Securing Your Mobile Environment

Report

Industry Research from AOTMP

December 2009

AOTMP®

Report

Industry Research from AOTMP

Table of Contents

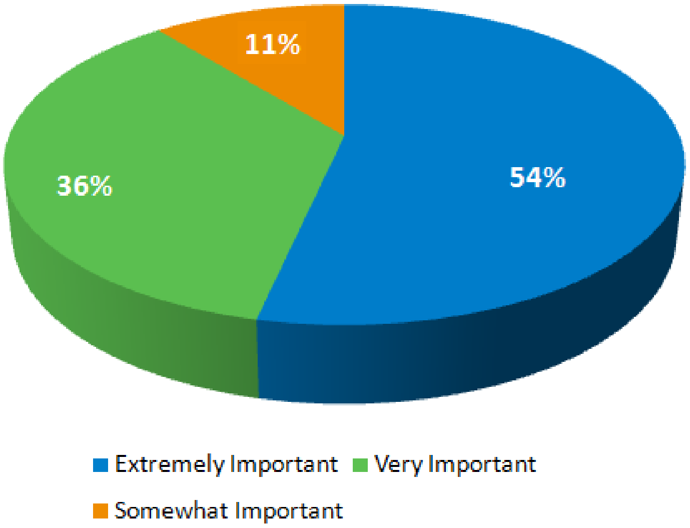
Figures

Executive Summary

With the explosive growth in wireless mobility, enterprises today are placing focus on security for their wireless environments. Recent AOTMP trends reflect the number of smart devices and sensitive applications being installed on these devices has significantly increased, bringing security to the fore-front of wireless mobility management. In fact, recent AOTMP research shows almost 90% of enterprises view security as an extremely or very important aspect of managing their wireless environment.

Furthermore, the mobile workforce is growing exponentially and enterprises must stay ahead of the curve to ensure sensitive data does not get into the wrong hands. Being able to terminate a wireless device that might have been lost or stolen or push a critical application update out to wireless users are just two examples of how security plays a crucial role in any wireless mobility management program.

Figure 1: Wireless Security – Overall Importance



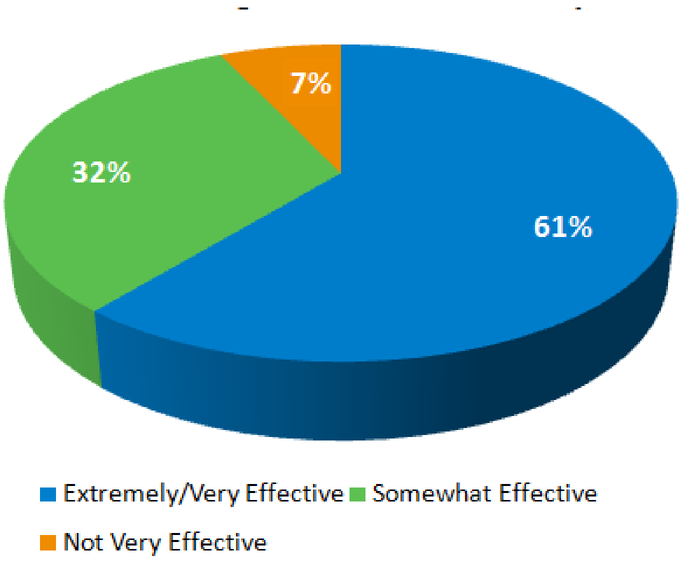
Source: AOTMP, December 2009

Chapter One: Enterprises At-Risk

There are certainly benefits in arming employees with mobile devices. Often, mobile workers are able to be just as productive as if they were physically in the office. While today's sophisticated mobile devices are advantages to business professionals across the globe, there are potential business risks involved when issuing employees with wireless devices. For example, consider the potential consequences of an employee using a personal phone for business use and then suddenly exiting the company. The employee may leave the organization with sensitive, company-related information stored on their device — such as company-related emails, business proposals, financial records and other critical information which places the company at risk. Alternatively, when a device is lost or stolen, this same level of critical information could be exposed if the device falls into the wrong hands. As a result, data could be viewed by or sent to a wide array of unintended recipients such as a competitor, news association or identity hacker, to name a few. Therefore, it is critical that enterprises anticipate these scenarios and plan accordingly, in order to adequately secure their wireless environments.

