Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

FORRESTER®

Prepared for Cisco Systems
April 21, 2006

The Total Economic Impact Of Deploying Mobility Services

Location, Voice, Guest Access, And Advanced Security

Project Director: Lauren Hughes
Contributor: Chris Andrews

FORRESTER®
Headquarters
Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • www.forrester.com

TABLE OF CONTENTS

Executive Summary

In January 2006, Cisco Systems commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) that enterprises may realize by deploying location, voice, guest access, and advanced security on the wireless LAN (WLAN). These four services are hereafter referred to as Mobility Services.

Forrester conducted in-depth interviews with 12 organizations that have recently deployed or are in the process of deploying pervasive WLANs (wireless networks to which all employees have access). The purpose of the interviews was to understand the key drivers for deployment of pervasive WLANs and to detail the use or intended use of Mobility Services. Forrester found that the deployment of Mobility Services allowed the organizations we interviewed to achieve cost savings and to improve employee productivity, customer satisfaction, and security.

Purpose

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Mobility Services. Forrester's aim is to clearly show all calculations and assumptions used in the analysis. Readers should use this study to better understand and communicate a business case for investing in Mobility Services.

Methodology

Cisco selected Forrester for this project because of its industry expertise in WLAN and Forrester's Total Economic Impact™ (TEI) methodology. TEI not only measures costs and cost reduction (areas that are typically accounted for within IT), but also weighs the enabling value of a technology in increasing the effectiveness of overall business processes.

For this study, Forrester employed four fundamental elements of TEI in modeling Mobility Services:

1. Costs and cost reduction
2. Benefits to the entire organization
3. Flexibility
4. Risk

Given the increasing sophistication that enterprises have regarding cost analyses related to IT investments, Forrester's TEI methodology serves an extremely useful purpose by providing a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

Approach

Forrester used a five-step approach for this study.

1. Forrester gathered data from existing Forrester research relevant to Mobility Services and the WLAN market in general.
2. Forrester interviewed Cisco marketing and product development personnel to fully understand the potential (or intended) value proposition of Mobility Services.

3. Forrester conducted a series of in-depth interviews with 12 organizations currently using Mobility Services. Cisco provided Forrester with three of the company names, and Forrester sourced the remaining organizations.

4. Forrester constructed a financial model representative of the interviews for each of the four Mobility Services. The models can be found in the TEI Framework section below.

5. Forrester created a composite organization for each of the four Mobility Services and populated the financial models using data from the interviews as applied to the composite organizations.

Key Findings

After populating the financial models with data from the composite organizations, Forrester constructed an associated ROI analysis for each of the Mobility Services, illustrating the financial impact areas. Forrester's study yielded four key findings:

- **Location.** Interviewed companies identify the quantifiable benefits of location services as a reduction in time spent to locate assets and a reduction in the cost to replace missing assets. As seen in Table 1, the ROI for the composite company is 55%, with a breakeven point (payback period) of 16 months after deployment.

  The qualitative benefits associated with location services include: improved security through location-based security features; improved employee productivity through location-based call routing and content distribution; improved IT productivity through location-based trend analysis; and improved customer satisfaction through reduction in wait time for services.

- **Voice.** Organizations using voice over the WLAN identify two key areas of quantifiable benefits: avoidance of cellular or pager charges for mobile workers and improved mobile worker productivity. The ROI for the composite company is 157%, with a breakeven point of nine months after deployment.

  The qualitative benefits associated with voice services include: improved employee accessibility through unified messaging; improved employee collaboration; decreased support costs for proprietary wireless voice systems; improved customer and employee satisfaction through enhanced mobility; and improved visibility into voice costs because all facility communication is controlled by the enterprise.

- **Guest Access.** Organizations using a guest network to provide visitors with wireless access to the Internet identify the reduction in IT support costs to manage wireless guest access as a quantifiable benefit. The ROI for the composite company is 328%, with a breakeven point of six months after deployment.

  The qualitative benefits associated with guest access include: improved security; improved customer service; improved network performance in shared space environments; improved ability to retain visitors on-site; and improved perception of the company as an advanced technology user by partners and other guests.

- **Advanced Security.** Forrester examined two advanced security features in this study: wireless intrusion detection and prevention (IDS/IPS) and single user identity via integrated 802.1X on the wired and wireless networks. Associated with wireless IDS/IPS, interviewees

attribute quantifiable benefits to faster identification and containment of rogue access points and a reduction in exposure to viruses. The quantifiable benefits associated with integrated 802.1X single user identity are: less time to manage users, improved protection against unauthorized users, and reduced theft of proprietary information. The ROI for the composite company is 114%, with a breakeven point (payback period) of 14 months after deployment.

The qualitative benefits associated with advanced security include: improved safeguarding of the brand; provision of a platform for physical security; improved employee security protection through reduction in phishing incidents; and potentially improved regulatory compliance.

Table 1 illustrates the risk-adjusted cash flow for the composite organizations, based on data and characteristics obtained during the interview process. Forrester risk-adjusts these values to take into account the potential uncertainty that exists in estimating the costs and benefits of a technology investment. The risk-adjusted value is meant to provide a conservative estimation, incorporating any potential risk factors that may later impact the original cost and benefit estimates. For a more in-depth explanation of the risk and risk adjustments used in this study, please see the "Risk" section.

Table 1: Composite Company ROI, Risk-Adjusted

Metric	Location	Voice	Guest Access	Advanced Security
Total three-year costs	($686,042)	($1,197,277)	($49,349)	($669,283)
Total three-year benefits	$1,065,720	$3,075,925	$211,134	$1,430,372
Total three-year net savings	$379,677	$1,878,648	$161,785	$761,089
ROI	55%	157%	328%	114%
Payback period (months)	16	9	6	14

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

- The study is commissioned by Cisco Systems and delivered by the Forrester Consulting group.
- Cisco reviewed and provided feedback to Forrester, but Forrester maintained editorial control over the study and its findings and did not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.
- Three of the customer names for the interviews were provided by Cisco. The rest were sourced by Forrester.
- Forrester makes no assumptions as to the potential return on investment that other organizations will receive. Forrester strongly advises that the readers should use their own

estimates within the framework provided in the report to determine the appropriateness of an investment in Cisco or Mobility Services.

- This study is not meant to be used as a competitive product analysis.

WLAN Market Trends

Wireless LAN usage is mainstream. Wireless LANs are being used or considered by more than 60% of North American and European enterprises, according to Forrester's Business Technographics® May 2005 North American And European Network And Telecommunications Benchmark Study. Today, WLANs:

- **Are deployed in one-quarter of enterprises, with another 40% evaluating or piloting.** North American WLAN enterprise adoption dramatically increased in the past two years. In February 2003, 9% had completed deployment; in May 2005, 24% had deployed or were upgrading.[1] North America still leads Europe slightly, where only 21% of enterprises had rolled out WLANs by May 2005.

- **Exhibit significant adoption variability across industries.** The public sector (including healthcare, education, and government) and manufacturing verticals lead in WLAN deployments at 33% and 30%, respectively. Meanwhile, only 5% of finance and insurance firms have deployed the technology, and 52% have expressed no plans for WLAN deployments. Why the variability? Security ranks as the No. 1 obstacle when acquiring wireless technologies across industries, and financial services firms are the most security-conscious vertical because of the sensitive nature of financial transactions.

- **Are adopted more by larger enterprises.** The larger the enterprise, the more WLAN adoption; 31% of enterprises with more than 20,000 employees have fully deployed WLANs, compared with 22% of enterprises with between 1,000 and 4,999 employees.

Wireless LAN adoption today is broad and growing. Forrester predicts an increased reliance on WLANs in 2006, resulting in 75% of North American enterprises using or evaluating WLANs by year end. Factors driving wireless LAN adoption include:

- **A culture of mobility.** Some of Forrester's clients are using wireless as their primary network, even when a wired one is available. In the morning, employees access the VPN from their desk over the wireless network to limit configuration changes as they get up and walk with their laptop to a meeting. An expectation of mobility has emerged not just away from the office, but within it as well.

- **Voice services.** Voice over WLAN and mobile data applications will drive WLAN deployments deeper in the company over the next five years. Potential cellular cost savings can be realized by using WLANs for voice coupled with the availability of dual-mode Wi-Fi/cellular handsets. WLANs will become a required addition to enterprises' network infrastructure — not a replacement for wired infrastructure but an augmentation. Users will depend on WLANs for voice and data, putting a greater emphasis on the manageability, security, and reliability of WLANs.

- **Location services.** Enterprises can now track 802.11 devices — such as active RFID tags and laptops — using the existing WLAN infrastructure. Early adopters in healthcare, manufacturing, and retail are using location tracking for inventory control. In the near future, new low-voltage Zigbee sensors will make it even more cost-effective to use WLANs to monitor equipment.

- **Improved security features.** Security concerns have caused some organizations to avoid installing wireless LANs. Now the landscape of wireless security has changed. Good

[1] Source for 2003 data: Forrester's Business Technographics February 2003 North American Benchmark Study

wireless intrusion detection and prevention solutions work to detect and block egregious behavior on the WLAN, such as rogue access points or probes from common attack tools. 802.1X authentication across the wired and wireless networks (single user identity) virtually eliminates losses from network entry unauthorized access and gives you the ability to simplify the number of moving parts in the identity/authentication process.

Mobility Services: Overview

Location

Location services leverage WLAN access point signal strength and position to provide accurate location tracking. Enterprises can track 802.11 devices like handheld devices and laptops, or they can put active (802.11) RFID tags on assets. In addition, the system provides a historical view of location data allowing for improved management and planning.

Voice

Voice over WLAN (VoWLAN) is a technology that enables calls made to a private branch exchange (PBX), or an IP switch serving in that capacity, to be converted to data format, sent over a wired LAN, and then transferred to a WLAN. An employee with a VoWLAN-enabled device is able to receive calls wherever wireless access points are available.

The VoWLAN system allows all regular functions and messaging applications available on wired phones to be available on VoWLAN devices. Business-class WLAN networks offer pervasive coverage within a building, improving right-time communications and mobile calls initiated on campus. This results in cost savings compared with cellular calls.

Guest Access

Guest access is the provision of a guest network whereby visitors are provided with wireless access to the Internet or other controlled resources. Typically, guest access securely segments guest traffic from the production network. It allows an organization to determine who is on the network and what they are doing, as well as to identify and restrict harmful behavior and protect the network.

