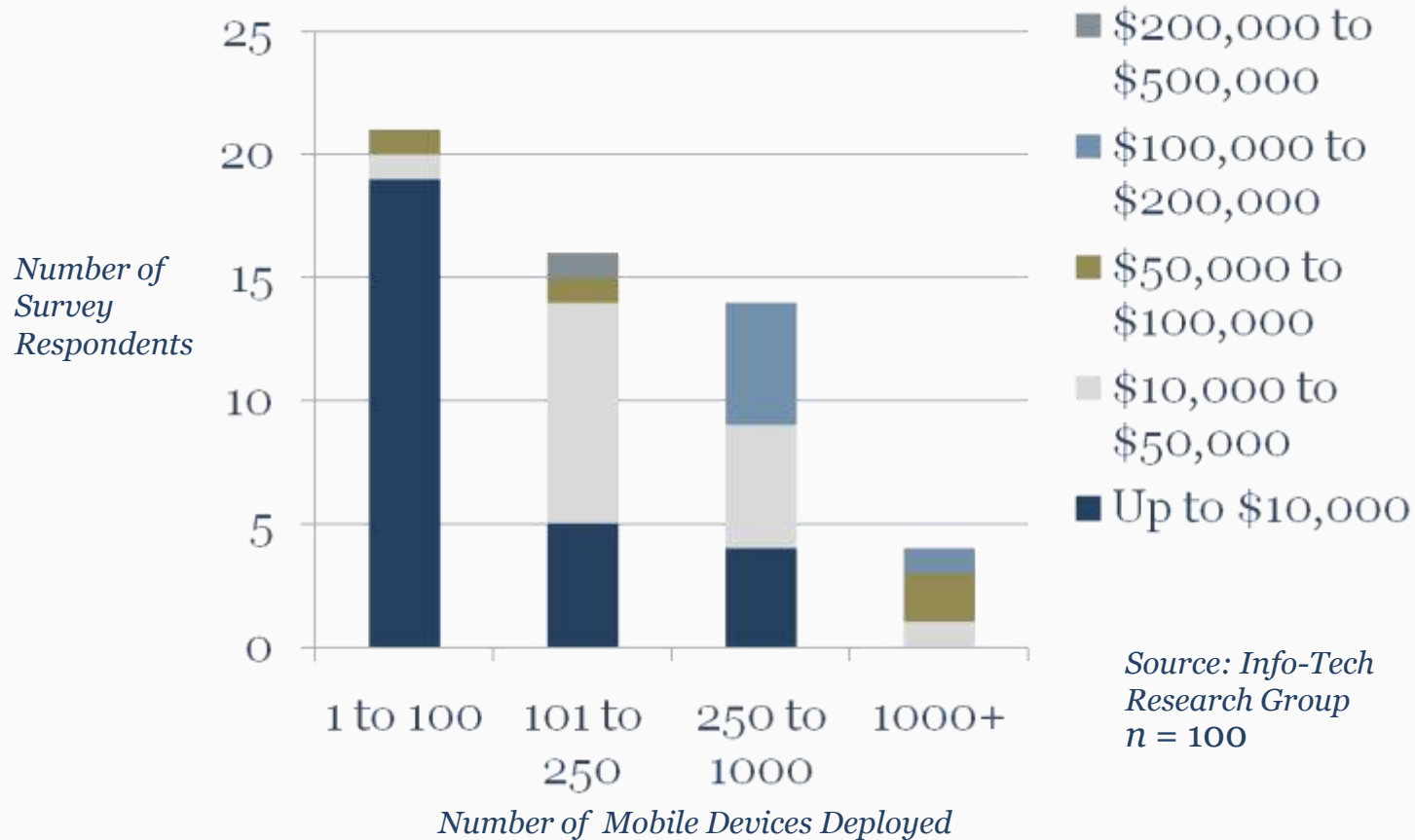
*Satisfaction with telecom and data cost managements lags while security and compliance success is high.*

Success Factors Measured
<b>Security</b> - Never had a serious mobile device security breach?
<b>Compliance</b> - Avoided issues passing compliance and regulatory audits?
<b>Application Deployment</b> - Are able to deploy mobile applications and updates over the air in less than 24 hours?
<b>Asset Management</b> - Can identify all mobile device assets, who has them and where they are?
<b>Remote Support</b> - Are able to provide remote support for corporate application users?
<b>Telecom and Data Cost Minimization</b> - Have the lowest possible telecom and data costs?



# Mobile Device Management Creates Ongoing Cost Savings that Grow with the Fleet

*62% of Info-Tech survey respondents indicated that they had ongoing cost savings stemming from managing their mobile fleet, exclusive of telecom and data costs.*



*Source: Info-Tech Research Group  
n = 100*

# Saving Big on Mobile Device Voice and Data Costs is as Simple as Switching to an Individual Liability Policy

*IT leaders are leaving money on the table by not getting out of the cell phone business.*

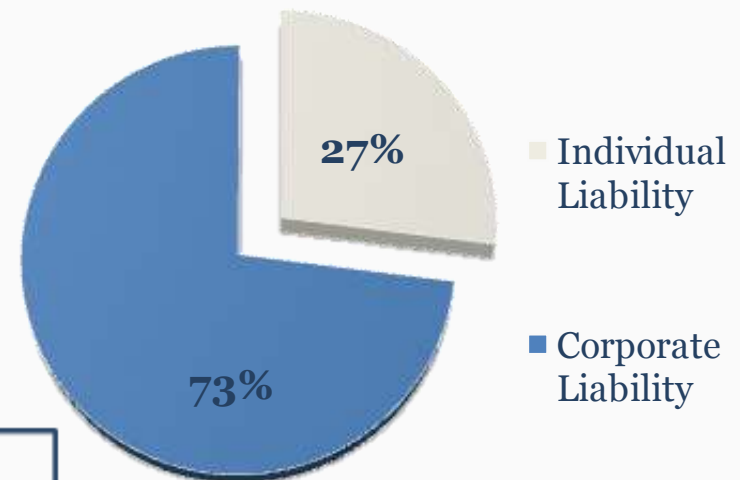
- While 73% of enterprises surveyed are still issuing cell phones, Info-Tech recommends individual liability is the best way to reduce costs
- Only 39% of enterprises Info-Tech surveyed have a corporate application deployed, one of the key factors in opting to issue a mobile device or cell phone
- Other criteria that may dictate a corporate liability policy, such as security and compliance needs or roaming costs, play a role but for most organizations it's time to reevaluate the need to continue issuing corporate devices

## *Info-Tech Recommends:*

### *Individually Liable Cell Phone Policy*

- 1) Users acquire their own device and plan.*
- 2) The business reimburses a capped expense amount monthly.*
- 3) Minimum security requirements are a prerequisite.*

**Among respondents who have no corporate applications deployed, 73% are using a corporate liability model.**



*Source: Info-Tech Research Group*

*n = 101*

# Proactively Manage your Mobile Fleet to Minimize Risk, Cost, Downtime, Audit and Data Loss Pain.

*Apple iPhone, RIM Blackberry, Google Android, Microsoft Windows Mobile (Windows Phone), Nokia, Palm/HP webOS and Symbian all need some form of proactive management.*

Objective	Methodology
Risk Minimization	Corporate data and security, backup and restore capability
Cost Minimization	Telecom and data communication expense management
IT Cost Minimization	Software deployment and maintenance
Downtime Minimization	Remote support
Audit and Data Loss Controls	Device lifecycle management, asset management, error and log management

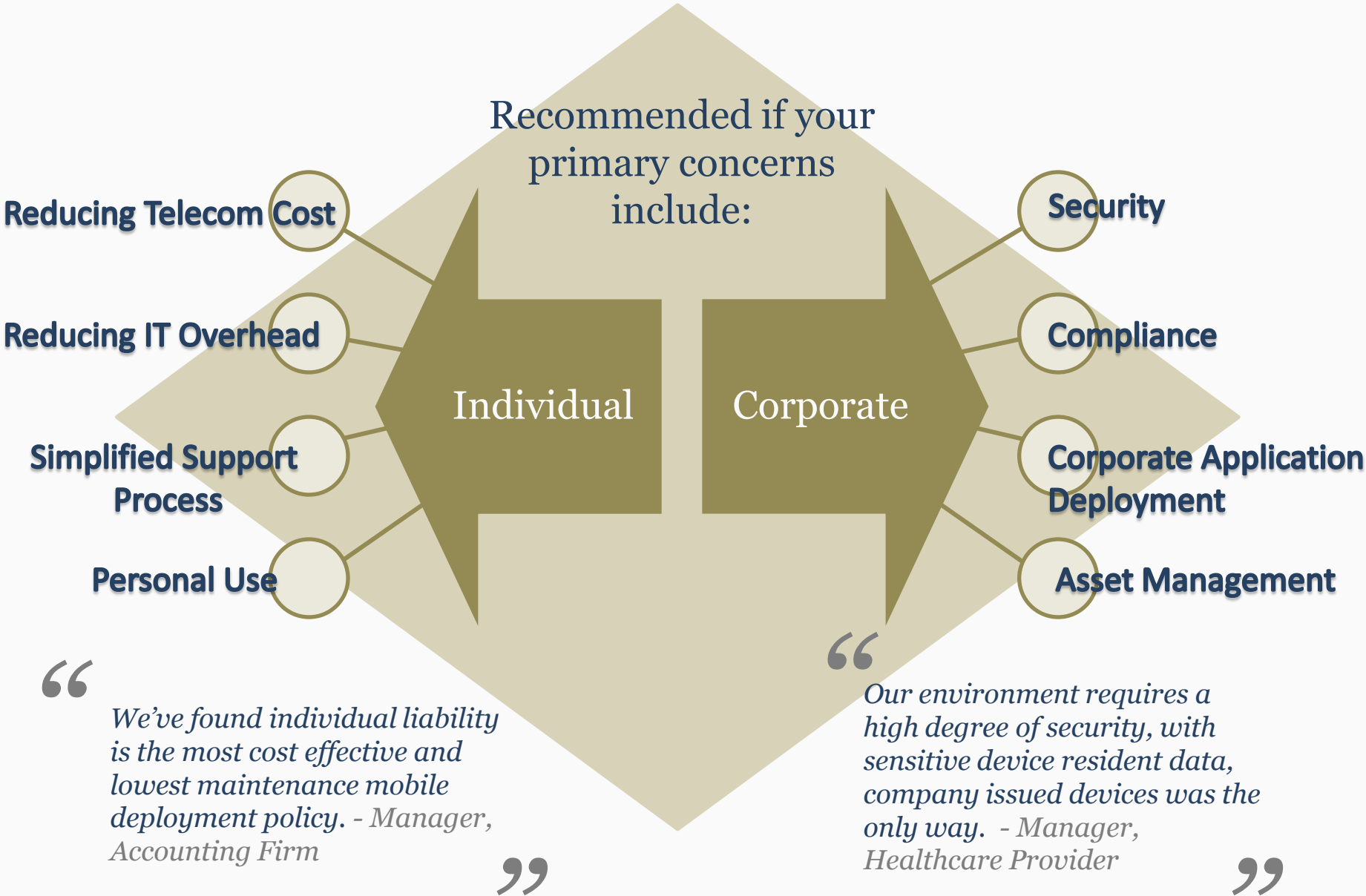
## *Info-Tech Insight:*

*Don't ignore those "non-smart phones". Simple cell phones, "Aircards" and tablet computers with cellular capabilities will need to be included in your management plan.*