The core of any successful wireless mobility security practice begins with developing policies to address the various elements of security. Based on AOTMP research, only 61% of enterprises indicated their current wireless policy was extremely or very effective in addressing the topic of security. If strong and enforceable policies are in place and the wireless user community has a good understanding of what the company expects from them in terms of when, where and how to use their devices, the enterprise can reduce the likelihood that security issues will creep into the environment.

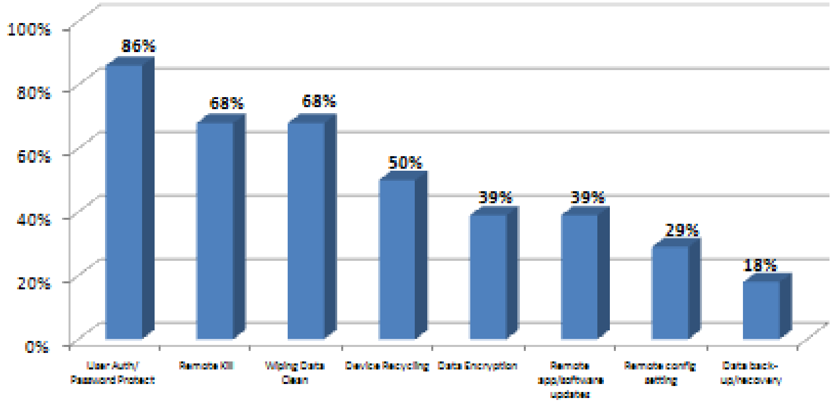
Figure 2: Effectiveness of Company Wireless Policy Addressing Security



Source: AOTMP, December 2009

Enterprises address security within their wireless environments in a number of different ways. AOTMP research reveals the most common security practices being deployed within wireless environments today include user authentication and password protection, followed by remote kills and wiping data clean from devices. User authentication and password protecting are used to validate authorized users seeking access to information. In the event a device is lost or stolen, remote kills and wiping of data are techniques which can be deployed to ensure sensitive data is not viewed by unauthorized personnel. Other security-related practices are also available, such as device recycling, data encryption and remote application updates which ensure the enterprise maintains a watchful eye on security of data on wireless devices and applications.

Figure 3: Most Common Mobile Device Security Strategies



Source: AOTMP, December 2009

Key Take-away From this Chapter:

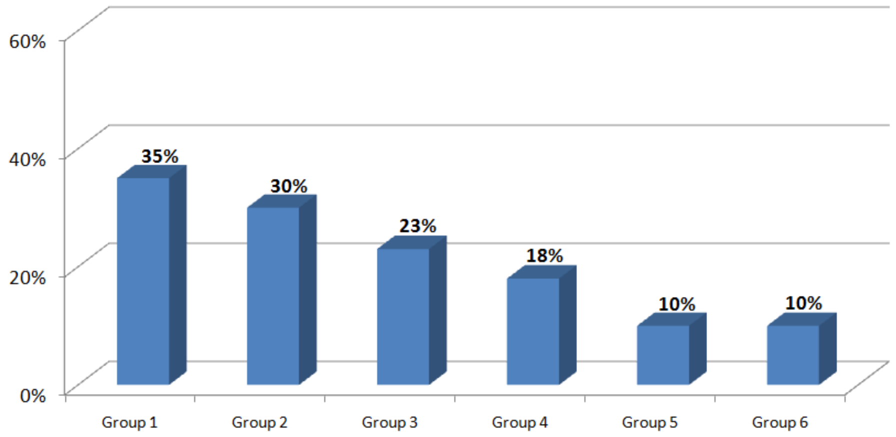
Enterprises should evaluate their current wireless environment to ensure appropriate security policies and strategies are in place. Nearly 40% of enterprises today may be vulnerable to security risks due to a lack of effective policies. An important measure for enterprises is to clearly define and communicate expectations and protocols around lost or stolen devices to decrease the risk of exposing sensitive information.

Chapter Two: Smart Device Presence on the Rise

One of the primary drivers for focusing on wireless device security is a result of the increasingly sophisticated smart devices employees are using to conduct day-to-day business. Organizations are quickly realizing the benefits which high-powered mobile devices can bring from a productivity standpoint. In the past, when voice-only devices existed, the primary focus of wireless mobility management was to ensure users had adequate territorial coverage so employees could communicate with internal and external stakeholders. With today's smart devices, enterprises now have many other items to consider and manage, such as security, international coverage, help desk services, data applications and more.