Advanced Security

Wireless intrusion detection provides 24x7 radio frequency (RF) surveillance and can detect rogue network activity and malicious attacks and identify trends that may indicate a threat. Wireless intrusion prevention predictively suggests actions to stop would-be attacks before they can do damage.

802.1X is a port-based authentication standard used to authenticate endpoints, such as PCs and IP phones, with network devices like access points, routers, and switches. 802.1X supports several extensible authentication protocol (EAP) technologies like EAP-FAST, EAP-PEAP, EAP-LEAP, and EAP-TTLS and works hand-in-hand with encryption to provide more robust WLAN security. Single user identification through 802.1X gives companies the ability to simplify the number of moving parts in the identity/authentication process. The primary benefits are savings related to policy creation and ongoing maintenance, auditing, and tweaking of identity policies (e.g., who should have access to what, where, when, why, and how).

Analysis

As stated in the Executive Summary, Forrester took a multistep approach to evaluate the impact that implementing Mobility Services can have on an organization:

- Interviews with Cisco marketing and product development personnel
- In-depth interviews with 12 organizations currently using Mobility Services
- Construction of a common financial framework for the implementation of each of the Mobility Services
- Construction of four composite organizations, one for each of the Mobility Services, based on characteristics of the interviewed organizations

Interview Highlights

A total of 12 interviews were conducted for this study. Nine of the 12 organizations have headquarters in the United States, and the remaining three have large operations in the United States.

Table 2: Interview Highlights

Interviewed organization	Current use of WLAN	Future use of WLAN
Software provider with more than 30,000 employees	Migrating from an autonomous access-point-based solution (distributed WLAN architecture) to a centralized architecture that utilizes wireless LAN controllers (centralized WLAN architecture). Initiative to centralize was to provide guest access on wireless networks. Currently using WLAN for frequent formation of diverse internal project teams that require office mobility. Using intrusion detection as part of centralized management of WLAN.	• Waiting for dual-mode phone technology before considering voice over the WLAN. • Still deploying 802.11i. • Using 802.1X-style implementation on the wireless side. Dealing with integration issues on the wired side.
Refining company with more than 50,000 employees	Ongoing deployment of wireless LAN, under the belief that networks will live on the Internet and new users should be wireless. Have guest access in corporate offices.	• Do not intend to deploy voice over WLAN. • Piloting wireless location services in the field. • Plan to deploy 802.1X integrated on the wired and wireless networks to tighten up security.
University with 12,000 students and 25,000 faculty and staff	Will complete deployment of three centralized wireless networks this year (medical school/hospital, business school, and rest of university) to improve student and faculty productivity. Using wireless IDS/IPS as part of centralized administration of WLAN.	• Investigating location tracking on WLAN for inventory control and movable equipment. • Piloting voice with the IT department. • Piloting guest access for visiting faculty, students, and vendors. • Piloting 802.1X authentication on wireless network.
Auto manufacturer with more than 200,000 employees	Implemented wireless LAN at manufacturing facility to manage inventory, and have deployed to eight plants and other offices. Implemented guest access to reduce the number of viruses guests were introducing to the network. Outsource IDS/IPS.	• Planning to pilot location services on the wireless LAN to solve problem of losing expensive equipment, components, and parts. • Piloting voice over WLAN but plan to wait for dual-mode phones before full deployment.
Lodging company with more than 70,000 employees	Recently completed WLAN deployment with distributed architecture at corporate offices to respond to access requests from contractors and vendors. Secondary reason was to provide employees with ubiquitous network access. Purchased overlay for IDS/IPS.	• Recently implemented 802.1X on wireless network and now attempting to integrate 802.1X with wired network. • Considering tracking luggage carts at hotels with location services.

Source: Forrester Research, Inc.

Interviewed organization	Current use of WLAN	Future use of WLAN
Hospital with 10,000 employees	Two years ago, completed deployment of two distributed architecture wireless networks, for academic and clinical communities. Key driver was to improve access to critical information and to improve productivity. Also deployed 802.1X across wired and wireless networks. Recently purchased an overlay for the latest generation IDS/IPS. Currently using location services to track laptops.	• Currently using a proprietary wireless technology for voice. • Plan to deploy network for guest access for PR reasons and to eliminate the labor-intensive configuration of guest machines. • In next five years, plan to use location services to track wheelchairs and beds and other "hoarded" equipment.
Large equipment distributor with approximately 1,000 employees	Recently completed WLAN deployment with distributed architecture, originally deployed to conference rooms at corporate offices and rolled out to other offices and sales branches. Key driver was improved employee productivity.	• Plan to go to IP trunking for voice during refresh cycle. • Considering voice over WLAN when dual-mode phones become available. • Plan to roll out intrusion detection with rollout of centralized architecture for WLAN.
Federal agency with 28,000 employees	Recently centralized multiple distributed WLAN environments. Key drivers included freeing up lab space and the desire to save costs in older buildings by putting in a wireless as opposed to a wired network.	• Intend to deploy voice over WLAN once interoperability issues resolved on PDA device. • Do not intend to deploy location tracking or guest access. • Currently investigating advanced security features such as intrusion detection and 802.11i.
Hospital with 20,000 employees	Deployed centralized wireless network 18 months ago along with industry's move towards electronic data records. More recently deployed voice over WLAN to 800 nurses for improved quality of care. Recently implemented guest access on patient floors. Have wireless intrusion detection and prevention as part of centralized infrastructure.	• Plan to implement location tracking in 2007 to track IV pumps and other high-value equipment. • In the future, doctors may end up with dual-mode phones with PDA capabilities. • Expect to use WLAN for telemetry, including patient monitoring devices.
School district with 34,000 students and 6,700 faculty and staff	Completing centralized WLAN deployment in the next 12 months. Key driver is cost savings achieved by providing teachers with a single wireless client device, instead of two devices. Currently using intrusion detection as part of centralized management of WLAN.	• Plan to buy devices for voice over WLAN once every campus has a complete wireless overlay (next 12 months). • Key users will be faculty, administrative staff, and perhaps maintenance. • Do not intend to deploy location tracking or guest access.
Transportation company with more than 200,000 employees	Deployed wireless network with distributed architecture more than 10 years ago to support scanning devices. Recently implemented guest access at two locations to improve vendor productivity and to stop vendors from bringing in rogue access points. Recently purchased overlay for IDS/IPS to prevent security breaches. Currently upgrading to 802.1X on wired and wireless networks.	• Piloting voice over WLAN with 12 warehouse managers. • Plan to deploy 700 voice over WLAN phones, replacing cell phones, to get rid of monthly cellular charges and improve productivity where coverage is poor. • Considering deploying location tracking over wireless network for ground support equipment (tugs, dollies, tow bars) to reduce wasted search time.
Hospital with 5,000 employees	Began campuswide rollout with distributed architecture 18 months ago, but recently began to replace original access points with new access points in centralized architecture. The reasons to deploy were to take advantage of mobile technology and improve clinical efficiency and patient care. Deployed location tracking for 14 medical devices in emergency room. Currently using centralized console to track and contain rogue access points.	• Plan to track all medical devices with minimum price of $10,000. • With rollout of centralized architecture, plan to roll out guest access to all buildings to allow patients, guests, other visitors to get online.

Source: Forrester Research, Inc.

TEI Framework

Introduction

From the information provided in the in-depth interviews, Forrester has constructed a TEI framework for those organizations considering implementation of Mobility Services. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that impact the investment decision.

Framework Assumptions

Table 3 lists the discount rate used in the PV and NPV calculations and time horizon used for the financial modeling.

Table 3: General Assumptions

Ref.	General assumptions	Value
	Discount rate	10%
	Length of analysis	Three years

Source: Forrester Research, Inc.

Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their finance department to determine the most appropriate discount rate to use within their own organization.

In addition to the financial assumptions used to construct the cash flow analysis, Table 4 provides salary assumptions used within this analysis.

Table 4: Salary Assumptions

Ref.	Metric	Calculation	Value
R1	Weeks per year		50
R2	Hours per day		8
R3	Hours per year	(R1*R2*5)	2,000
R4	Days per year	(R1*5)	250
R5	Fully burdened senior IT salary		$90,000
R6	Senior IT hourly	(R5/R3)	$45
R7	Fully burdened junior IT salary		$60,000
R8	Junior IT hourly	(R7/R3)	$30

Source: Forrester Research, Inc.

Table 5 provides access point density metrics used within this analysis.

Table 5: Access Point Density Metrics

Ref.	Metric	Calculation	Value
R9	Typical office square footage per occupant		250
R10	Recommended office square footage per access point for data		5,000
R11	Recommended office square footage per access point for location and voice		3,000

Source: Forrester Research, Inc.

Location

Introduction

Of the 12 interviewed organizations, one has deployed location tracking on the WLAN and two have completed pilots and plan to roll out full deployments within the next six to 12 months. Two of the three organizations are hospitals that track mobile medical devices including EKG machines, IV pumps, and glucometer kits, as well as other, often "hoarded," assets such as wheelchairs. Using location services, the interviewed hospitals noted a significant reduction in the time spent tracking down assets and expect to realize improved asset utilization. The third organization is a refining company tracking expensive movable equipment at its field locations and warehouses. The company has realized significant cost savings in not having to replace rented equipment that cannot be located.

Five of the 12 organizations are planning to deploy location tracking over the WLAN. One is a hospital with the primary driver of right-sizing expensive mobile inventory. Right now, doctors may order 10 scanning devices to make sure that one is always available. At a price of $100,000 per scanning device, this is a costly expenditure. With asset tracking, staff would be able to find a scanning device when it is required and reduce the number of devices held in inventory. Another organization, a university, plans to deploy location tracking on the card swipe machines for its auxiliaries group, as well as on equipment maintained by facilities. The transportation company hopes to deploy location tracking on ground support equipment including tugs, dollies, and jacks in order to cut the time currently wasted searching for parts and equipment. The lodging company is considering the deployment of location tracking on the luggage carts at its hotels. A final interviewee, the auto manufacturer, plans to use location tracking on mobile equipment in its plants. The manufacturer indicated that losing custom-built equipment is very expensive because it can require an entire assembly line to shut down to find a missing piece of equipment.

The remaining four interviewed organizations, including the school district, government agency, software provider, and large equipment distributor, do not have location tracking over the WLAN as a near-term objective.

Composite Organization

The composite company represents an organization with approximately 6,000 employees. Two years ago, IT staff at the company began a campuswide rollout of WLAN using a centralized architecture to provide data access for mobile employees and guests. The WLAN deployment was recently completed with 300 access points.