# Mobile Device Management Roadmap

Understand Mobile Device Management	Corporate or Individual Liability		Mobile Device Management	Policies and Standards	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing	
Real World Examples	Small Enterprise		Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment			Strategy	

# Corporate vs Individual Liability - Which is Best for You?



# Making Users Responsible for Mobile Device Expenses Reduces Direct Costs.

- 1 Users acquire their own device and plan.
  - Users acquire either a plan and device of their own choosing or a plan and device recommended by IT. Any phone number used in a corporate context becomes company property.
- 2 The business reimburses a capped expense amount monthly.
  - IT leaders interviewed by Info-Tech indicated that they capped expense reimbursement for non-management staff at \$65 to \$80 per month and managers at \$95 to \$125 per month.
- 3 Minimum security requirements are a prerequisite.
  - Employees must agree to the following policies:
    - **Personal Identification Number(PIN).** Users will be required to have their phone's locked with a PIN. Ten incorrect PIN entries will wipe the device.
    - **Remote Wipe.** Users must agree that if they leave the company or lose their device, IT will remotely wipe out the content of the device.
    - **Encryption.** All or part of the data communicated and stored on the device must be encrypted.

## Individual Liability Mobile Policy

Pros	Cons
<ul style="list-style-type: none"> <li>• Reduces direct costs</li> <li>• Minimizes management costs with less IT oversight required</li> <li>• Sidesteps any taxable benefit issues</li> </ul>	<ul style="list-style-type: none"> <li>• Deploying corporate applications becomes difficult or impossible without operating system standardization</li> <li>• Employees control what other applications live on their devices, a potential security risk</li> </ul>

An Individual Liability Mobile Policy will be ineffective in environments where :

- Extensive roaming or timely communication is required or expected.
- Dedicated devices for warehouse or delivery staff are required.
- Compliance needs override cost concerns.

### *Info-Tech Insight:*

*Enterprises have been held accountable for cellphones as a taxable benefit. Understand tax policies for individual and corporate cellphones, i.e. [IRS - Employee Cellphones](#).*

# Education, Transportation, Utilities and Government are Leading the Individual Liability Charge

*Individual liability cell phone policy is gaining ground with cost conscious enterprises dominated by information workers.*

Some industries will naturally gravitate to corporate mobile devices for a variety of reasons:

- Specialized devices such as barcode, RFID or meter readers are impractical for individual liability
- Other factors such as timely communications, on-call, high mobility or extensive travel may warrant a corporately provided cell phone.
- In industries where IT resources are at a premium, cost is a significant concern, and information workers dominate, individual liability will flourish.

“

*We're seeing much greater adoption of individual liability mobile policy to reduce cost and stabilize monthly bills. - Manager, Mobile Device Manufacturer*

”



Source: Info-Tech Research Group  
n = 101

# Minimize Pain by Planning the conversion to Individual Liability Mobile Policy

## Communicate Usage and Administrative Policy

- Clearly communicate cell phone usage and reimbursement policies.

## Define Reimbursement Processes

- Leverage existing expense reimbursement processes and make modifications where necessary to handle cell phone policy.

## Consider Creating Loaner Phones

- Formerly corporate cell phones make excellent loaners for staff when unusual situations arise, such as international travel.

## Establish a Conversion Process

- Allow workers to assume responsibility for the phone, the plan, and the cell phone number. Some employees may prefer to retain their cellular phone number. Work with the cellular provider to create a process that transfers ownership from the company to the employee.
- Have a realistic timeline for completion. Be aware that workers will need at least four weeks to absorb the impact of this change, investigate cellular plans, and execute the administrative transfer.
- Provide for the disposal of turned-in cell phone equipment. Contact the cellular provider for the organization to arrange for the donation of working equipment to a local charity or other relief organization. Ensure that all data is completely erased from the devices prior to disposal.

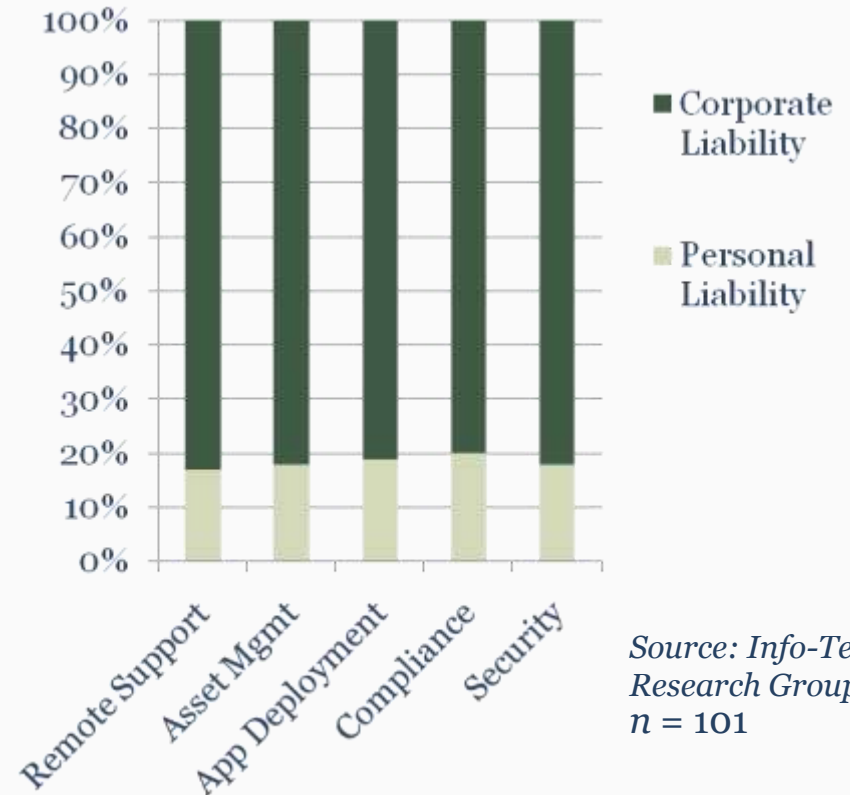
# Corporate Liability Policy Breeds Success by Meeting Security and Compliance Requirements

*Remote support, asset management and application deployment also benefit from a corporate liability policy.*

## Corporate Liability Mobile Policy When:

- Compliance requirements, to ensure the security of personal information, require robust encryption and logging that isn't possible with employee owned devices
- Corporate liability funding model produces a higher success rate in the following areas:
  - Remote Support
  - Asset Management
  - Corporate Application Deployment
  - Compliance
  - Security
- If these are among your primary concerns, choose corporate liability. Otherwise, it creates unnecessary overhead which can be eliminated with an Individual Liability model.

Companies choosing a Corporate Liability Funding Model were more successful in areas such as security and compliance



Source: Info-Tech Research Group  
n = 101

# Mobile Device Management Roadmap

Understand Mobile Device Management	Corporate or Individual Liability		Mobile Device Management	Policies and Standards	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing	
Real World Examples	Small Enterprise		Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment			Strategy	

# Understand key mobile device management needs and capabilities to develop an effective policy.

*Apply enough management to get the job done without overspending.*

Objective	Methodology
Risk Minimization	Corporate data and security, backup and restore capability
Cost Minimization	Telecom and data communication expense management
IT Cost Minimization	Software deployment and maintenance
Downtime Minimization	Remote Support
Audit and Data Loss Controls	Device lifecycle management, asset management, error and log management

# The Most Important Part of Mobile Device Security is an Educated User

*Without security policies, it's the wild west for your mobile device.*

## Build/Activate Mobile Security Policy

A clear and comprehensive mobile security policy is the foundation for driving more responsible usage. This document should explain all employee responsibilities and work expectations and include clear statements about the roles of users, management, and security staff in upholding the enterprise mobile security policy. Use Info-Tech publications and templates to speed policy development:

- [Mobile Device Acceptable Use Policy](#)
- [Mobile Policy: Enterprise and User Responsibilities](#)
- [Mobile Policy: Security from a Data Perspective](#)
- [Mobile Policy: Enforcement Is a Key Component](#)