As mentioned previously, the presence of smart devices has grown significantly in a short period of time. Realizing the effect smart devices have on wireless security considerations, AOTMP sought to quantify the prevalence of smart devices within today's wireless environments. According to AOTMP research, about 21% of all enterprise employees utilize a smart device for business purposes. Taking this a step further, AOTMP also uncovered differences in the presence of smart devices based upon the industry. The graphic below depicts how smart device utilization differs based upon vertical market. As a percentage of total employees, smart device utilization was highest within Technology-oriented organizations, while employees within industries such as agriculture, manufacturing, and retail were least likely to incorporate smart devices within their wireless communications strategy.

Figure 4: Percentage of Employees with Smart Devices – By Industry Group



Source: AOTMP, December 2009

Group 1: Software, Technology, Telecommunications

Group 2: Business Services, Consulting, Finance, Insurance, Legal Services, Real Estate, Travel

Group 3: Transportation, Utilities

Group 4: Education, Government, Healthcare, Not for Profit

Group 5: Agriculture, Construction, Engineering, Consumer Goods, Manufacturing

Group 6: Retail, Wholesale

Key Take-away From this Chapter:

Prevalence of smart devices in the enterprise continues to grow, posing more considerations for wireless mobility management. While there is an increase in smart device use overall, the software, technology and telecommunications sectors have the heaviest concentration of smart devices within their environments. Enterprises should anticipate an increase in the time associated with managing elements such as security and help desk tickets in relation to having more smart devices across the employee base.

Chapter Three: Standards and Best Practices

AOTMP best practices outline Wireless Mobility Management as six core activities:

- **eProcurement:** This activity specifically relates to providing an online portal to order and secure services, devices and/or accessories from Carriers.

- **Asset/Inventory Management:** This area involves offering the capability to track the wireless assets (e.g., devices, accessories, service plans, contracts, and software licenses) of an organization so at any given time a company has visibility into the wireless environment.

- **Expense Management:** This area involves providing the ability to manage wireless expenses. This includes activities such as invoice processing and contract lifecycle management. This also involves offering rate plan optimization and being able to communicate with carriers on any contract or invoice disputes.

- **Help Desk Management:** This aspect constitutes having dedicated staff who can be contacted in order to troubleshoot technical issues and manage trouble-tickets on behalf of the customer.

- **Mobile Device Management:** This involves providing the ability to manage devices and provide security services such as wiping stolen or lost devices clean (e.g., remote “kills”), remote application updates and device server administration.

- **Reporting & Analysis Tools:** This area specifically encompasses providing an online tool which provides visibility into expenses, consumption, assets and inventory as well as usage trending. Basic information that is available includes wireless expenses for the month as well as specific call details for each user.

Integration of these practices into the management of your wireless environment provides the ability to drive effectiveness across operational performance, financial performance and technical performance objectives, and their contribution to overall business requirements.

Central to AOTMP's Wireless Mobility Management standards and best practices is methodology that promotes informed decision making and success monitoring to achieve intended results. An effective wireless security strategy will implement sound security measures while ensuring the needs of the wireless user community are met. AOTMP has outlined key best practices to follow when managing security within your wireless environment:

1. **Assess Current State of Wireless Security**
    - Understand how employees are utilizing mobile devices today and how usage may change going forward
    - Determine where security vulnerabilities exist
    - Identify and deploy specific security practices which will address vulnerabilities
    - Ensure practices achieve security objectives while ensuring employee business needs continue to be met

2. Establish / Update Wireless Policy

- Establish guidelines for appropriate usage including where, when and how devices are to be used
- Ensure users are properly educated regarding security and their devices
- Establish procedures around what to do in the event a device is lost or stolen
- Ensure policies and procedures are clearly communicated and enforced

3. Ensure Appropriate Support Resources are Available

- Determine whether security will be managed internally or through an external third-party
- Ensure support staff is properly trained on deployed wireless devices and technologies, common requests for support, etc.
- Ensure wireless users know who to contact in the event assistance is needed

4. Monitor and Reassess Security Practices

- Establish means to monitor security practices
- Identify current weaknesses and new threats as it relates to wireless security
- Update security policies and practices as needed

Conclusion

The rapid growth in the mobile workforce and the sophistication of today's wireless devices have dictated that security become a priority for many enterprises. A reactive approach to security management could have severe consequences for organizations. If a device is stolen and appropriate security measures are not in place, critical information including customer information and proprietary business data could be exposed and sensitive data may be compromised. However, taking proactive security measures such as user authentication as well as remote kills and application updates, the enterprise will ensure due diligence has been performed in addressing security for valuable data which may accessed from wireless devices.