The organization currently performs an average of 34 asset searches per day to locate mobile assets, including servers, laptops, and other non-IT assets. An average search takes 30 minutes, and 5% of the time the search is unsuccessful. To reduce the time wasted searching for assets, IT staff plan to roll out location tracking for 4,750 mobile assets, including 1,750 assets frequently searched for, and 3,000 infrequently searched for assets like laptops.

Costs

This section reflects the overall costs of deploying location tracking on the wireless network, including: 1) network design update to include requirements for location tracking; 2) purchase of incremental access points, switches, and back-end infrastructure; 3) installation of incremental access points and infrastructure; 4) cost of the wireless location appliance; 5) installation of the wireless location appliance; 6) cost of asset tags (and ongoing costs to replace missing, stolen, and broken tags); 7) time and effort for IT staff to assign tags to all assets and enter tags in the asset management system; 8) training for IT staff on tagging and tracking mobile assets; and 9) ongoing management of asset management system.

Network Design To Include Requirements For Location Tracking

Network design costs depend on a variety of factors, including whether or not the original site survey included requirements for location tracking. Using information collected in the customer interviews, Forrester assumes that one senior IT employee spends two days on network design to include requirements for location tracking for the composite organization. At an hourly salary of $45 for the senior IT employee, the cost of network design is equal to $720 (= 1 x 2 x 8 x $45).

Table 6: Cost Of Network Design

Ref.	Metric	Calculation	Value
A1a	Senior IT staff required for network design to include requirements for location tracking		1
A1b	Days of network design		2
A1c	Cost of network design	(A1a*A1b*R2*R6)	$720

Source: Forrester Research, Inc.

Additional Access Points, Switches, And Back-End Infrastructure

Using a standard for location of 3,000 square feet per access point, 250 square feet per occupant and assuming 6,000 employees, the composite organization requires 500 access points to ensure coverage (= 6,000 x 250 / 3,000). The company has already deployed 300 access points, or 60% of the desired number of access points, and it will purchase and install 200 additional access points while rolling out location tracking.

A cost per access point of $1,000 is used in this analysis to include the cost of the access point and any required back-end infrastructure (e.g., additional switches and cabling). The cost of additional access points and back-end infrastructure is equal to the product of the cost per access point and the number of additional access points required, or $200,000 (= $1,000 x 200).

Table 7: Cost Of Access Points, Switches, And Back-End Infrastructure

Ref.	Metric	Calculation	Value
A2a	Number of new access points required for location tracking		200
A2b	Cost per access point (includes cost of back-end infrastructure)		$1,000
A2c	Cost of access points	(A2a*A2b)	$200,000

Source: Forrester Research, Inc.

Installation Of Additional Access Points, Switches, And Back-End Infrastructure

The cost to install the additional access points and infrastructure is equal to the product of the time to install each access point (building in time to install switches and back-end infrastructure), the junior IT hourly salary, and the total number of additional access points to install. Based on customer interviews, the average time to install a thin access point (with time built in to install switches and back-end infrastructure) is 1 hour. Therefore, the cost to the composite company to install the additional access points and back-end infrastructure is equal to $6,000 (= 1 x $30 x 200).

Table 8: Cost To Install Access Points, Switches And Back-End Infrastructure

Ref.	Metric	Calculation	Value
A3a	Hours to install per access point		1
A3b	Cost to install access points	(A3a*A2a*R8)	$6,000

Source: Forrester Research, Inc.

Wireless Location Appliance

Using market data, Forrester assumes that the cost of the wireless location appliance is equal to $15,000.

Table 9: Cost Of Wireless Location Appliance

Ref.	Metric	Calculation	Value
A4a	Cost of wireless location appliance		$15,000

Source: Forrester Research, Inc.

Installation Of Wireless Location Appliance

One senior IT employee spends one day, or 8 hours, to install the wireless location appliance. At an hourly rate of $45, the total cost to install the wireless location appliance is equal to $360.

Table 10: Cost To Install Wireless Location Appliance

Ref.	Metric	Calculation	Value
A5a	Senior IT staff required to install wireless location appliance		1
A5b	Days of installation		1
A5c	Cost to install wireless location appliance	(A5a*A5b*R2*R6)	$360

Source: Forrester Research, Inc.

Asset Tags

Of the 4,750 assets to be tracked, only 1,750 require asset tags (the 3,000 laptops have 802.11 devices built in). Market data provides the cost per asset tag of $65. The total cost to purchase asset tags in the initial year is equal to $113,750 (= 1,750 x $65). Forrester assumes that 1% of tags per week require replacement over the three-year analysis. This results in the replacement of 875 assets per year at a cost of $56,875. To reduce complexity, Forrester assumes no growth in assets to be tracked over the three-year period.

Table 11: Cost Of Asset Tags

Ref.	Metric	Calculation	Value
A6a	Cost of asset tag		$65
A6b	Number of assets to be tracked		4,750
A6c	Number of assets requiring asset tags		1,750
A6d	Percent of asset tags requiring replacement per week		1%
A6e	Ongoing number of assets tags to be purchased	(A6c*A6d*R1)	875
A6f	Initial cost of asset tags	(A6c*A6a)	$113,750
A6g	Ongoing cost of asset tags	(A6a*A6e)	$56,875

Source: Forrester Research, Inc.

Time To Tag Assets And Enter Serial Numbers Into Asset Management System

For each asset to be tagged, Forrester assumes that IT staff will spend one hour searching for the asset and fifteen minutes entering the serial number into the asset management system. At a junior IT hourly salary of $30, the initial cost to tag assets and enter the serial numbers into the system is equal to $88,125. The ongoing cost to replace missing, stolen, and broken tags is equal to $32,813.

Table 12: Cost To Assign Tags And Enter Tags Into Asset Management System

Ref.	Metric	Calculation	Value
A7a	Hours to locate and tag asset		1
A7b	Hours to enter serial number into asset management system (per asset)		0.25
A7c	Initial cost to assign tags to assets and enter tags into asset management system	(A6c*A7a*R8)+(A6b*A7b*R8)	$88,125
A7d	Ongoing cost to assign tags and enter tags into asset management system	(A6e)*((A7a+A7b)*(R8)	$32,813

Source: Forrester Research, Inc.

Training Costs For IT Staff

Four junior IT employees are trained on tagging and tracking mobile assets at a cost of $1,500 per employee. The total training cost is equal to $6,000.

Table 13: Cost Of Training

Ref.	Metric	Calculation	Value
A8a	Junior IT staff trained on asset tracking		4
A8b	Cost of training per employee		$1,500
A8c	Cost of training	(A8a*A8b)	$6,000

Source: Forrester Research, Inc.

Ongoing Administration For Asset Management System

Junior IT employees spend 4 hours per week for ongoing administration of the asset management system. The total cost of ongoing administration is equal to the product of the junior IT salary per hour, the number of hours per week, and the number of weeks per year, or $6,000.

Table 14: Cost Of Ongoing Administration For Asset Management System

Ref.	Metric	Calculation	Value
A9a	Junior IT staff hours per week for ongoing administration of asset management system		4
A9b	Cost of ongoing administration of asset management system	(A9a*R1*R8)	$6,000

Source: Forrester Research, Inc.

Total Costs

Table 15: Total Costs To Deploy Location Services, Non-Risk-Adjusted

Ref.	Project costs	Initial cost	Year 1	Year 2	Year 3	Total	PV
A1c	Cost of network design	$720				$720	$720
A2c	Cost of access points	$200,000				$200,000	$200,000
A3b	Cost to install access points	$6,000				$6,000	$6,000
A4a	Cost of wireless location appliance	$15,000				$15,000	$15,000
A5c	Cost to install wireless location appliance	$360				$360	$360
A6f	Cost of asset tags	$113,750	$56,875	$56,875	$56,875	$284,375	$255,190
A7c	Cost to assign tags	$88,125	$32,813	$32,813	$32,813	$186,563	$169,725
A8c	Cost of training	$6,000				$6,000	$6,000
A9b	Cost of ongoing administration of asset		$6,000	$6,000	$6,000	$18,000	$14,921
A10a	Total cost	$429,955	$95,688	$95,688	$95,688	$717,018	$667,916

Source: Forrester Research, Inc.

Benefits

Interviewed companies attribute quantifiable benefits to location tracking in the form of a reduction in time spent to locate assets and a reduction in the cost to replace missing assets. Higher returns are associated with companies that track very expensive mobile assets and assets that are critical to workflow.

Reduction In Time Spent Searching For Assets

On average, the composite organization searches for each of the 3,000 laptops once every 2 years. For the remaining 1,750 mobile assets, there are on average four searches performed per asset per year. In total, the organization performs 34 asset searches per day, or 8,500 searches per year (= 34 per day x 250 days per year).

Prior to the deployment of location tracking, IT employees spend on average 30 minutes per search to track down an asset. With the introduction of location tracking, IT employees spend on average 5 minutes to locate an asset. This results in a savings of 25 minutes per search. At a junior IT hourly salary of $30, the organization is able to save $106,250 per year (= $30 x 25 / 60 x 8,500) with location tracking over the WLAN.

Table 16: Savings From Reduction In Time Spent To Locate Assets

Ref.	Metric	Calculation	Value
A11a	Number of asset searches per day		34
A11b	Number of asset searches per year		8,500
A11c	Average length of asset search before location tracking (minutes)		30
A11d	Average length of asset search after location tracking (minutes)		5
A11e	Savings from reduction in time spent to locate assets	(A11b*((A11c-A11d)/60)*R8)	$106,250

Source: Forrester Research, Inc.

Reduction In Cost To Replace Missing Assets

With location tracking, organizations realize a reduction in the percent of searches that are unsuccessful. Prior to deploying location tracking, the composite company is unsuccessful in its searches 5% of the time. After implementing location tracking, the organization is unsuccessful in its searches only 1% of the time. As a result of the improvement in the success rate of searches, the company is required to replace 4% fewer assets. Forrester assumes that the average asset value is $1,200. The total annual savings is equal to the product of the number of searches per year, the percent improvement, and the average asset value, or $408,000 (= 8,500 x 4% x $1,200).

Table 17: Savings From Reduction In Cost To Replace Missing Assets

Ref.	Metric	Calculation	Value
A12a	Percent of asset searches that are unsuccessful before location tracking		5%
A12b	Percent of asset searches that are unsuccessful after location tracking		1%
A12c	Average asset value		$1,200
A12d	Savings from reduction in costs to replace missing assets	(A12c*(A12a-A12b)*A11b)	$408,000

Source: Forrester Research, Inc.