## Assemble Security Awareness Training

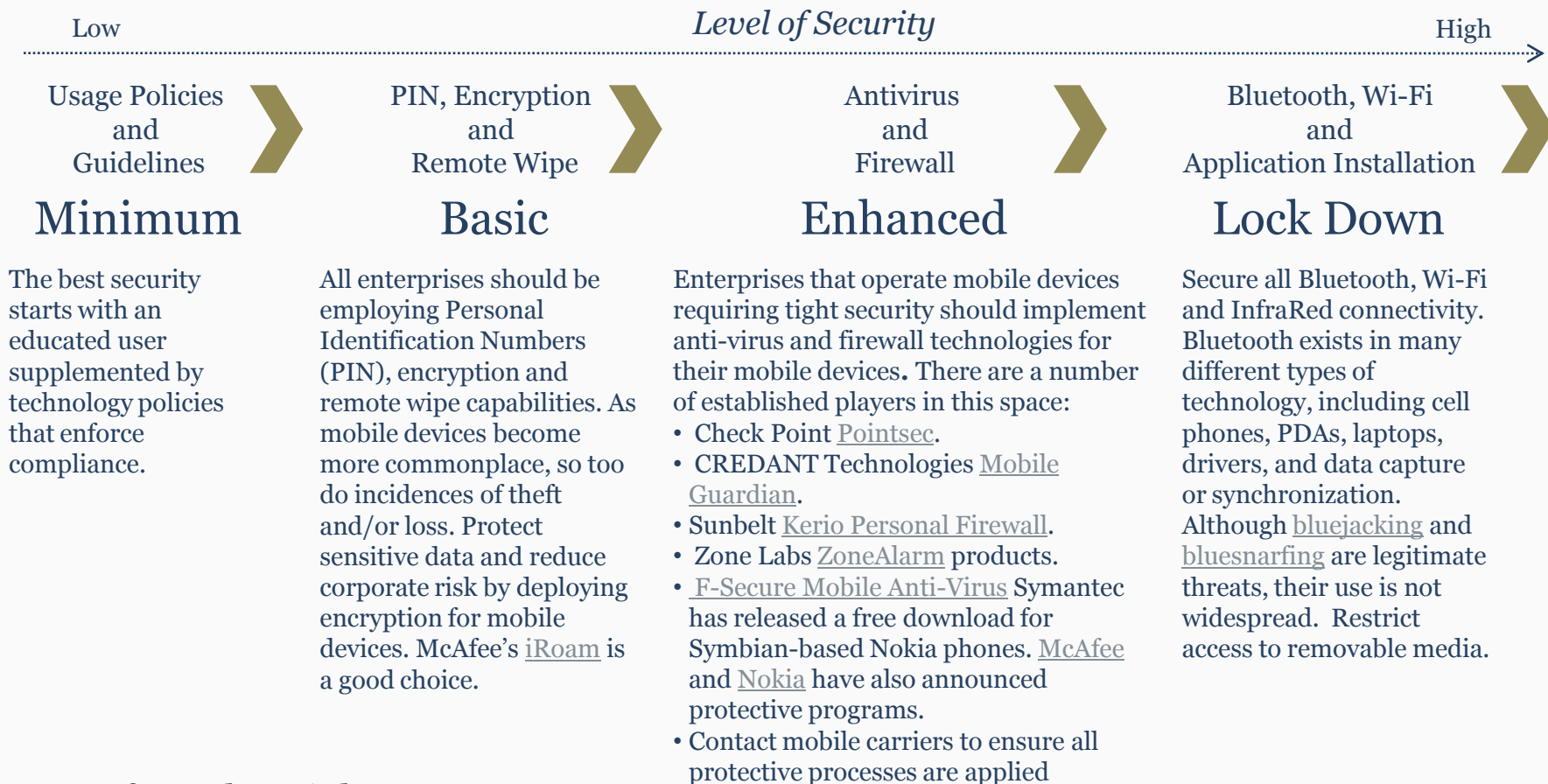
Organizing and scheduling formal training sessions for enterprise users entrusted with mobile capabilities is essential to raise awareness and understanding of the corporate mobile security policy. Users will also need to receive specific instruction on the course of action they are expected to take in the event that a device is lost or stolen. Useful resources for building a training plan include:

- [Mandate Security Training to Safeguard Your Mobile Fleet](#)
- [Special Publication 800-50 – Building an Information Technology Security Awareness and Training Program from NIST.](#)
- [Security Awareness Training](#) resources from the SANS Institute.
- The Microsoft TechNet [Security Awareness Program Tool Kit and Guide.](#)



# Mobile Devices Are an Extension of Your Network Beyond The Corporate Shields

*Just because you can't see them doesn't mean the security breach won't hurt.*



## *Info-Tech Insight:*

*Beware of devices, such as the [Nexus One](#), that can be turned into Wi-Fi Hotspots, creating a potential security risk.*

# Evaluate data backup requirements before determining a mobile device backup and recovery strategy.

*In most cases mobile device backup and recovery is not a requirement since important data is already stored and backed up on the corporate infrastructure.*

- Mobile devices are being used more and more as primary end-user computers. Many devices are always on, connected to the network and internet and synchronized with data sources, negating the need for backup.
- For those devices that are not always on, ensure complete business continuity by enforcing proper backup and by clearly defining backup roles and responsibilities for both IT and end users.
- The problem is that these mobile devices are frequently disconnected from the corporate LAN, meaning that scheduled network backups are impossible.
- Some users feel that occasional synchronization of the mobile device with their office desktop PC provides enough data redundancy to offset any risks. If the user's device should fail, become lost, or is stolen while on the road without a backup having been conducted, that information will become irretrievably lost.
- It is very easy for someone to ignore backups, especially if it is an informal or voluntary requirement. A mobile backup strategy is more than an IT issue: understand specific needs of mobile users and choose the right strategy for the enterprise



## *Info-Tech Insight:*

*Many users will only use email, contacts and calendaring which is typically synchronized to a server on a regular basis, negating the need for backup.*

# Look before Leaping on a Mobile Device Backup Solution to Avoid Unnecessary Cost

*If backup is required, get to the right solution by assessing needs first.*

Assess Risk	Create a Clearly Defined Policy	Determine the Appropriate Backup Frequency	Make Provisions for Heavy Mobile Device Users
<ul style="list-style-type: none"><li>• Determine if the data on a cell phone is mission critical. (e.g., contact lists are not critical). However, devices containing any of the following should be backed up:<ul style="list-style-type: none"><li>• Client lists, including sales figures and other sales activity.</li><li>• ERP mobile editions.</li><li>• CRM mobile editions.</li><li>• Employee/personnel records.</li><li>• Patient files (healthcare only).</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Put in place rules and guidelines to solidify commitment from the entire enterprise, even if this means disciplinary action.</li><li>• Teach users to perform backups by walking them through the process, focusing on making this an easy process. If it's too complicated, users will avoid backing up.</li></ul>	<ul style="list-style-type: none"><li>• Incremental backups:<ul style="list-style-type: none"><li>• Not time-consuming, and can be performed on the road with relative ease.</li><li>• Perform incremental backups nightly.</li></ul></li><li>• Full backups:<ul style="list-style-type: none"><li>• Due to sheer amount of data involved, perform full backups at the office.</li><li>• Perform full mobile backups as often as the enterprise typically runs full backups (e.g. monthly, weekly, etc.).</li><li>• However, if users are on the road for extended periods of time, conduct a full backup when they return to the office.</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Cell phones and smart phones can be synchronized with PCs every night, but this is a manual process that is prone to error.</li><li>• Use specialized point solutions to assist in backup procedures for phone contacts, email, and other data.</li></ul>

## *Info-Tech Insight:*

*If mobile device backup is required for an offline device, automate the process to ensure compliance and data security.*

# The Biggest Cost of Operating a Mobile Device Fleet is Voice and Data Communications Connectivity

*If issuing mobile devices is necessary, usage policy and plan selection are the places to start saving.*

## Enforce Cellular Usage Policy

- Actively manage and enforce cellular phone policies to gain immediate and future cost savings.
- Cellular usage policies establish rules for company-issued phones (e.g., who qualifies and usage guidelines) and personal phones used for business (e.g., reimbursement practices).
- Policies protect companies from legal matters concerning cellular phone use and from employees that abuse their phone privileges. For a sample cell phone policy, use the Info-Tech “[Mobile Device Acceptable Use Policy](#).”

## Choose the Best Plans for Employee Needs

- A one-size-fits-all plan is not cost effective, since this can result in many employees with a higher usage plan than needed. At the same time, a separate plan for each employee would be an administrative nightmare.
- Instead, identify light, heavy, and international cell phone users and put each group on an appropriate plan for their needs. Periodically review employee usage to ensure they are in the right group.
- For light cell phone users, a shared minutes plan is generally the cheapest alternative.
- For heavy domestic cell phone users, unlimited voice and data plans such as the \$99.99 plans released in early 2008 by the big four North American wireless carriers are suitable. An unlimited plan makes it easier to forecast costs and simplify bill auditing. For more information, refer to the Info-Tech research note, “[All You Can Eat Wireless Plans to Invade North America](#).”
- For employees who travel abroad, long distance, data and roaming charges can be costly. The following measures can result in savings of 30%-50%. These include:
  - Negotiating plans with international coverage; best for high level executives.
  - Switching SIMcards to ones supported by foreign carriers when travelling; best for frequent travelers.
  - Using company rental phones supported by foreign carriers; appropriate for infrequent travelers.

# Device Selection Can Impact Support and Operational Costs

*Standardized devices that deliver on the business need while minimizing connectivity requirements further trim costs.*

## Standardize Cellular Devices

- The cellular phones used in a company and supported by the help desk should be standardized. While standardization may be difficult to enforce with employees such as high level executives, IT departments should make an effort to standardize cellular devices. Standardizing company cellular devices serves two main benefits:
  - Makes the management of mobile devices easier and requires lower support costs. “Rogue devices,” ones that are not supported by the company help desk, can result in unnecessary employee downtime, and costly security and technical issues.
  - Standardizing cellular devices allows the IT department to assign phones with the necessary functionality to employees. Extra functionality usually results in extra and unnecessary costs.