Appendix A: Research Methodology

Research Demographics

AOTMP collected benchmark data from a variety of industries to examine wireless security management strategies. The findings in this report represent benchmark data from 190 enterprise professionals across 23 different industries that had knowledge of overall wireless mobility security within the organization.

Job Title / Function:

Sr. Mgt/CIO/CFO/VP	5%
Director/Manager	51%
Staff	34%
Other	10%

Geography:

North America	96%
Europe	3%
Asia Pacific	1%

Annual Revenue:

Above $1 billion	48%
$50 million - $1 billion	37%
Less than $50 million	15%

Report

Industry Research from AOTMP

About AOTMP Research

AOTMP research is supported through data collected from a variety of sources. Data points are collected through enterprise and supplier benchmarking projects, training and certification events, research surveys, frequent hot topic polls, virtual conference audience polling, live conference audience polling, and AOTMP Access benchmarking events. AOTMP's data point contributors include over 60,000 IT, telecom and business professionals, supporting domestic and international enterprises and industry suppliers. Data points contributing to research are carefully analyzed using advanced statistical methods. Research findings are confirmed through test/retest validity methodology and, therefore, paint an accurate picture of the industry. The clarity and detail of AOTMP research is unmatched in the practice of telecom environment management, and AOTMP expertise translates analysis into actionable findings representative of the industry and all related industry segments.

About AOTMP

AOTMP is the leading provider of information solutions for managing fixed and wireless telecom environments. Our proprietary certifications, benchmarks, standards and best practices deliver measurable improvement in efficiency and productivity for managing wireless, voice, data and network services. From Fortune 50 companies to SMB, enterprises seeking the best return on telecom services turn to AOTMP's industry research, advisory services, events, educational programs and performance management systems to achieve operational and financial efficiency.

Research & Benchmarks

AOTMP conducts industry-leading research to provide benchmarks, reference points, case studies and reports that deliver timely and relevant insight. We help enterprises make confident, informed decisions affecting their telecom and IT environment, and provide information to recognize trends affecting performance and efficiency, determine budget allocations and resources, and understand how others are achieving success.

AOTMP University

Implementing and executing best practices in your enterprise begins with a staff that understands and supports industry standards. AOTMP University offers staff development and training packages to educate telecom and IT professionals on best practices for driving efficiency and optimizing budgets. You can learn more about our certification programs, online training courses and certified professional program at www.aotmpuniversity.com.

AOTMP®

Report

Industry Research from AOTMP

Advisory & Consulting Services

Our team of industry experts can help you improve and gain visibility into your current management processes, and understand how to effectively measure performance. Put the power of AOTMP's expertise to work in your telecom and IT environment to create the most effective telecom environment management program for your enterprise.

Tools & Resources

AOTMP offers a comprehensive array of tools, templates and reference information for telecom financial, operational, and technology management. Tools like our online Telecom Knowledge Base (TKB), supplier directories, Telecom Environment Management enewsletter, and other resources help telecom and IT professionals increase efficiency, make tactical decisions, cut costs, and plan strategic moves.

Events & Programs

AOTMP produces several industry events and programs throughout the year to bring end users, industry experts and suppliers together for education, networking, and collaboration. Our events and programs include semi-annual virtual conferences, monthly web events, an Industry Advisory Board, and an annual in-person conference featuring AOTMP's *Industry Excellence Awards* recognizing the successes of both enterprises and suppliers in telecom environment management.

Performance Management Systems

Our Performance Management Systems help you apply standards and best practices throughout your enterprise to drive continuous improvement of people and processes using benchmarks, metrics and scoring algorithms. AOTMP's Performance Index provides a consistent means of evaluation, and our comprehensive methodology enables you to optimize performance in your telecom environment, and then leverage telecom assets to drive growth, profitability and competitive advantage.

Additional information on AOTMP publications, programs and research can be found at www.aotmp.com.

AOTMP, 6510 Telecom Drive, Suite 100, Indianapolis, IN 46278
1.800.460.9568 www.aotmp.com