Qualitative Benefits

Through the 12 company interviews and general industry knowledge, Forrester identifies the following qualitative benefits associated with location services:

- Improved security with location-based security features (e.g., authentication, alerts for relocation)
- Improved employee productivity through location-based call routing and content distribution
- Improved IT productivity through location-based trend analysis (e.g., troubleshooting, RF capacity management based on location)
- Improved customer satisfaction through reduction in wait time for services (e.g., employees are able to locate wheelchairs immediately for patients who require them)

For the purpose of this study, these benefits are not quantified because they are too indirectly tied to financial returns.

Total Benefits

Table 18: Total Benefits From Location Services, Non-Risk-Adjusted

Ref.	Project benefits	Year 1	Year 2	Year 3	Total	PV
A11e	Savings from reduction in time spent to locate assets	$106,250	$106,250	$106,250	$318,750	$264,228
A12d	Savings from reduction in costs to replace missing assets	$408,000	$408,000	$408,000	$1,224,000	$1,014,636
A13a	Total benefits	$514,250	$514,250	$514,250	$1,542,750	$1,278,864

Source: Forrester Research, Inc.

Voice

Introduction

One of the 12 interviewed organizations, a hospital, has rolled out voice over the WLAN to 800 nurses in order to improve quality of care for patients. Now, patients can call for a nurse and be immediately connected. The hospital is awaiting standards-based voice devices of proven reliability to deploy dual-mode phones to doctors, who desire to carry one device both inside and outside of the hospital.

Five of the interviewed organizations are currently piloting voice over the WLAN. The transportation organization recently deployed VoWLAN to warehouse managers in one of its large facilities in order to avoid expensive cellular phone costs in a location where cellular coverage is poor. The university has replaced two-way pagers with IP wireless phones for its IT employees. The main driver is to allow employees to answer their desk phones anywhere they are on university grounds, which is a significant benefit to a university where meetings can occur all over campus. The three other organizations piloting the technology do not plan to move forward into full deployments. Although they see some benefits with VoWLAN, they believe that they can realize more significant benefits when carriers are able to provide dual-mode handsets and service.

Another two interviewed organizations would like to take advantage of voice over the WLAN but believe it is cost-prohibitive at this point because they have not yet deployed IP capability at the PBX (IPT). Two more are waiting for the cost of the IP wireless phone devices to come down before deploying. Another interviewee is waiting to complete a pervasive WLAN deployment before piloting voice over the WLAN. The final interviewed organization is currently using a proprietary wireless technology for voice and does not intend to switch to voice over the WLAN.

Composite Organization

The composite company represents an organization with 10,000 employees staffed in multiple buildings in a campus environment. The organization completed a pervasive WLAN deployment with centralized access points two years ago and deployed voice over IP technology (IPT, within the LAN) one year ago. The company now plans to undertake a role-based deployment of voice over the WLAN. Employees to receive voice over the WLAN capabilities are those that are highly mobile within the campus environment and those for whom reachability is important. Targeted mobile workers make up 10% of the workforce and include field service workers; repair personnel; and

point-of-care, monitoring, and auditing workers. The company chooses to wait for prices to drop for dual-mode phones before deploying voice over the WLAN to mobile executives.

Costs

This section reflects the overall costs of deploying voice services over the WLAN, including: 1) network design to include requirements for voice over the WLAN and a capacity use plan; 2) cost of additional access points, switches, and back-end infrastructure; 3) time and effort to install additional access points and infrastructure; 4) cost of IP wireless phones; 5) time and effort for IT staff to install VoWLAN and integrate it with the IP PBX; 6) time and effort for IT staff to handle user help calls; and 7) cost of incremental monitoring of the wireless network.

Network Design To Include Requirements For Voice Over WLAN

Using results from the interviews, Forrester assumes that two senior IT staff each spend five days on network design to include requirements for voice.

Table 19: Cost Of Network Design

Ref.	Metric	Calculation	Value
B1a	Senior IT staff required for network design to include requirements for VoWLAN		2
B1b	Days of network design		5
B1c	Cost of network design	(B1a*B1b*R2*R6)	$3,600

Source: Forrester Research, Inc.

Additional Access Points, Switches, And Back-End Infrastructure

Using a standard for data of 5,000 square feet per access point and 250 square feet per occupant and assuming 10,000 employees, the composite organization requires 500 access points. Forrester assumes that the composite organization has already deployed 500 access points but would now like to have one access point for every 3,000 square feet to ensure coverage for voice services over the WLAN. This requires a deployment of an additional 333 access points.

A cost per access point of $1,000 is used in this analysis to include the cost of the access point and any required back-end infrastructure (e.g., additional switches, cabling). The cost of adding 333 access points is equal to the product of the cost per access point and the number of additional access points required, or $333,000.

Table 20: Cost Of Access Points, Switches, And Back-End Infrastructure

Ref.	Metric	Calculation	Value
B2a	Number of additional access points required for voice		333
B2b	Cost per access point (includes cost of back-end infrastructure)		$1,000
B2c	Cost of access points	(B2a*B2b)	$333,000

Source: Forrester Research, Inc.

Installation Of Additional Access Points, Switches, And Back-End Infrastructure

The cost to install the additional access points, switches and back-end infrastructure is equal to the product of the time to install each access point (with time built in to install switches and back-infrastructure) of one hour, the Junior IT hourly salary, and the total number of additional access points to install. The cost to the composite company to install the additional access points, switches and back-end infrastructure is equal to $9,990.

Table 21: Cost To Install Access Points, Switches, And Back-End Infrastructure

Ref.	Metric	Calculation	Value
B3a	Hours to install per access point		1
B3b	Cost to install access points	(B3a*B2a*R8)	$9,990

Source: Forrester Research, Inc.

Wireless IP Phones

The cost of wireless IP phones is equal to the product of the cost per phone and the total number of mobile workers who will receive phones. Using market data, Forrester uses a price per wireless IP phone of $500. Ten percent of the workforce, or 1,000 employees, are mobile workers who will replace current cellular phones with wireless IP phones. The total cost of wireless IP phones for the composite organization is equal to $500,000.

Table 22: Cost Of IP Wireless Phones

Ref.	Metric	Calculation	Value
B4a	Cost per IP wireless phone		$500
B4b	Number of mobile employees		1,000
B4c	Cost of IP wireless phones	(B4a*B4b)	$500,000

Source: Forrester Research, Inc.

Installation And Integration Of VoWLAN With IP PBX

Forrester assumes that one senior IT employee spends two days to install and integrate voice services over the WLAN with the IP PBX. The total cost of installation and integration is equal to the product of the senior IT hourly rate and the number of hours of effort and is equal to $720.

Table 23: Installation And Integration Costs

Ref.	Metric	Calculation	Value
B5a	Senior IT staff required to install and integrate VoWLAN with IP PBX		1
B5b	Days of installation and integration		2
B5c	Installation and integration costs	(B5a*B4b*R2*R6)	$720

Source: Forrester Research, Inc.

Help Desk Support Costs

The composite company allocates two junior IT staff to resolve user help calls and deal with hardware issues for the 1,000 mobile workers with wireless IP phones. At a fully burdened annual salary of $60,000, help desk support costs equal $120,000.

Table 24: Installation And Integration Costs

Ref.	Metric	Calculation	Value
B6a	Junior IT staff required to support incremental calls to help desk		2
B6b	Cost to support incremental calls to help desk	(B6a*R7)	$120,000

Source: Forrester Research, Inc.

Incremental Monitoring Of WLAN

With a larger wireless LAN deployment like this one, IT employees must spend more time to monitor the wireless network. Forrester assumes that this requires an additional 2 hours per week of junior IT staff time. The total cost of incremental monitoring of the WLAN is equal to the product of the junior IT staff salary per hour, the number of additional hours per week and the number of weeks per year, or $3,000 (= $30 x 2 x 50).

Table 25: Cost Of Incremental Monitoring Of The Wireless Network

Ref.	Metric	Calculation	Value
B7a	Junior IT staff hours per week for incremental monitoring of the wireless network		2
B7b	Cost of incremental monitoring of the wireless network	(B7a*R8*R1)	$3,000

Source: Forrester Research, Inc.

Total Costs

Table 26: Total Costs Of Deploying Voice Over The WLAN, Non-Risk-Adjusted

Ref.	Project costs	Initial cost	Year 1	Year 2	Year 3	Total	PV
B1c	Cost of network design	$3,600				$3,600	$3,600
B2c	Cost of access points	$333,000				$333,000	$333,000
B3b	Cost to install access points	$9,990				$9,990	$9,990
B4c	Cost of IP wireless phones	$500,000				$500,000	$500,000
B5c	Installation and integration costs	$720				$720	$720
B6b	Cost to support incremental calls to help desk		$120,000	$120,000	$120,000	$360,000	$298,422
B7b	Cost of incremental monitoring of the wireless network		$3,000	$3,000	$3,000	$9,000	$7,461
B8a	Total cost	$847,310	$123,000	$123,000	$123,000	$1,216,310	$1,153,193

Source: Forrester Research, Inc.

Benefits

According to those interviewees that have deployed voice over the WLAN, there are two areas where quantifiable benefits may be realized: 1) avoidance of cellular or pager charges with free in-

house phone calls, and 2) improved mobile worker productivity through the ability to contact an employee anywhere within the enterprise. To realize these benefits, an organization must replace mobile worker's cellular phones or pagers with IP wireless phones and voice services over the WLAN, and these capabilities must be an improvement over existing voice services on cellular or pager networks (e.g., existing coverage). A number of interviewees indicated that poor cellular coverage is a reason why voice service over the WLAN is an improvement over the cellular network, and other interviewees noted that the variability in monthly cellular charges was a reason to switch from cellular service to voice over the WLAN.

Higher returns are associated with companies that have: 1) greater numbers of mobile workers who require access to voice services, and 2) more significant differences in services available through IP wireless phones and cellular or pager services.

Cost Avoidance Of Monthly Cellular Charges

Prior to the deployment of voice over the WLAN, the composite company incurs costs of $69 per month in cellular charges for each its mobile workers. Once cellular phones are replaced with IP wireless phones for the mobile workers, the organization is able to avoid this cost. The cost avoidance is equal to the product of the number of mobile workers (1,000), the monthly cellular charge, and the number of months per year, or $828,000.