## Consider Other Mobile Options

- Viable alternatives to traditional cellular phones are available. For mobile or teleworking employees who use laptops to perform most of their work, IP softphones may be a good alternative. These are PC applications that act like fully functional IP phones and are accessible through USB headsets or handsets. IP softphones are available for a fraction of the price of regular IP phones, costing less than \$100 per seat.
- Another alternative is exploring the availability and viability of Fixed Mobile Convergence (FMC). These phones can seamlessly switch from a network carrier, to a network hotspot, to a home or office wireless LAN. This allows IT departments to reduce mobile costs since users that spend a lot of time in multiple company offices can make calls through the wireless connections, not the network carrier. For more information on fixed mobile convergence, refer to the Info-Tech research note, “[Divitas Brings Mobile-to-Mobile Convergence to the Enterprise.](#)”

### *Info-Tech Insight:*

*Consider reducing mobile voice and data costs by configuring in-office Wi-Fi connectivity for users that are often in the office. For those users who don't need offsite connectivity, issue Wi-Fi only devices. i.e. iPod Touch versus iPhone*

# Telecommunications providers will not go out of their way to save you money.

*There's gold in those cellular phone bills! Mining for it will yield big returns.*

## Implement Telecom Expense Management(TEM)

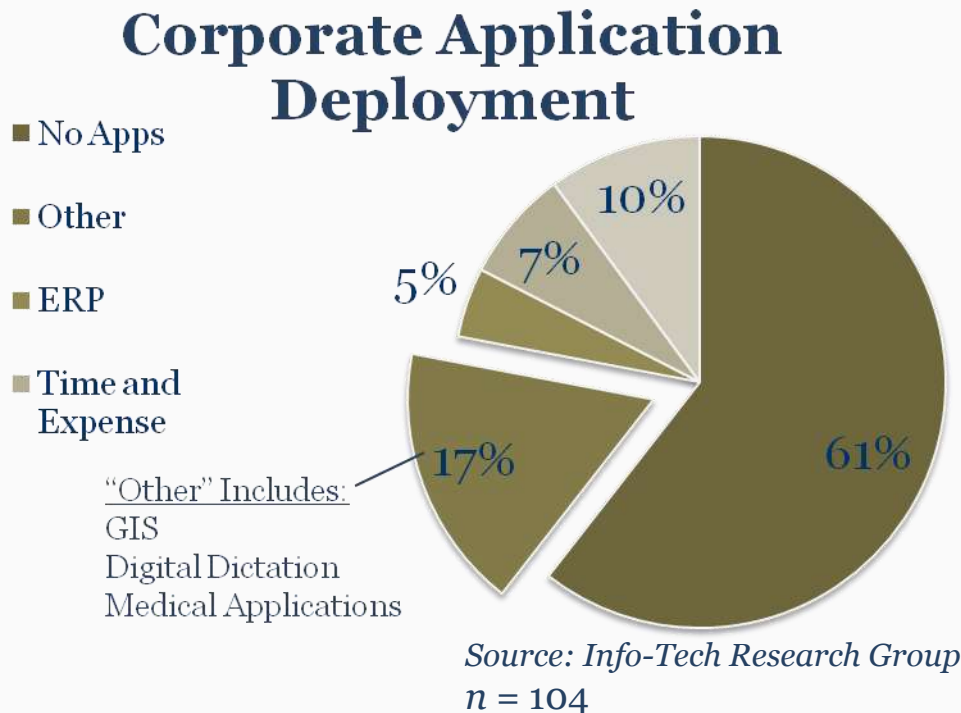
- IT departments should perform regular audits of cellular phone bills. The regular analysis of bills is an important step in Telecommunications Expense Management (TEM). Auditing bills can uncover:
  - Overbilling.
  - Unused and unnecessary services.
  - Abuse of company phones by employees.
  - Usage trends.
- TEM is the practice of actively managing a company's telecom requirements in order to reduce cellular phone costs. If a company wants a low risk way of testing TEM, the easiest and cheapest alternative is to hire a TEM service provider to perform an audit of all billing records. These companies are generally paid a percentage of the savings found and boast recovered savings of up to 50% of the annual cellular phone costs. Companies that offer TEM services include [Auditel, Inc.](#), [Advantage IQ](#), [ISI Telemanagement Solutions, Inc.](#), [Profit Enhancement Services](#) and [Rainbow Information Systems](#).
- For companies that prefer to perform their cell phone audits in-house, there is TEM software available. Vendors offering TEM software solutions include [AnchorPoint](#) , [Integrated Mobile](#) , [Invoice Insight](#) , [Rivermine](#), [Tangoe](#) and [mindWireless](#).
- In large companies with multiple departments, cellular phone bills are usually paid by individual departments. In order to keep the cellular billing centrally managed, bills should be put into TEM software before being paid.

“ *After reviewing our cell phone deployment we saved \$1M per year in telecom costs by de-issuing devices, enforcing policy and consolidating plans. – IT Director, Software Company* ”

# 61% of Enterprises Have Not Deployed Corporate Applications on their Mobile Device Fleet

*For the 39% that do, management and support is critical.*

- Deploying mobile applications isn't easy, despite improved bandwidth and connection reliability
- Manufacturer management platforms offer some deployment capabilities
- Mobile application vendors often offer deployment mechanisms
- Third party tools offer the greatest degree of power and flexibility but at a greater cost



“*Companies need to develop a mobile strategy before figuring out how they will manage it.*

*Those organizations that have deployed a mobile application are reaping the greatest benefit from the technology.*

*- Manager, Mobile Device Manufacturer*

# Mobile Device Application Deployment is Getting Easier

*Advances in deploying consumer devices are accelerating applications deployment technology for the enterprise user.*

- Mobile device application deployment follows the same processes as traditional computing devices:
  - Deploy the applications or operating system upgrades
  - Provide updates and patches
  - Deploy new policies
  - Ensure applications are up to date
  - Ensure policy compliance
- In today's mobile society, software deployment is almost exclusively over-the-air(OTA) and done without user intervention
- Traditional application package deployments, i.e. .CAB etc., have matured and stabilized as IT gains experience with mobile technology
- Consumer-like methods of distributing and maintaining applications, i.e. iTunes, are getting attention from the enterprise



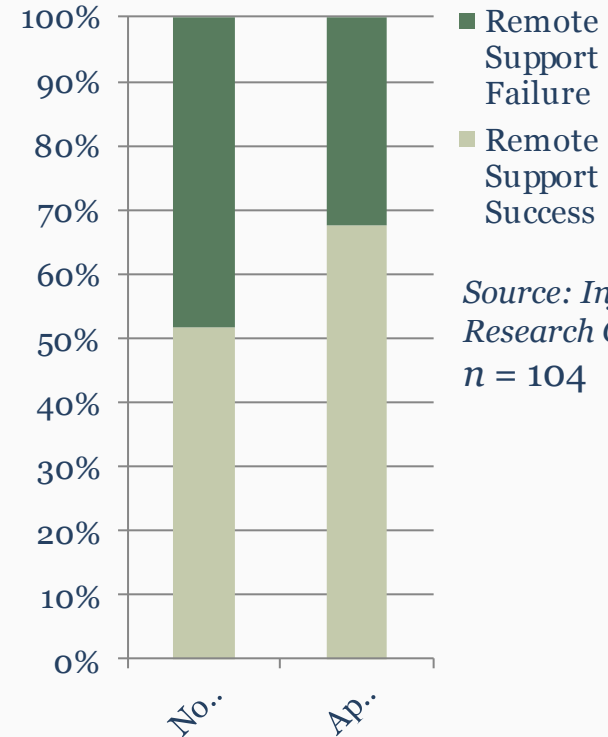
## *Info-Tech Insight:*

*The days of deploying mobile applications by tethering to a PC in the office are long gone. Users are not going to afford IT that luxury anymore.*

# Define Support Processes for Mobile Users, Particularly When a Corporate Application is Deployed

*Info-Tech survey respondents indicate that remote support success is greater for those with applications deployed but could be better.*

- 70% of Info-Tech survey respondents felt they were successful at providing remote support when a mobile application was deployed.
- Only 52% indicated they were providing adequate support in the absence of a mobile application.
- Individually liable users should get assistance from the help desk with email, contact and calendar update connectivity, all other support should reside with the carrier
- Corporately liable users, particularly when a mobile application is deployed, need to be supported by the help desk
- Communicate to the help desk and users how to effectively get support for their mobile needs



“ *Mobile devices are like laptops with hemorrhoids, you can support them but it's painful.*  
– IT Director, Software Company

”

# Manage your mobile hardware and software assets to save money and minimize data loss.

*While it seems like a chore, failing to manage your inventory means you can't track carrier plans or determine if a device has gone missing, increasing cost and risk.*

- Most applicable to corporately provided devices, but individually liable devices require a subset of asset management
- Allows easy identification of devices requiring vital operating system and manufacturer application updates reducing help desk load and improving audit and compliance processes
- Capture important mobile device information during initial provisioning:
  - Device ESN
  - SIM information if applicable
  - Phone number
  - Carrier and plan details and expiry
  - Device warranty coverage
- When a device is lost, carriers can quickly be provided the information necessary to shut down the device. IT can more quickly issue a remote wipe to remove any corporate data
- Provides a means of ensuring end-of-life devices have been properly disposed of, with sensitive data and applications removed



# Compliance and Reliability Requirements Drive the Need for Error and Log Management

*Don't get caught without mobile device traceability when the auditor comes calling.*

- Where audit and compliance requirements are rigorous, mobile device logs are a requirement to ensure a continuous audit path, should an issue occur
- Error logging also allows mobile device management to proactively detect a non-recoverable error and re-provision the device automatically
- Info-Tech survey respondents report a high degree of security and compliance success with their mobile fleet
- Automatically fixing mobile issues in the field may be critical to time sensitive processes.



# Mobile Device Management Roadmap

<b>Understand Mobile Device Management</b>	Corporate or Individual Liability	Mobile Device Management	<b>Policies and Standards</b>	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing
Real World Examples	Small Enterprise	Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment		Strategy	

# People and Technology Policies Make Mobile Management Work

*Technology can't defeat all the threats your mobile fleet will face but it helps.*

## **Technology Policy**

- 1** [Microsoft ActiveSync Policy Guidance](#)
- 2** [Understanding Exchange ActiveSync Mailbox Policies](#)
- 3** [RIM BES IT Policy](#)
- 4** [RIM BES Express IT Policy](#)

## **People Policy**

- 1** Refer to the Info-Tech “[Internet Acceptable Use Policy](#)” and “[Laptop Loan Policy](#)” templates, as well as the following sample policies published by the [SANS Institute](#):
  - [Personal Communications Devices and Voicemail Policy](#)
  - [Remote Access Policy](#)
- 2** Don't leave mobile devices unattended in vehicles, bags or jackets
- 3** Immediately report the loss or theft of a mobile device to IT and the carrier

### *Info-Tech Research Article:*

Use Info-Tech Research Group's "[Mobile Device Acceptable Use Policy](#)" template to fast track your policy creation.

# Mobile Device Management Roadmap

Understand Mobile Device Management	Corporate or Individual Liability	Mobile Device Management	Policies and Standards	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing
Real World Examples	Small Enterprise	Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment		Strategy	

# The Consumerization of Enterprise Mobility has Challenged IT's Ability to Manage these Devices

*Don't assume the manageability of a mobile device until you've evaluated its capabilities against your device management software.*

- Apple recognized this challenge to corporate adoption and introduced the iPhone v4 operating system with more enterprise management capabilities
- Google Android 2.2 (Froyo) operating system release now offers greater manageability for the corporate environment
- Windows Mobile 7 is a whole new platform so it remains to be seen how to manage it
- Previous versions of these operating systems did not effectively support the deployment of enterprise mobile policies and offered no management console errors or warnings when policies were not deployed



## *Info-Tech Insight:*

*Even though manufacturers will release newer versions of their operating systems with greater enterprise manageability, until they displace those devices currently available, you'll need to single out those older devices or face upgrading them.*

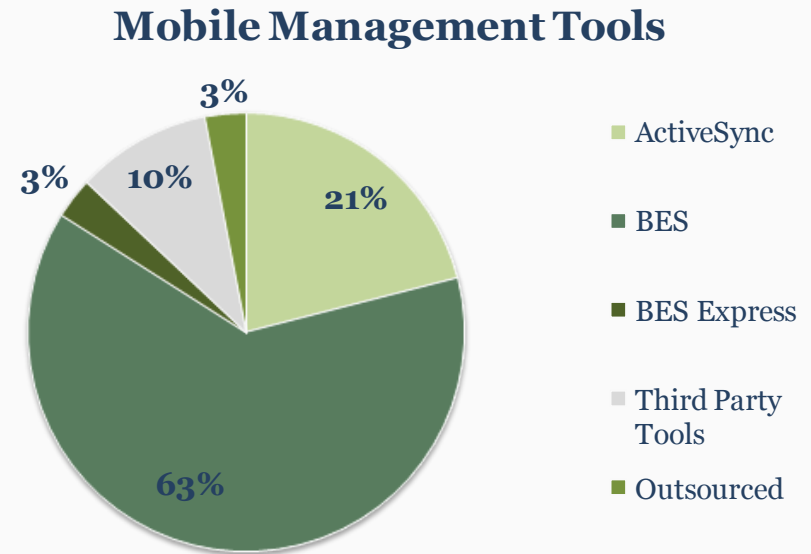
# Mobile Device Management Standards Will Make Life Easier

*Mobile device management standards are gaining traction worldwide but still aren't quite ready for prime time.*

- The industry has recognized the need for some common device management capabilities and has been steadily implementing them on new phones being deployed.
- The Open Mobile Alliance(OMA) has created two standards:
  - OMA-CP, for client provisioning
  - OMA-DM, for device management
- OMA-DM is a more robust protocol for the management of mobile devices and will likely supersede OMA-CP
- The SyncML initiative has been consolidated into the OMA
- See Appendix II for detailed OMA mobile device management enablers.

# RIM and Microsoft Dominate the Mobile Device Management Landscape

- Mobile device management tools exist in many forms:
  - Unless your requirements are truly rigorous, stick with ActiveSync or BES
  - ActiveSync and Blackberry Enterprise Server (BES) from the operating system developers enjoy the highest adoption
  - System management software developers such as [HP](#), [Symantec](#) and [Microsoft](#)
  - Third party point tools from developers such as [Sybase](#), [MobileIron](#) and [MFormation](#)
  - Complete or specialized outsourced solutions from [Tangoe](#), [IBM](#) and a number of wireless carriers



Source: Info-Tech Research Group  
n = 104

# Microsoft ActiveSync Gets the Job Done

*ActiveSync popularity is pushed along with support from Apple, Google and Symbian*


Category	Supported	Product: Microsoft ActiveSync		
		The Good	The Bad	The Bottom Line
Multiple E-Mail Systems	✘	<ul style="list-style-type: none"> <li>• Provides all the basic functionality to support Apple iPhone, Google Android, Nokia, Symbian and Windows Mobile Devices</li> <li>• Management interface is integrated with Exchange</li> <li>• Cost is Free!</li> </ul>	<ul style="list-style-type: none"> <li>• Exchange-Centric</li> <li>• No device ID specific registration or authentication</li> <li>• Policy deployment capabilities vary widely with device operating system</li> <li>• No validation of policy deployment</li> <li>• No native RIM device support</li> </ul>	<ul style="list-style-type: none"> <li>• Good enough for most enterprises</li> <li>• Should not be used alone where compliance and security needs are high</li> </ul>
Multiple Device OS's	✓			
Device Backup	✘			
Application Deployment	✘			
Redundancy	✘			
Communications Encryption	✓			
E-Mail Encryption	✓			
Device Log Management	✘			
Communications Compression	✘			



“ We didn't want to spend money on a BES server so we only support devices capable of working with ActiveSync. – Manager, Accounting Firm ”

# Blackberry Enterprise Server Rules the Roost

*With device form factor pushing out established OS standards and enterprises having to support more device operating systems, BES will have to continue to evolve.*

Category		Supported	Product: Blackberry Enterprise Server(BES)		
			The Good	The Bad	The Bottom Line
Multiple E-Mail Systems		✓	<ul style="list-style-type: none"> <li>• De facto management tool for RIM Blackberry devices</li> <li>• High degree of functionality</li> <li>• 400 security and operating policies provided vs. BES Express's 35</li> <li>• Strong redundant architecture</li> </ul>	<ul style="list-style-type: none"> <li>• Only for managing RIM Blackberry devices</li> </ul>	<ul style="list-style-type: none"> <li>• If managing corporately liable Blackberry devices BES is called for.</li> <li>• If deploying individually liable Blackberry devices Blackberry Express Server is the way to go.</li> </ul> 
Multiple Device OS's		✗			
Device Backup		✓			
Application Deployment		✓			
Redundancy		✓			
Communications Encryption		✓			
E-Mail Encryption		✓			
Device Log Management		✗			
Communications Compression		✓			

# Third Party Tools Help Most with Advanced Features, Multiple OS Support, Application Deployment and Error Handling

## Third Party

Security and compliance sensitive enterprises with multi-device mobile environments must look to a third party for comprehensive capabilities. There are a number of third party tools that deliver additional power, flexibility and compatibility. Scripting, TEM integration and automated device recovery are a few of the advanced capabilities offered. See [Appendix IV](#) for a more complete list.

The logo for SYBASE, featuring the word "SYBASE" in a serif font.

## Outsourced

Outsource mobile device management if more than 1000 devices are deployed, particularly if outsourcing is standard practice. Telecom expense management should be on every IT leader's mind, don't do it yourself.

The logo for Rivermine, featuring a stylized blue and white wave icon followed by the word "Rivermine" in a bold, sans-serif font.The logo for IBM, featuring the letters "IBM" in a bold, blue, sans-serif font.

# As Enterprise Device Diversity Grows, Third Party Management Tools Will Become More Important

*Until then don't invest in third party tools unless mobile security is a primary concern.*

- Info-Tech survey respondents report third party mobile management tools play a key role in managing high security environments
- The impact of multiple mobile management platforms is now being felt and enterprises are looking to a “Single Pane of Glass” for mobile management
- All those separate mobile management tools increase IT resource requirements
- Forget about traditional systems management tools unless you can afford a Tier 1 solution such as IBM Tivoli. Once mid-size system management tool providers mature their mobile offerings, reevaluate integrating mobile management with your overall systems management toolset
- Info-Tech’s “Vendor Landscape: Wireless Telecom Expense Management” will help you choose an expense management solution.



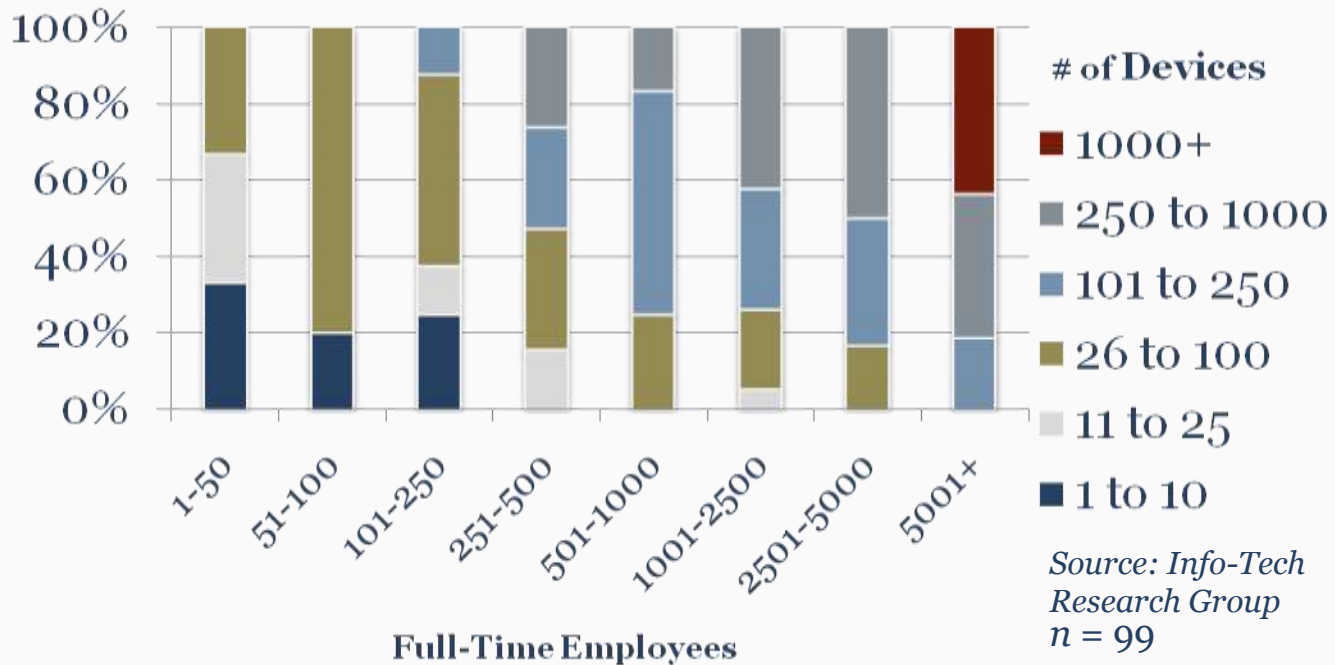
“ *Because we must now support multiple OS's we're exploring third party mobile device management tools to simplify our task. – IT Manager, Utility Company* ”