Table 27: Cost Avoidance Of Monthly Cellular Charges

Ref.	Metric	Calculation	Value
B9a	Average monthly cellular charges per mobile worker		$69
B9b	Cost avoidance of monthly cellular charges	(B9a*12*B4b)	$828,000

Source: Forrester Research, Inc.

Improved Productivity For Mobile Workers

With voice services on the WLAN, employees can answer the desk phone from anywhere on campus. Forrester assumes that mobile workers save 30 minutes per week moving from cellular phones with spotty coverage to IP wireless phones on a pervasive WLAN deployment. To calculate the productivity gains of mobile workers, Forrester multiplies the time saved per week, the percent of time saved that translates into productive time, the average fully loaded annual salary per mobile worker per hour, and the total number of mobile workers. To be conservative, Forrester assumes that for mobile workers only 75% of time saved is converted into productive time. The total productivity gain for the composite organization is equal to $656,250.

Table 28: Productivity Gains For Mobile Workers

Ref.	Metric	Calculation	Value
B10a	Hours saved per week per mobile worker with VoWLAN		0.50
B10b	Average fully loaded annual salary per mobile worker		$70,000
B10c	Percent of hours saved translated into productive time		75%
B10d	Productivity gains for mobile workers	(B10a*R1*B10b/R3*B10c*B4b)	$656,250

Source: Forrester Research, Inc.

Qualitative Benefits

From results of the company interviews and general industry expertise, Forrester identifies the following qualitative benefits associated with voice services:

- Improved employee accessibility through unified messaging. With unified messaging, a user can access a single voicemail box or messaging mailbox, reducing time to return messages and improving accessibility to the user. VoWLAN also allows network capabilities like presence to be leveraged by mobile employees, improving right-time communications. Dual-mode handsets further improve employee accessibility as employees move inside and outside of the enterprise campus.

- Improved collaboration (e.g., a user is able to conference with three colleagues and view an upcoming presentation from anywhere geographically within the company; team members can contact each other anywhere across the enterprise by calling a single desk phone number)

- Decreased support costs for proprietary wireless voice systems

- Improved customer and employee satisfaction with enhanced mobility

- Improved visibility into costs because the enterprise controls all facility communication

These benefits are too indirectly tied to financial returns to be quantified in this study.

Total Benefits

Table 29: Total Benefits Of Voice Over the WLAN, Non-Risk-Adjusted

Ref.	Project benefits	Year 1	Year 2	Year 3	Total	PV
B9b	Cost avoidance of monthly cellular charges	$828,000	$828,000	$828,000	$2,484,000	$2,059,113
B10d	Productivity gains for mobile workers	$656,250	$656,250	$656,250	$1,968,750	$1,631,997
B11a	Total benefits	$1,484,250	$1,484,250	$1,484,250	$4,452,750	$3,691,110

Source: Forrester Research, Inc.

Guest Access

Introduction

Seven of the 12 interviewed organizations have implemented a guest network in order to provide visitors with wireless access to the Internet. Another two organizations are in the process of rolling out wireless guest networks. The remaining three interviewees are not currently providing wireless guest access, nor do they plan to offer guest access in the near future. The federal agency indicated that a guest network isn't necessary because even though all visitors are put through an intense security screening before being allowed onto campus, they are rarely allowed onto the wireless network. The large equipment distributor indicated that a guest network isn't required because the most frequent visitors to the sales offices are from corporate headquarters and they are automatically allowed onto the wireless network.

Three of the seven interviewees that have deployed guest access are hospitals, all of which indicated that primary drivers for guest access were a desire to compete with other local hospitals on patient perks, generate good public relations, and improve customer service. Revenue was not a driver for the hospitals. The remaining four organizations all had frequent visitors coming on-site to their corporate campuses and chose to deploy a guest network to reduce IT support costs to manage wireless guest access and to improve security by ensuring that guests do not have access to company confidential information. Secondary drivers were the ability to improve guest productivity while on-site and to improve customer service for visitors.

Composite Organization

Forrester created a composite organization based on the interviews and populated a financial framework using data from the interviews as applied to the composite organization. The composite company represents an organization with 7,500 employees dispersed across four corporate campuses. Approximately 200 vendors and other guests visit the corporate campuses each week. Over the past two years, the company has deployed a WLAN at its campuses with 338 centralized access points. Currently, the organization's WLAN network resides behind the firewall and the company does not have a segmented network for guests. Guests must be validated onto the network and given a user ID and password via an authorized employee. Approximately 30% of guests are allowed onto the wireless corporate network after an employee has validated them. This is a time-intensive effort for IT staff because it requires one person in the back room to register the IP address and a second person to physically go to the location of the guest and configure the device. The company estimates that IT staff spend one hour per visitor allowed onto the network. In addition, once a guest is on the network, he or she has access to all network resources, so this approach requires greater emphasis on ensuring that visitors do not gain access to company confidential resources.

The composite organization decides to deploy guest access on a segment of the network to provide visitors with direct access to the Internet. Guest access will be locked down such that visitors will be given the SSID name after signing in at the lobby and then will be asked to register on the site. IT staff at the company will not turn on encryption at the access points, nor will they broadcast the SSID for the guest network.

Costs

This section reflects the overall costs of deploying guest access on a segmented network, including: 1) network design to include requirements for guest access; 2) purchase of additional access points, switches, and back-end infrastructure; 3) installation of additional access points and infrastructure; 4) time and effort for IT staff to implement the guest network, including configuring the server to segment the network; and 5) incremental help desk support for guests who have trouble accessing the Internet.

Readers may wish to include in their own financial analyses any applicable software cost for guest access. Forrester has chosen not to include this in the model because of its variability and overall minor significance.

Network Design To Include Requirements For Guest Access

Forrester assumes that two senior IT staff each spends three days on network design to include requirements for guest access across the four corporate campuses. The cost of network design is equal to the product of the number of senior IT staff, the hourly salary, the number of days of network design, and the number of hours per day, or $2,160.

Table 30: Cost of Network Design

Ref.	Metric	Calculation	Value
C1a	Senior IT staff required for network design to include requirements for guest access		2
C1b	Days of network design		3
C1c	Cost of network design	(C1a*C1b*R2*R6)	$2,160

Source: Forrester Research, Inc.

Additional Access Points, Switches, And Back-End Infrastructure

The majority of interviewed customers purchased and installed additional access points in the process of deploying guest access. Using a standard for data of 5,000 square feet per access point, 250 square feet per occupant, and 7,500 employees, the composite organization requires 375 access points for a pervasive WLAN deployment (= 7,500 x 250 / 5,000). The company has already deployed 90% of the required access points and purchases and installs 37 additional access points while rolling out the guest network.

A cost per access point of $1,000 is used in this analysis to include the cost of the access point and any required back-end infrastructure. The cost to add 37 access points is equal to the product of the cost per access point and the number of additional access points, or $37,000.

Table 31: Cost Of Access Points, Switches And Backend Infrastructure

Ref.	Metric	Calculation	Value
C2a	Number of new access points required for guest access		37
C2b	Cost per access point (includes cost of back-end infrastructure)		$1,000
C2c	Cost of access points	(C2a*C2b)	$37,000

Source: Forrester Research, Inc.

Installation Of Additional Access Points, Switches, And Back-End Infrastructure

The cost to install the additional access points and infrastructure is equal to the product of the time to install each access point (building in time to install switches and back-end infrastructure), the junior IT hourly salary, and the total number of additional access points to install. Based on customer interviews, the average time to install a thin access point (with time built in to install the infrastructure) is 1 hour. Therefore, the cost to the composite company to install additional access points is equal to $1,110.

Table 32: Cost To Install Access Points, Switches, And Back-End Infrastructure

Ref.	Metric	Calculation	Value
C3a	Hours to install per access point		1
C3b	Cost to install access points	(C3a*C2a*R8)	$1,110

Source: Forrester Research, Inc.

Implementation Of Wireless Guest Access

Forrester assumes that a senior IT employee at each of the four corporate campuses spends 4 hours to configure the server to segment the network for guest access. The cost to implement the guest network is equal to the product of the number of senior IT employees, the senior IT hourly salary, and the number of hours of implementation, or $720.

Table 33: Implementation Costs For Guest Access

Ref.	Metric	Calculation	Value
C4a	Senior IT staff required to configure the server to segment the network for guest access		4
C4b	Hours to configure the server		4
C4c	Implementation costs for guest access	(C4a*C4b*R6)	$720

Source: Forrester Research, Inc.

Help Desk Support Costs

Interviewed organizations indicated minimal support costs associated with guest access. As a result, Forrester assumes an additional 2 hours per week to support additional calls to the help desk for visitors who have trouble accessing the Internet.

Table 34: Incremental Help Desk Support

Ref.	Metric	Calculation	Value
C5a	Junior IT staff hours per week to support calls to help desk for visitors		2
C5b	Cost of incremental help desk support for visitors	(C5a*R8*R1)	$3,000

Source: Forrester Research, Inc.

Total Costs

Table 35: Total Costs For Guest Access, Non-Risk-Adjusted

Ref.	Project costs	Initial cost	Year 1	Year 2	Year 3	Total	PV
C1c	Cost of network design	$2,160				$2,160	$2,160
C2c	Cost of access points	$37,000				$37,000	$37,000
C3b	Cost to install access points	$1,110				$1,110	$1,110
C4c	Implementation costs for guest access	$720				$720	$720
C5b	Cost of incremental help desk support for visitors		$3,000	$3,000	$3,000	$9,000	$7,461
C6a	Total costs	$40,990	$3,000	$3,000	$3,000	$49,990	$48,451

Source: Forrester Research, Inc.

Benefits

Interviewees identified the reduction in IT support costs to manage wireless guest access (including moves, adds, and changes) as a quantifiable benefit associated with guest access. Higher returns are associated with companies with large numbers of visitors arriving on campus with requirements for Internet access.

Reduction In IT Support Costs To Manage Wireless Guest Access

Prior to the deployment of wireless guest access, IT employees spend on average 1 hour per visitor requiring access to the network to register the IP address and configure the guest's device. Segmenting the wireless network for guests allows IT employees to avoid this task. Assuming that 200 guests visit the composite company's corporate campuses per week and 30% of the guests require access to the Internet, IT employees save 60 hours per week by providing wireless guest access. The value of the benefit is equal to the product of the junior IT salary per hour, the number of hours saved per week, and the number of weeks per year, or $90,000.