# Mobile Device Management Roadmap

Understand Mobile Device Management	Corporate or Individual Liability	Mobile Device Management	Policies and Standards	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing
Real World Examples	Small Enterprise	Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment		Strategy	

# Even the Largest of Enterprises Don't Necessarily Have A Lot of Mobile Devices Deployed

*Mobile device management strategy should be geared to the actual or expected number of devices to be deployed.*



## Info-Tech Insight:

*Don't let enterprise size fool you into selecting a complex mobile device management tool.*

# Real World Mobility Management: 50 Device Scenario

**The Scenario:** A small enterprise has approximately 50 users who need access to email, calendaring and cell phone capabilities. They are a rapidly growing entrepreneurial company where management and key staff must be readily available and general staff would like to be more productive. They do not have a corporate application deployed in their mobile fleet.

## **The Solution:**

Device choice is left to the user but carrier plan is standardized.

Corporately liable devices for key management and support staff.

Individually liable devices for general staff.

ActiveSync for iPhones, Android and Windows Mobile Devices.

BES Express for Blackberry Devices.

General email connectivity support is provided by the help desk with all other support provided by the carrier.

## **The Good:**

Users have the flexibility to choose the devices they wish.

Liability policy is flexible and accounts for user and business needs.

ActiveSync and BES Express allow for the greatest possible device selection at the lowest cost.

Support processes have been identified.

## **The Bad:**

As this enterprise grows, the flexibility to choose user devices, rather than standardize for corporate users, may make application deployment difficult.

# Real World Mobility Management: 200 Device Scenario

The Scenario: A mid-size enterprise has approximately 50 corporate users who need access to email, calendaring and cell phone capabilities. A key enterprise application is running on 150 mobile devices providing access to CRM for sales staff.

## The Solution:

Device choice is standardized for sales staff and corporate users.

Corporately liable device policy applies to all users. Consolidated standardized plans with a single carrier.

ActiveSync is the only device management platform.

All mobile device support is funneled through the help desk, carrier issues are escalated when necessary.

## The Good:

Standardized devices and corporately liable device policy means application deployment will be easier.

Consolidated standardized carrier plans will save money.

ActiveSync as the only management platform will simplify administration.

Users will get timely and informed application support.

## The Bad:

While it would be nice to insist on standardized devices, at some point reality will kick in and corporate users will rebel.

Corporately liable device policy may be leaving savings on the table if corporate users do not travel heavily.

The jury is still out on whether or not you can effectively deploy a corporate application on an individual's mobile device. Current trends show corporate liability is most practical for now but it definitely isn't the most cost effective.

# Real World Mobility Management: 1000 Device Scenario

**The Scenario:** A large pharmaceutical enterprise has approximately 200 users who need access to email, calendaring and cell phone capabilities. An additional 300 devices used throughout the production line for running an enterprise quality assurance system. Approximately 500 sales staff utilize mobile devices to track sales data as well as gather sensitive patient data regarding reactions.

## **The Solution:**

Device choice is standardized by user profile. Consolidated standardized plans with a single carrier.

Third party mobile device management has been implemented.

A telecom expense management (TEM) provider examines plans and billing on a monthly basis.

All mobile device support is funneled through the help desk, carrier issues are escalated when necessary. TEM issues are funneled to the appropriate business management.

## **The Good:**

Security and compliance needs have been dealt with using a solid third party management tool.

Consolidated standardized plans with a single carrier will save money.

Engaging telecom expense management will ensure someone is proactively managing costs.

## **The Bad:**

Further savings may have been realized by outsourcing mobile device management.

Individual liability for corporate users may have reduced cost.

# Mobile Device Management Roadmap

Understand Mobile Device Management	Corporate or Individual Liability		Mobile Device Management	Policies and Standards	
Mobile Device Management Solutions	Manufacturer Solutions	Point Solutions	Enterprise Systems Management Solutions	Outsourcing	
Real World Examples	Small Enterprise		Mid-Size Enterprise	Large Enterprise	
Arrive at a Strategy	Assessment			Strategy	

# Assess Your Needs by Answering Eight Simple Questions

- Info-Tech’s “Mobile Device Management Strategy Selection Tool” will help you determine the right approach.
- By answering eight simple questions you will be given a mobile device strategy appropriate to your enterprise.
- For complex scenarios, use the tool to analyze each situation to determine the best strategy.

	Question	Answer
Size		
1	How many mobile devices is your organization managing, or anticipating managing?	101 - 250
Internal IT Experience & Complexity		
2	What level of mobile device management understanding and expertise exists in IT?	Medium
3	Does the IT department have access to, and experience with, a System and Asset Management solution (i.e. Microsoft System Center Configuration Manager (SCCM), Symantec Altiris, LANDesk, Novell Zenworks)?	No
4	Does IT have an existing help desk capable of providing mobile device support?	Yes

# Your Strategy Will Change as Quickly as the Mobile Device Landscape Does



- Annually reevaluate your mobile device management strategy as business needs and technology change.
- Reexamine your mobile user deployment policy to determine if individual liability may make sense for all or part of your enterprise.
- Annually review your mobile application strategy to ensure you're reaping all the benefits of mobile technology.

“There are a lot more interesting applications we've seen with more to come.” – *Manager, Mobile Device Manufacturer*

# Conclusion

- Implement individual liability mobile device policy to keep operational costs predictable
- Management functionality included in the email delivery platform (i.e. BES or ActiveSync) gets the job done in most cases
- Third party mobile management tools offer up power and flexibility when compliance, security or multi-platform support is necessary
- Educate users about mobile device care and security to safeguard corporate data and assets
- Beware of operating system specific device management limitations, they are a silent security issue waiting to happen
- Define and communicate the mobile device support process to drive user satisfaction
- Annually review your mobile device management strategy

Understand Mobile  
Device Management

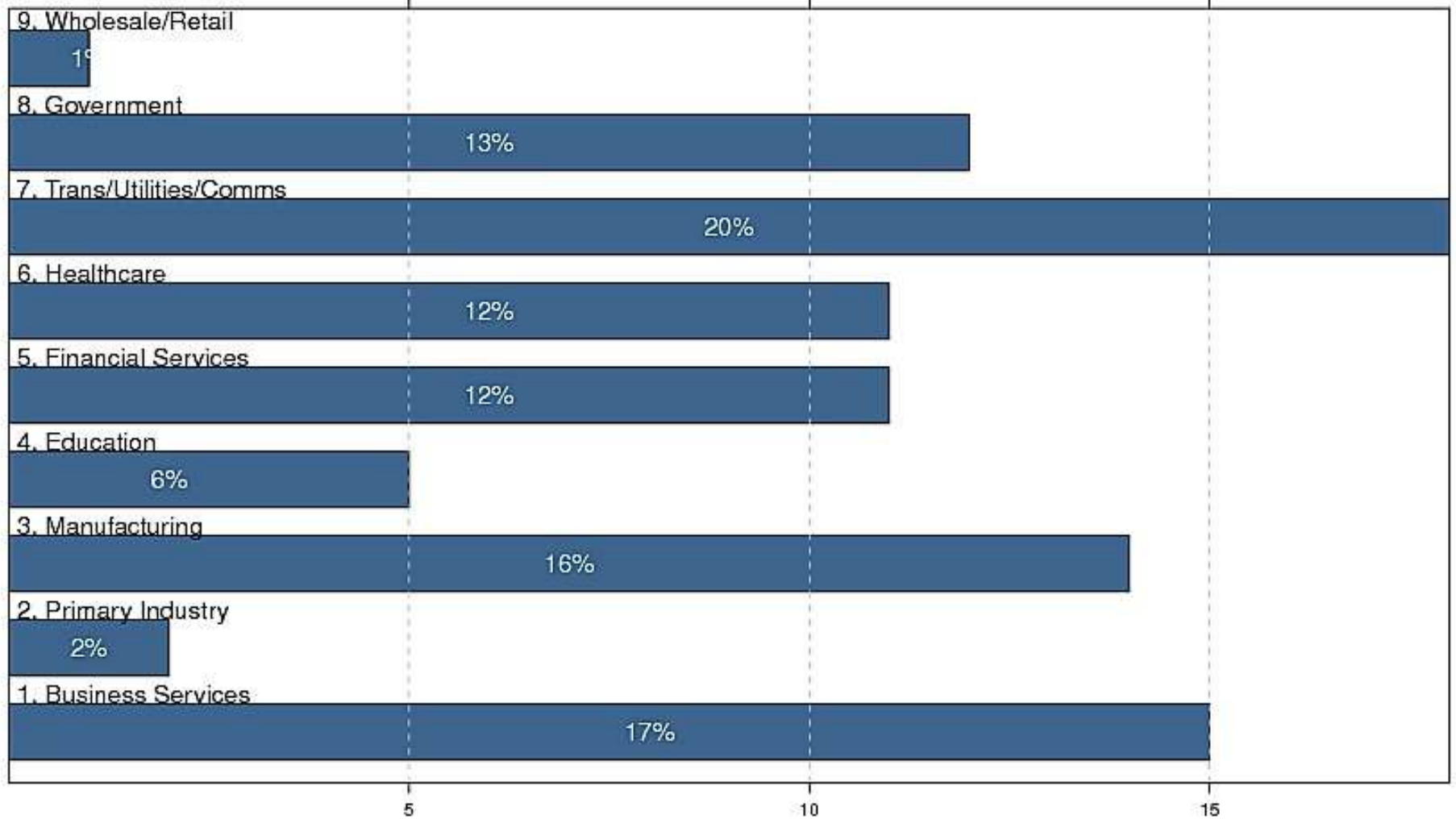
Mobile Device  
Management  
Solutions

Real World Examples

Arrive at a Strategy

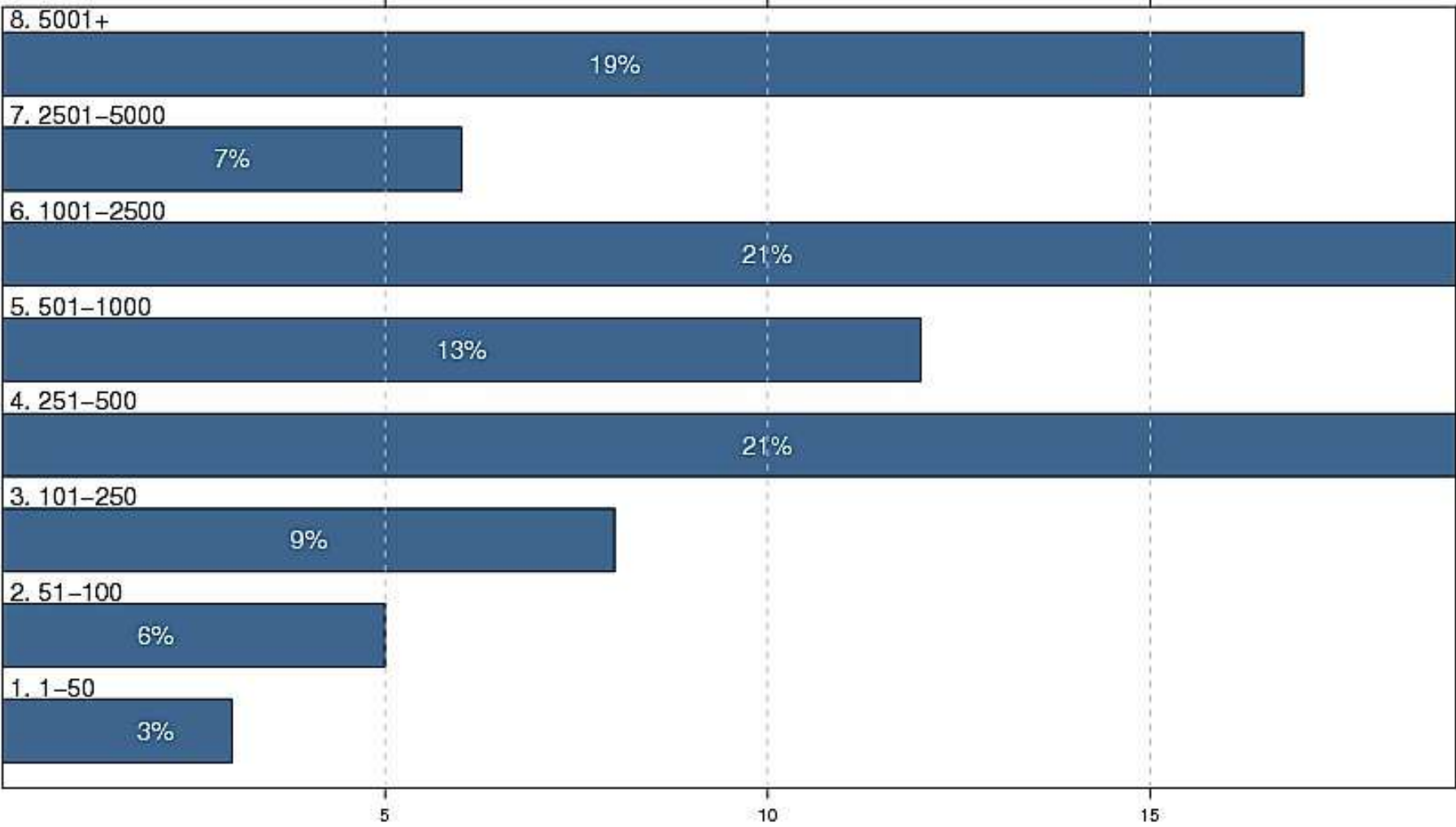
# Appendix I - Survey Demographics

## Industry



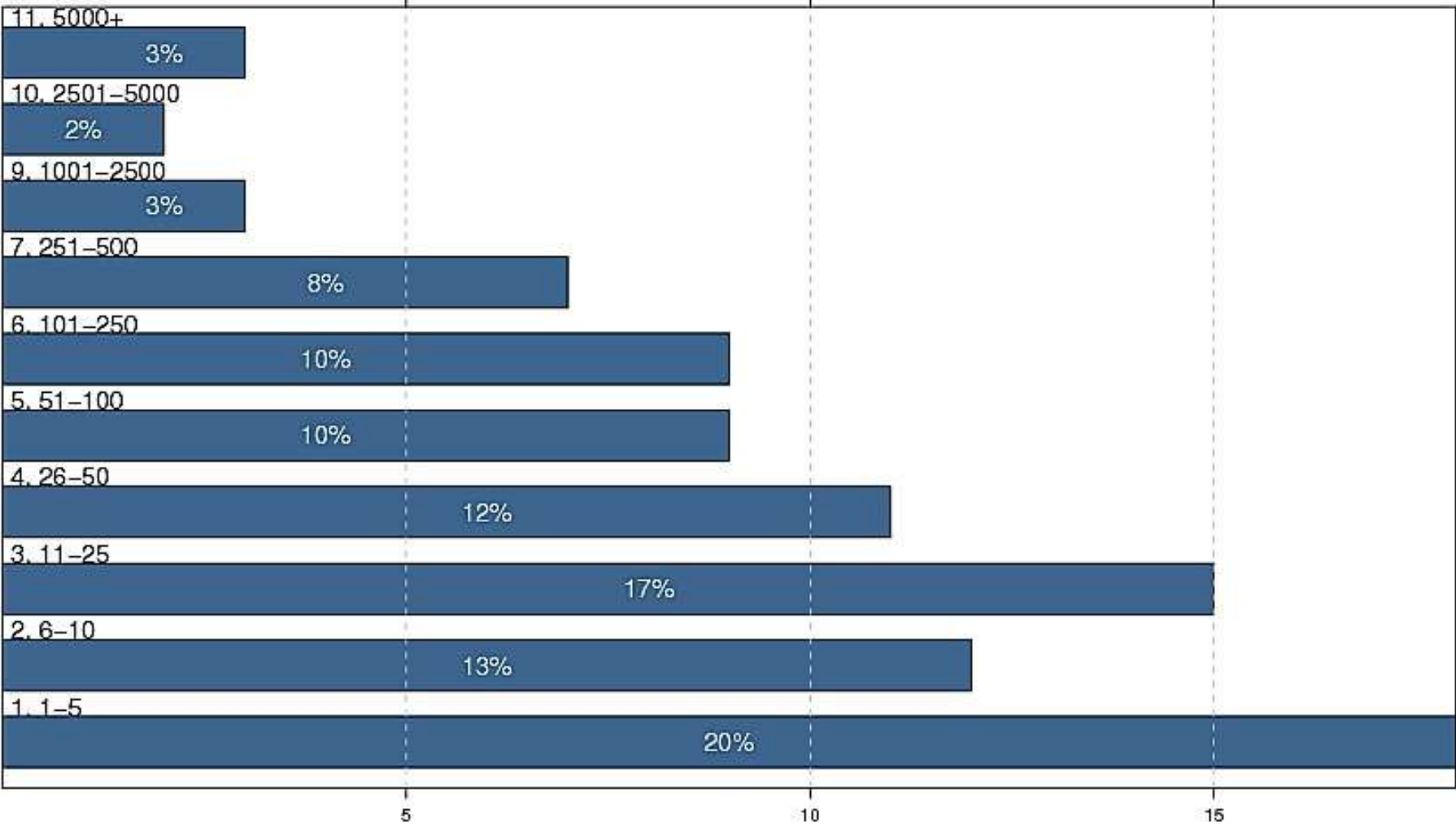
N = 89

# Full-Time Employees



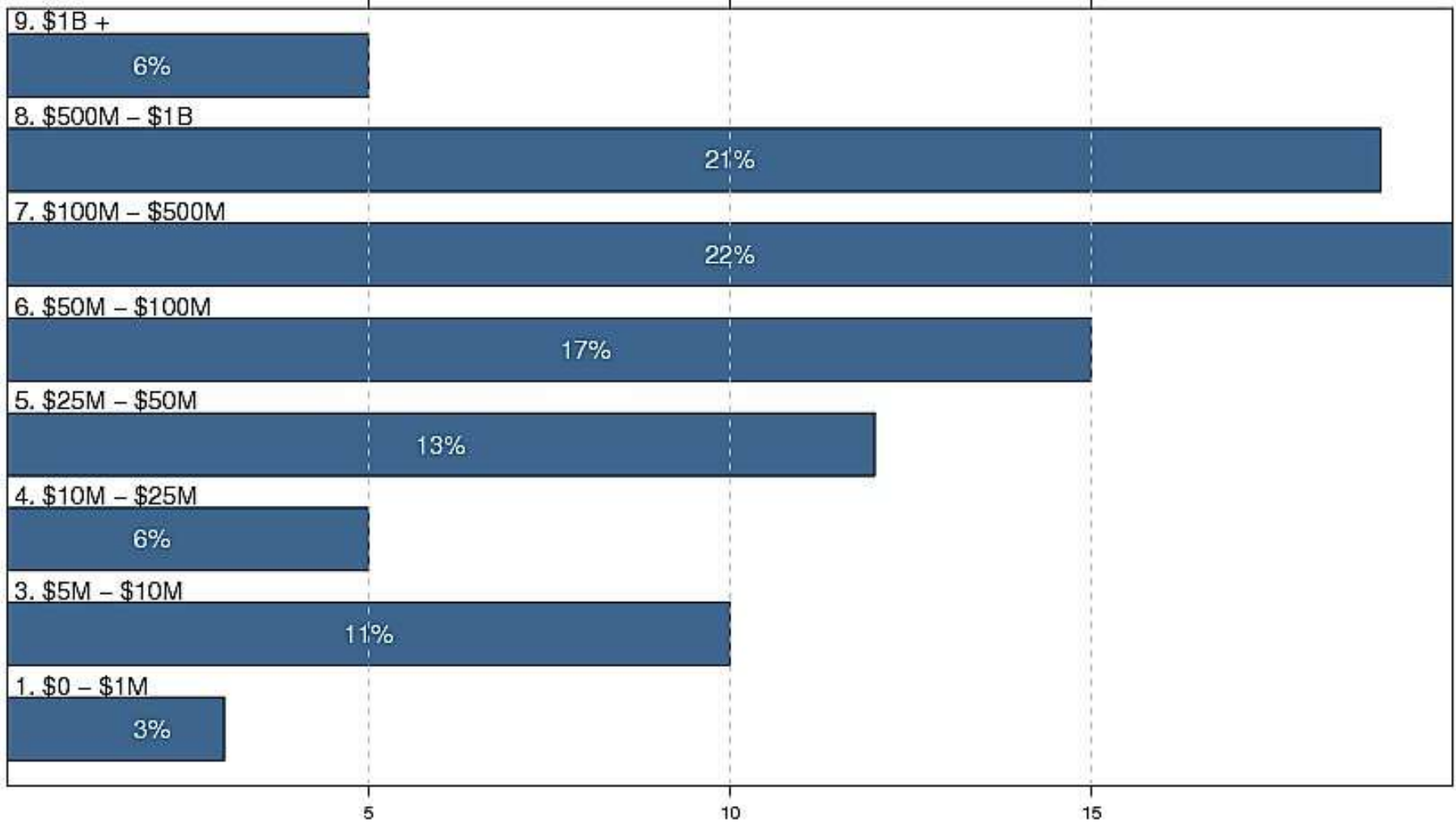
N = 89

# IT Employees



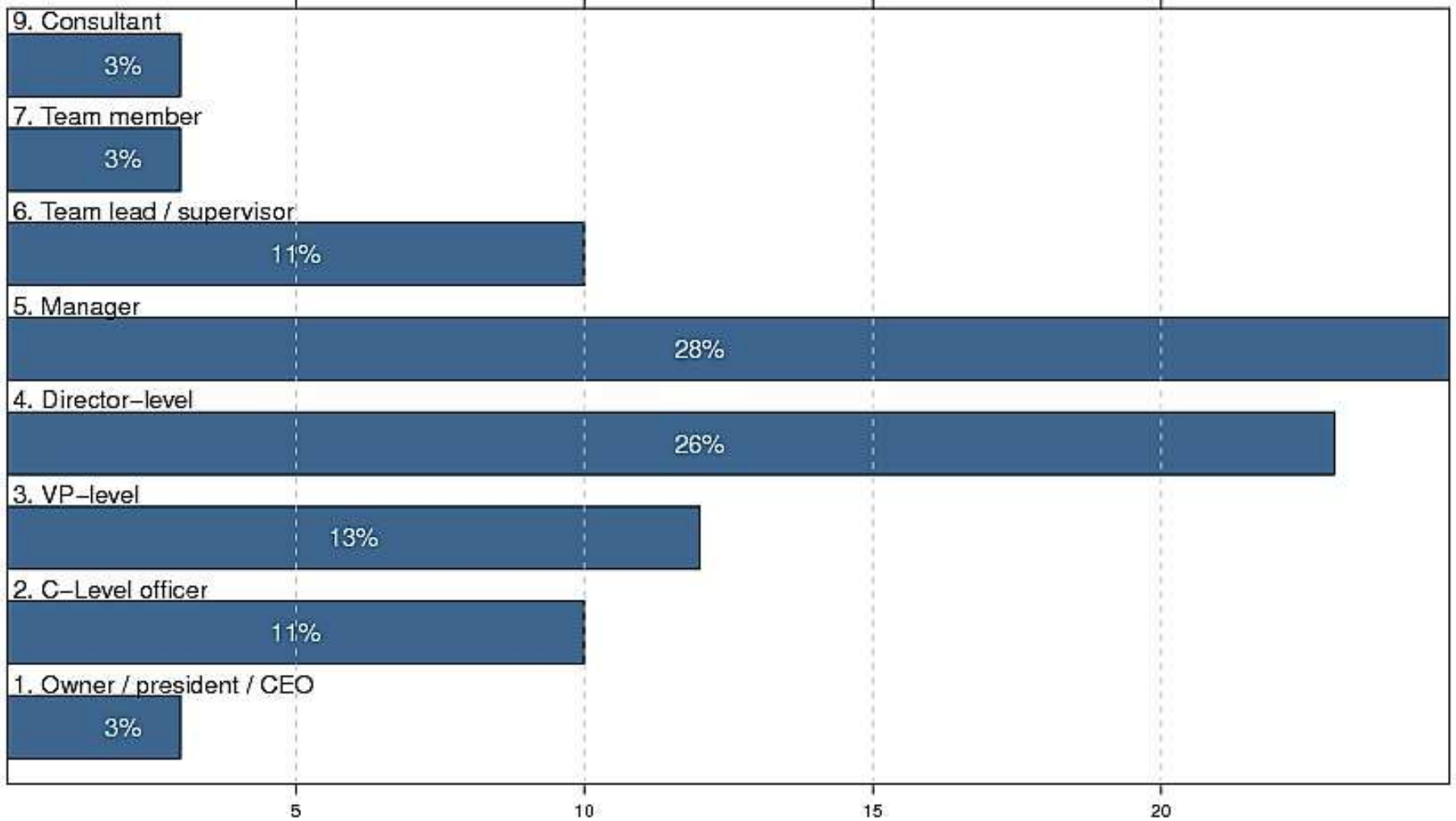
N = 89

# Revenue



N = 89

## Job Title



*N* = 89

# Appendix II - Device Management Enablers

**FUMO.** FUMO stands for Firmware Update Management Object and allows mobile device firmware to be updated over the air. FUMO provides an interface between the client and server and enables mobile operators and device manufacturers to develop and deploy interoperable firmware update solutions. FUMO updates the device firmware and thus can be used to manipulate anything implemented in firmware including the device operating system, security, display and so on.

**LAWMO.** LAWMO stands for Lock And Wipe Management Object. It provides the ability to lock and unlock a device, wipe a device's data and factory reset operations. Its purpose is to protect the device from un-authorized use should it ever be lost or stolen. It also provides the ability to ensure privacy of data on a lost or stolen device, by remotely deleting all data on the device and/or returning it to its factory settings. The LAWMO enabler defines a standard method for all operators and device manufacturers to implement lock and wipe.

**SCoMO.** SCoMO: This enabler stands for Software Component Management Object and it is designed to be a standardized solution for managing Software Components and its requirements. SCoMO provides the ability to Download, Install, Update, Remove, Activate and Deactivate software as well as query for an inventory of software on the device. Whereas the idea of the FUMO enabler is to manage the firmware of the device, the Software Component Management Object is intended to manage software assets other than firmware. Examples include applications, executables, libraries, UI-elements, certificates, licenses etc.

**DIAGMON.