Table 36: Savings In Time Spent To Provide Guest Access

Ref.	Metric	Calculation	Value
C7a	Visitors per week on corporate campuses		200
C7b	Percent of visitors requiring network access		30%
C7c	Junior IT staff hours to configure visitor's machine prior to implementation of guest access		1
C7d	Savings in time spent to deliver guest access	(C7a*C7b*C7c*R1*R8)	$90,000

Source: Forrester Research, Inc.

Qualitative Benefits

Forrester has identified the following qualitative benefits associated with guest access:

- Improved security by ensuring that guests do not have access to company confidential information and by reducing viruses introduced by guests to the corporate network. This is because now guest connectivity is isolated into its own network segment.
- Improved customer service by extending network services to partners and other visitors. For certain organizations with frequent on-site visitors, providing visitors with guest access is not just a nice-to-have; it is a requirement. At hospitals, guests include patients and their visitors. Their satisfaction with the services provided by the hospital is incorporated into the hospital's quality of care score. At the software provider's corporate campus, guests are potential customers who are visiting the campus for on-site training sessions on the vendor's products.
- Improved network performance in shared space environments due to better RF usage and lower interference between user groups.
- Improved ability to retain visitors on-site, which for retail organizations can translate into increased sales.
- Improved perception of the organization as an advanced technology user by its partners and other guests.

These benefits are not quantified for the purpose of this study because they are too indirectly tied to financial returns.

Total Benefits

Table 37: Total Benefits For Guest Access, Non-Risk-Adjusted

Ref.	Project benefits	Year 1	Year 2	Year 3	Total	PV
C7d	Savings in time spent to deliver guest access	$90,000	$90,000	$90,000	$270,000	$223,817

Source: Forrester Research, Inc.

Advanced Security

Forrester considers two advanced security features in this study: 1) intrusion detection and prevention, and 2) single user identification using 802.1X authentication across the wired and wireless networks.

Introduction To Intrusion Detection And Protection

Six of the 12 interviewed organizations have wireless intrusion detection and prevention (IDS/IPS) working in conjunction with their centralized WLAN infrastructure. Interviewees discussed a significant improvement in rogue access point detection, monitoring, and containment with a centralized WLAN infrastructure and IDS/IPS as compared to distributed access points and no overlay for intrusion detection and prevention. The university mentioned that the "before and after" is dramatic. With a distributed architecture, IT employees were required to follow up on reports of problems and manually identify where the problems were occurring. With a centralized infrastructure and intrusion detection and prevention system, the university has seen a dramatic improvement in threat visibility and a reduction in the time spent monitoring and containing rogue access points. One hospital mentioned that with a central console and networkwide visibility, IT employees spend half as much time tracking rogue access points as they did before.

Another three organizations have purchased overlays for intrusion detection and prevention for their distributed architectures. Prior to purchasing an overlay, a hospital mentioned that it had numerous rogue access points show up and then disappear. This required someone on the IT staff to walk around, find the access point, and ask someone to remove it. Now they get a report every 15 minutes and spend seconds reading through the report to monitor rogue access points. For the transportation company, the main reason to deploy an overlay for improved security was because a news organization publicly implied that it could get into the company's wireless network.

One interviewee, the auto manufacturer, outsources its intrusion detection and prevention. The IT manager responsible for building the business case explained that his department was able to sell it easily by showing the cost of three major attacks to the wireless network resulting from viruses introduced to the wireless network. Each attack cost $1 million per facility.

The remaining two organizations have distributed architectures and have not invested in overlays, nor have they outsourced intrusion detection and prevention. The federal agency is investigating advanced security features such as intrusion detection and prevention but believes it has such high physical security at its site that this isn't a near term requirement. The large equipment distributor plans to roll out intrusion detection as it migrates from a thick architecture to a thin architecture.

Introduction To Single User Identification

One interviewee, a hospital, has deployed 802.1X across an integrated wired and wireless network. Another six companies are in the process of deploying integrated 802.1X on their wired and wireless networks. Right now, 802.1X is the way the university authenticates someone across the wired and wireless networks for a pilot group of users. Because the university's mechanism for

authentication is not built into the operating system currently in use, the university has been forced to work with third-party authentication supplicants. The software provider is using 802.1X style implementation on the wireless side to ensure that users get onto the right network and authenticate, but currently the company has not integrated this with the wired network. In the wired space, the software provider is using it to identify employee machines. The challenge for the company has been managing group policy capabilities. Interviewees expect to realize improvements in security pertaining to unauthorized access and theft of proprietary information and a reduction in operating expenses to handle the moving parts in the identity/authentication process with single user identification.

The transportation company has approval and is ready to go forward with an integrated wired/wireless 802.1X implementation. The challenge for this organization has been legacy ring scanners with dumb DOS. The options were to either replace the devices or upgrade the devices. The company partnered with a third party to push the security configurations downward to the devices. The auto manufacturer has been trying to deploy 802.1X for the past two years on the wireless network but has struggled because the company's laptop vendor is not working well with the WLAN vendor.

The remaining five organizations are investigating 802.1X but have no current plans to deploy it on the wireless network.

Composite Organization

The composite company represents a large organization with 15,000 employees. The organization deployed a WLAN network four years ago using a distributed architecture and WEP for security. For improved management, the organization plans to deploy a centralized architecture integrated with the wired network that has intrusion detection and prevention for monitoring and containing RF-related attacks. The organization also plans to deploy WPA2, or 802.11i, and integrate 802.1X on the wired and wireless networks.

Costs

This section reflects the overall costs of deploying intrusion detection and prevention and single user identification: 1) cost to deploy intrusion detection and prevention; 2) cost to deploy 802.1X on the wired and wireless networks; and 3) cost to integrate 802.1X across the wired and wireless networks.

Deployment Of Intrusion Detection And Prevention

Forrester takes a two-step approach to calculate the cost to deploy intrusion detection and prevention for the composite organization. First, Forrester calculates the total cost for the composite organization to deploy a WLAN with centralized architecture. Second, Forrester attributes a percent of the cost to deploy the centralized WLAN to the need for intrusion detection and prevention.

For the first step, Forrester uses a standard for data of 5,000 square feet per access point and 250 square feet per occupant and assumes 15,000 employees. Therefore, the composite organization needs to deploy 750 access points. Forrester assumes a cost per access point of $1,700 to include the cost of the access point, a portion of the switch and cabling costs, the cost for design and installation, and the cost to configure the device for 802.1X. The total cost to deploy the centralized WLAN is equal to $1,275,000.

For the second step, Forrester assumes that 25% of the total cost to deploy the centralized WLAN is attributed to the desire for intrusion detection and prevention. (The primary reasons to move from a distributed, decentralized architecture with a lot of intelligence in thick access points to a centralized architecture using thin access points with intelligence are for easier management and

the ability for the WLAN network to act in a coordinated fashion.) The total cost of deploying intrusion detection and prevention is therefore equal to $318,750 (= $1,275,000 x 25%).

Table 38: Cost of Intrusion Detection And Prevention

Ref.	Metric	Calculation	Value
D1a	Number of access points deployed for thin WLAN architecture		750
D1b	Cost per access point (includes cost for design and installation, back-end infrastructure, and configuration of 802.1X)		$1,700
D1c	Cost to upgrade to thin WLAN architecture	(D1a*D1b)	$1,275,000
D1d	Percent of cost to upgrade to thin WLAN architecture attributed to need for IDS/IPS		25%
D1e	Cost of IDS/IPS	(D1c*D1d)	$318,750

Source: Forrester Research, Inc.

Deployment Of 802.1X

Forrester takes a three-step approach to calculate the cost to deploy and integrate 802.1X across the wired and wireless networks. The first step is to calculate the cost to upgrade edge switches on the wired network and configure the switches for 802.1X. The second step is to attribute a percent of the cost to upgrade the edge switches to the need for integration of 802.1X across the wired and wireless networks. The third step is to calculate the cost to configure the remaining edge switches for 802.1X on the wired network and to solve any integration problems with 802.1X on the wired and wireless networks.

For step one, Forrester calculates the total number of edge switches required to support the composite organization on the wired network. Assuming a 48-port switch and 15,000 employees, the organization requires 313 edge switches for the wired network (= 15,000 / 48). Forrester assumes that the majority of edge switches have been upgraded previously and now only 30%, or 94 switches, must be upgraded to support 802.1X. Using market data, Forrester uses a cost per 48-port switch of $10,000 and to that adds a 15% markup to take into account the additional cost to configure the switch to turn on 802.1X. The total cost to upgrade the edge switches is equal to $1,081,000 (= $10,000 x (1 + 0.15) x 94).

In step two, Forrester assumes that 25% of the total cost to upgrade the edge switches is attributed to the desire for integrated 802.1X across the wired and wireless networks. Forrester only assumes 25% of the cost because other factors including end of life of switches and increased capacity on the wired networks comprise the majority of the impetus to upgrade edge switches. The cost of deploying 802.1X on the upgraded edge switches is equal to $270,250.

For the third step, Forrester assumes that two senior IT employees each spend 40 days to configure the remaining edge switches on the wired network and to solve any integration issues for 802.1X across the wired and wireless networks. The total cost is equal to the product of the number of senior IT employees required, the senior IT hourly salary, the number of days of work required, and the number of hours per day, and is equal to $28,800 (= 2 x $45 x 40 x 8). The total cost to deploy 802.1X on the wired and wireless networks is equal to $299,050 (= $270,250 + $28,800).

Table 39: Cost To Deploy 802.1X On Wired And Wireless Networks

Ref.	Metric	Calculation	Value
D2a	Number of employees		15,000
D2b	Total edge switches to support wired infrastructure (assumes 48 ports per switch)	(D2a/48)	313
D2c	Percent of edge switches that must be upgraded to support 802.1X		30%
D2d	Total switches that must be upgraded to support 802.1X	(D2b*D2c)	94
D2e	Cost per 48-port edge switch		$10,000
D2f	Incremental cost to configure edge switch to turn on 802.1X		15%
D2g	Cost to upgrade edge switches for 802.1X	(D2d*D2e*(1+D2f))	$1,081,000
D2h	Percent of total cost to upgrade switches attributed to the need for integration of 802.1X on wireless/wired networks		25%
D2i	Senior IT staff required to configure remaining edge servers for 802.1X and to solve any integration problems with 802.1X on wired and wireless networks		2
D2j	Days to configure and solve integration issues		40
D2k	Cost to deploy 802.1X on wireless/wired networks	((D2g*D2h)+(D2i*D2j*R2*R6))	$299,050

Source: Forrester Research, Inc.