** DIAGMON stands for Diagnostics and Monitoring. DIAGMON is designed to enable management authorities such as network operators to proactively detect and repair troubles even before the users are impacted. In order to achieve this, 6 key areas are addressed:

- Diagnostics Policy Management: Setting and enforcing policies for diagnostics features and data.
- Fault Reporting: Reporting faults to the network as trouble is detected at the device.
- Performance Monitoring: Measuring, collecting and reporting key performance indicators (KPIs) data as seen by the device (may be on a periodic basis.)
- Device Interrogation: Enabling the DM Server to query the device for additional diagnostics data in response to a fault
- Remote Diagnostics Procedure Invocation: Enables a DM Server to run diagnostics procedures embedded in the device to perform maintenance and diagnostics.
- Remote Device Repairing: Enables a DM Server to run repair procedures based on diagnostic test results.

# Appendix III - Third Party Mobile Device Management Software

- [Odyssey Software](#)
- [Synchronica](#)
- [Nitrodesk](#)
- [HP](#)
- [Symantec](#)
- [Microsoft](#)
- [Funambol](#)
- [Sybase iAnywhere Afaria](#)
- [AirWatch - AirWatch](#)
- [OTA Mobile Device Management - CallUp OTA Mobile Device Management](#)
- [ITFellas PocketManager - Web-based Mobile Device Management Solution](#)
- [Hewlett Packard - HP Mobile Management Center](#)
- [CloudSync SaaS Mobile Device Management](#)
- [SOTI MobiControl](#)
- [Capricode - SyncShield](#)
- [Fromdistance MDM](#)
- [InnoPath Software ActiveCare](#)
- [Invigo - Automatic Device Management Server](#)
- [Mformation - MFORMATION SERVICE MANAGER](#)
- [MobileIron - MobileIron Virtual Smartphone Platform](#)
- [Nokia Siemens Networks - Device management solution](#)
- [Smith Micro Software - Insignia](#)
- [Sparus Software - EveryWAN Mobility Manager](#)
- [Télélogos - Mediacontact](#)
- [Tangoe - Mobile Device Manager](#)
- [Trust Digital](#)
- [FancyFon - FancyFon](#)
- [Wavelink - Avalanche MC](#)
- [MobiDM](#)
- [B2M Solutions - mprodigy](#)
- [T-Systems - Managed Mobility Services \(MDM Service\), SIMKO II \(MDM for very high Security requirements\)](#)
- [Excitor - DME](#)