Total Costs

Table 40: Total Costs For Advanced Security, Non-Risk-Adjusted

Ref.	Project costs	Initial cost	Year 1	Year 2	Year 3	Total	PV
D1e	Cost of IDS/IPS	$318,750				$318,750	$318,750
D2k	Cost to deploy 802.1X on wireless/wired networks	$299,050				$299,050	$299,050
D3a	Total costs	$617,800	$0	$0	$0	$617,800	$617,800

Source: Forrester Research, Inc.

Benefits

Interviewees identified two categories of benefits associated with intrusion detection and protection: 1) faster identification and containment of rogue access points, and 2) reduction in losses from

exposure to viruses because IDS/IPS can stop a self-propagating worm and confine it to a particular area of the network. Forrester quantifies the first benefit but does not quantify the second benefit because of its variability.

With single user identification, interviewees expect to realize a reduction in operating expenses and improved protection against unauthorized users and theft of proprietary information.

Faster Identification And Containment Of Rogue Access Points

Prior to the deployment of intrusion detection and prevention, junior IT staff spend on average 3 hours per week walking around the corporate offices to search for rogue access points and, when one is located, asking the owner to remove it. With intrusion detection and prevention, IT employees are able to detect, monitor, and contain rogue access points by spending minutes per day reviewing reports. Forrester assumes that IT employees are able to save 2 hours per week with intrusion detection and prevention. At an hourly salary of $30 for junior IT staff, the total cost savings is equal to $3,000 per year, or the product of the hourly salary, the number of hours saved per week, and the number of weeks saved per year (= $30 x 2 x 50).

Table 41: Savings From Faster Identification And Containment Of Rogue Access Points

Ref.	Metric	Calculation	Value
D4a	Hours spent per week by junior IT staff tracking, monitoring, and containing rogue access points prior to IDS/IPS		3
D4b	Hours spent per week by junior IT staff tracking, monitoring and containing rogue access points after IDS/IPS		1
D4c	Hours saved per week for junior IT staff	(D4a-D4b)	2
D4d	Savings from faster identification and containment of rogue access points	(D4c*R1*R8)	$3,000

Source: Forrester Research, Inc.

Reduction In Operating Expenses With 802.1X Authentication

Prior to the deployment of 802.1X on the wired and wireless networks, Forrester assumes that the composite company has an eight-to-one support ratio of switches to full-time equivalents (FTEs). Once 802.1X has been deployed across the wired and wireless networks, Forrester assumes that this ratio improves by 35%; one FTE can now support 11 switches. The organization has 313 edge switches on the wired network and six switches on the wireless network, for a total of 319 switches. Using the initial support ratio (prior to deployment and integration of 802.1X across the wired and wireless networks), the organization requires 40 junior IT employees to support the switches. After the deployment of 802.1X, the organization requires only 29 junior IT employees to support the switches. The annual savings to the composite organization are equal to $660,000 (= 11 x $60,000).

Table 42: Savings In Operating Expenses With 802.1X Authentication

Ref.	Metric	Calculation	Value
D5a	Total switches on wired network with 802.1X turned on		313
D5b	Total switches on wireless network with 802.1X turned on		6
D5c	Support ratio (switches per FTE) prior to 802.1X on wired/wireless networks		8
D5d	Number of junior IT staff required to support switches prior to 802.1X	((D5a+D5b)/D5c))	40
D5e	Productivity improvement with 802.1X		35%
D5f	Support ratio (switches per FTE) after 802.1X on wired/wireless networks	(D5c*(1+D5e))	11
D5g	Number of junior IT staff required to support switches after 802.1X	((D5a+D5b)/D5f))	29
D5h	Savings from fewer junior IT staff required to support switches after 802.1X	((D5d-D5g)*R7)	$660,000

Source: Forrester Research, Inc.

Reduction In Exposure To Losses From Unauthorized Access

The 2005 CSI/FBI Computer Crime and Security Survey provides an estimate for losses from unauthorized access of $48,878 per survey respondent per year. In the survey, unauthorized access includes “network entry” unauthorized access and “resource” unauthorized access (e.g., OS, folder, or application unauthorized access; authorization creep). Given that 802.1X across wired/wireless virtually eliminates losses from network entry unauthorized access but does not impact resource unauthorized access, Forrester assumes a 40% reduction in overall loss from unauthorized access. This results in an annual cost savings to the composite organization of $19,551 (= $48,878 x 40%).

Reduction In Exposure To Losses From Theft Of Proprietary Information

The 2005 CSI/FBI Computer Crime and Security Survey also provides an estimate for losses from theft of proprietary information, in this case in an amount of $48,408 per survey respondent per year. The survey does not break out the loss into authorized versus unauthorized network access. Because a large majority of data breaches are accidental, Forrester assumes a conservative 15% reduction in overall loss from theft of proprietary information attributed to single user identification, or integrated 802.1X across the wired and wireless networks. This results in an annual cost savings to the composite organization of $7,261 (= $48,408 x 15%).

Table 43: Savings From Reduction In Exposure To Losses From Unauthorized Access And Theft Of Proprietary Information

Ref.	Metric	Calculation	Value
D6a	Average annual dollar amount loss for unauthorized access prior to deployment of advanced security		$48,878
D6b	Percent reduction in exposure to losses from unauthorized access with advanced security features		40%
D6c	Value of reduction in exposure to losses from unauthorized access with advanced security features	(D6a*D6b)	$19,551
D6d	Average annual dollar amount loss for theft of proprietary information prior to deployment of advanced security		$48,408
D6e	Percent reduction in exposure to losses from theft of proprietary information with advanced security features		15%
D6f	Value of reduction in exposure to losses from theft of proprietary information with advanced security features	(D6d*D6e)	$7,261

Source: Forrester Research, Inc.

Qualitative Benefits

Through the 12 company interviews and general industry knowledge, Forrester has identified the following qualitative benefits associated with advanced security:

- Improved safeguarding of the brand (eliminate spoofing of the wireless network)
- Provision of a platform for physical security (e.g., IP video surveillance, badge readers)
- Improved employee security protection through reduction in phishing incidents
- Potentially improved regulatory compliance

These benefits are too indirectly tied to financial returns to be quantified in this study.

Total Benefits

Table 44: Total Benefits From Advanced Security, Non-Risk-Adjusted

Ref.	Project benefits	Year 1	Year 2	Year 3	Total	PV
D4d	Savings from faster identification and containment of rogue access points	$3,000	$3,000	$3,000	$9,000	$7,461
D5h	Savings from fewer junior IT staff required to support switches after 802.1X	$660,000	$660,000	$660,000	$1,980,000	$1,641,322
D6c	Value of reduction in exposure to losses from unauthorized access with advanced security features	$19,551	$19,551	$19,551	$58,654	$48,621
D6f	Value of reduction in exposure to losses from theft of proprietary information with advanced security features	$7,261	$7,261	$7,261	$21,784	$18,058
D7a	Total benefits	$689,813	$689,813	$689,813	$2,069,438	$1,715,462

Source: Forrester Research, Inc.

Risk

Risk is the third component within the TEI model; it is used as a filter to capture the uncertainty surrounding different cost and benefit estimates. If a risk-adjusted ROI still demonstrates a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as "realistic" expectations, since they represent the expected values considering risk. In general, risks impact costs by raising the original estimates and impact benefits by reducing the original estimates.

For the purpose of this analysis, Forrester risk-adjusts cost and benefit estimates to better reflect the level of uncertainty that exists for each estimate. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points.

For example, take the case of the cost of network design to include requirements for location tracking. The $720 value used in this analysis can be considered the "most likely" or expected value. The cost of network design, however, will vary based on an organization's pre-existing environment. This variability represents a risk that must be captured as part of this study. Forrester assumes a medium level of risk associated with the cost of network design and uses a risk factor of 115% on the high end, 100% as the most likely, and 100% on the low end (costs are rarely lower than the most likely, or expected, value). This has the effect of increasing the cost estimate to take into account the fact that original cost estimates are more likely to be revised upward than downward. Forrester then creates a triangular distribution to reflect the range of expected costs, with 105% as the mean (105% is equal to the sum of 115%, 100%, and 100% and then divided by three). Forrester applies this mean to the most likely estimate, $720, to arrive at a risk-adjusted value of $756.

Risk adjustments for benefits reduce the original benefits estimates. For example, Forrester applies a risk range of 50% on the low end of the estimate and 100% on the most likely and high end for

reduction in time spent to locate assets. This has the effect of reducing the benefit estimate by 16.67% so that it is now equal to 83.33% of the original value of $106,250, or $88,542.

See Appendix A for details on the risk level applied to each cost and benefit estimate.

Forrester considered the following general risk in this study:

- The risk that cost savings and productivity gains realized by other organizations may vary from those realized by the interviewed customers.

Forrester considered the following risk specific to location services in this study:

- The risk of a poor site survey that results in the deployment of too few access points to successfully track assets.

Forrester considered the following risk specific to voice services in this study:

- The risk that an organization does not have an IP PBX in place before deploying VoWLAN. This would require a significant additional investment to implement a gateway to translate voice signals to an IP format.

- The risk of a poor capacity design that results in a poor user experience, with a noticeable drop in call quality using VoWLAN.

Forrester considered the following risk specific to guest access in this study:

- The risk that a significant portion of visitors have trouble getting onto the guest network, necessitating IT employees to support these guests.

Forrester considered the following risk specific to advanced security in this study:

- The risk that an organization has a significantly larger portion of switches older than three years that must be upgraded. Enterprises commonly upgrade LAN switching infrastructure every five years, but those that are specifically looking to deploy an integrated wired/wireless switch-based WLAN or network quarantine may have to acquire the newer versions now.

Flexibility

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment (described in more detail in Appendix B).

An investment in a wireless LAN provides an organization with multiple flexibility options, including the four highlighted in this study: location, voice, guest access, and advanced security. The up-front investment in the WLAN allows an organization, with some future incremental investment, to take advantage of advanced services and realize benefits in the form of: 1) reduction in time spent to locate assets and cost to replace missing assets with location tracking; 2) avoidance of cellular charges and improved mobile worker productivity with voice services; 3) lower cost to provide visitors with access to the Internet through guest access; 4) a reduction in time spent to monitor and contain rogue access points with IDS/IPS and a reduction in operating expenses and exposure to losses from unauthorized access and theft of proprietary information with single user identification.

TEI Framework: Summary

Considering the financial framework constructed above, the results of the costs, benefits, flexibility, and risk sections using the representative numbers can be used to determine a return on investment, net present value, and payback period. Table 45 shows the consolidated risk-adjusted values for Location, applying the risk factors identified in Tables 49 and 50 (shown in Appendix A) to the numbers in Tables 15 and 18.

Table 45: Risk-Adjusted Financial Results For Location

Metric	Initial	Year 1	Year 2	Year 3	Total	PV
Risk-adjusted project costs						
Cost of network design	$756				$756	$756
Cost of access points	$202,000				$202,000	$202,000
Cost to install access points	$6,060				$6,060	$6,060
Cost of wireless location appliance	$15,750				$15,750	$15,750
Cost to install wireless location appliance	$378				$378	$378
Cost of asset tags	$119,438	$59,719	$59,719	$59,719	$298,594	$267,949
Cost to assign tags	$89,006	$33,141	$33,141	$33,141	$188,428	$171,422
Cost of training	$6,060				$6,060	$6,060
Cost of ongoing administration of asset management system		$6,300	$6,300	$6,300	$18,900	$15,667
Total costs	$439,448	$99,159	$99,159	$99,159	$736,926	$686,042
Risk-adjusted project benefits						
Savings from reduction in time spent to locate assets		$88,542	$88,542	$88,542	$265,625	$220,190
Savings from reduction in costs to replace missing assets		$340,000	$340,000	$340,000	$1,020,000	$845,530
Total benefits	$0	$428,542	$428,542	$428,542	$1,285,625	$1,065,720
Risk-adjusted cash flow						
Cash flow	($439,448)	$329,382	$329,382	$329,382	$548,699	$379,677
ROI						55%
Payback period (months)						16

Source: Forrester Research, Inc.

Table 46 shows the consolidated risk-adjusted values for Voice, applying the risk factors identified in Tables 51 and 52 (shown in Appendix A) to the numbers in Tables 26 and 29.

Table 46: Risk-Adjusted Financial Results For Voice

Metric	Initial	Year 1	Year 2	Year 3	Total	PV
Risk-adjusted project costs						
Cost of network design	$3,900				$3,900	$3,900
Cost of access points	$336,330				$336,330	$336,330
Cost to install access points	$10,090				$10,090	$10,090
Cost of IP wireless phones	$525,000				$525,000	$525,000
Installation and integration costs	$780				$780	$780
Cost to support incremental calls to help desk		$126,000	$126,000	$126,000	$378,000	$313,343
Cost of incremental monitoring of the wireless network		$3,150	$3,150	$3,150	$9,450	$7,834
Total costs	$876,100	$129,150	$129,150	$129,150	$1,263,550	$1,197,277
Risk-adjusted project benefits						
Cost avoidance of monthly cellular charges		$690,000	$690,000	$690,000	$2,070,000	$1,715,928
Productivity gains for mobile workers		$546,875	$546,875	$546,875	$1,640,625	$1,359,997
Total benefits	$0	$1,236,875	$1,236,875	$1,236,875	$3,710,625	$3,075,925
Risk-adjusted cash flow						
Cash flow	($876,100)	$1,107,725	$1,107,725	$1,107,725	$2,447,075	$1,878,648
ROI						157%
Payback period (months)						9

Source: Forrester Research, Inc.

Table 47 shows the consolidated risk-adjusted values for Guest Access, applying the risk factors identified in Tables 53 and 54 (shown in Appendix A) to the numbers in Tables 35 and 37.

Table 47: Risk-Adjusted Financial Results For Guest Access

Metric	Initial	Year 1	Year 2	Year 3	Total	PV
Risk-adjusted project costs						
Cost of network design	$2,268				$2,268	$2,268
Cost of access points	$37,370				$37,370	$37,370
Cost to install access points	$1,121				$1,121	$1,121
Implementation costs for guest access	$756				$756	$756
Cost of incremental help desk support for visitors		$3,150	$3,150	$3,150	$9,450	$7,834
Total costs	$41,515	$3,150	$3,150	$3,150	$50,965	$49,349
Risk-adjusted project benefits						
Savings in time spent to deliver guest access		$84,900	$84,900	$84,900	$254,700	$211,134
Total benefits	$0	$84,900	$84,900	$84,900	$254,700	$211,134
Risk-adjusted cash flow						
Cash flow	($41,515)	$81,750	$81,750	$81,750	$203,735	$161,785
ROI						328%
Payback period (months)						6

Source: Forrester Research, Inc.

Table 48 shows the consolidated risk-adjusted values for Advanced Security, applying the risk factors identified in Tables 55 and 56 (shown in Appendix A) to the numbers in Tables 40 and 44.

Table 48: Risk-Adjusted Financial Results For Advanced Security

Metric	Initial	Year 1	Year 2	Year 3	Total	PV
Risk-adjusted project costs						
Cost of IDS/IPS	$345,313				$345,313	$345,313
Cost to deploy 802.1X on wireless/wired networks	$323,971				$323,971	$323,971
Total costs	$669,283	$0	$0	$0	$669,283	$669,283
Risk-adjusted project benefits						
Savings from faster identification and containment of rogue access points		$2,830	$2,830	$2,830	$8,490	$7,038
Savings from fewer junior IT staff required to support switches after 802.1X		$550,000	$550,000	$550,000	$1,650,000	$1,367,769
Value of reduction in exposure to losses from unauthorized access with advanced security features		$16,293	$16,293	$16,293	$48,878	$40,518
Value of reduction in exposure to losses from theft of proprietary information with advanced security features		$6,051	$6,051	$6,051	$18,153	$15,048
Total benefits	$0	$575,174	$575,174	$575,174	$1,725,521	$1,430,372
Risk-adjusted cash flow						
Cash flow	($669,283)	$575,174	$575,174	$575,174	$1,056,238	$761,089
ROI						114%
Payback period (months)						14

Source: Forrester Research, Inc.

It is important to note that values used throughout the TEI Framework are based on in-depth interviews with 12 organizations and the resulting composite organizations built by Forrester. Forrester makes no assumptions as to the potential return that other organizations will receive within their own environment. Forrester strongly advises that readers use their own estimates within the framework provided in this study to determine the expected financial impact of implementing Mobility Services.

Study Conclusions

The financial analysis provided in this study illustrates the potential way an organization can evaluate the value proposition of Mobility Services.

- **Location.** With location tracking, interviewees find quantifiable benefits in a reduction in the amount of time spent to locate assets and a reduction in the cost to replace missing assets. The ROI for the composite company is 55%, with a breakeven point of 16 months after deployment.

  The qualitative benefits associated with location services include: improved security with location-based security features; improved employee productivity through location-based call routing and content distribution; improved IT productivity through location-based trend analysis; and improved customer satisfaction through reduction in wait time for services.

- **Voice.** Organizations using voice over the WLAN realize quantifiable benefits in the form of avoidance of cellular or pager charges for mobile workers and improved mobile worker productivity. The ROI for the composite company is 157%, with a breakeven point of nine months after deployment.

  The qualitative benefits associated with voice services include: improved employee accessibility through unified messaging; improved employee collaboration; decreased support costs for proprietary wireless voice systems; improved customer and employee satisfaction through enhanced mobility; and improved visibility into costs because all facility communication is controlled by the enterprise.

- **Guest Access.** Organizations using a guest network to provide visitors with wireless access to the Internet identify as a quantifiable benefit a reduction in IT support costs to manage wireless guest access. The ROI for the composite company is 328%, with a breakeven point of six months after deployment.

  The qualitative benefits associated with guest access include: improved security; improved customer service; improved network performance in shared space environments; improved ability to retain visitors on-site; and improved perception of the company as an advanced technology user by partners and other guests.

- **Advanced Security.** Forrester examined two advanced security features in this study: intrusion detection and prevention and single user identification through integrated 802.1X on the wired and wireless networks. Interviewees attribute quantifiable benefits in the form of faster identification and containment of rogue access points and a reduction in exposure to losses from viruses with IDS/IPS. Organizations attribute a reduction in operating expenses and improved protection against unauthorized users and theft of proprietary information with single user identification. The ROI for the composite company is 114%, with a breakeven point of 14 months after deployment.

  The qualitative benefits associated with advanced security include: improved safeguarding of the brand; provision of a platform for physical security; improved employee security protection through a reduction in phishing incidents; and potentially improved regulatory compliance.

Using the TEI framework, many companies may find the potential for a compelling business case to make an investment in Mobility Services.

Appendix A: Risk Analysis

For the purpose of this analysis, Forrester risk-adjusts cost and benefit estimates to better reflect the level of uncertainty that exists for each estimate. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points. Different benefit and cost estimates have different levels of risk adjustments. Readers are urged to apply their own risk ranges based upon their own degree of confidence in the cost and benefit estimates.

Location

The following tables show the values used to adjust for uncertainty in cost and benefit estimates for location services.

Table 49: Cost Category Risk Adjustments For Location Services

Ref.	Risk to cost	Risk level	Low	Most likely	High	Risk-adjusted
A1c	Cost of network design	Medium	100%	100%	115%	105.0%
A2c	Cost of access points	Low	98%	100%	105%	101.0%
A3b	Cost to install access points	Low	98%	100%	105%	101.0%
A4a	Cost of wireless location appliance	Medium	100%	100%	115%	105.0%
A5c	Cost to install wireless location appliance	Medium	100%	100%	115%	105.0%
A6g	Cost of asset tags	Medium	100%	100%	115%	105.0%
A7d	Cost to assign asset tags and enter serial number into asset management system	Low	98%	100%	105%	101.0%
A8c	Cost of training	Low	98%	100%	105%	101.0%
A9b	Cost of ongoing administration of asset management system	Medium	100%	100%	115%	105.0%

Source: Forrester Research, Inc.

Table 50: Benefit Category Risk Adjustments For Location Services

Ref.	Risk to benefit	Risk level	Low	Most likely	High	Risk-adjusted
A11e	Savings from reduction in time spent to locate assets	High	50%	100%	100%	83.3%
A12d	Savings from reduction in costs to replace missing assets	High	50%	100%	100%	83.3%

Source: Forrester Research, Inc.

Voice

The following tables show the values used to adjust for uncertainty in cost and benefit estimates for voice services.

Table 51: Cost Category Risk Adjustments For Voice Services

Ref.	Risk to cost	Risk level	Low	Most likely	High	Risk-adjusted
B1c	Cost of network design	High	100%	100%	125%	108.3%
B2c	Cost of access points	Low	98%	100%	105%	101.0%
B3b	Cost to install access points	Low	98%	100%	105%	101.0%
B4c	Cost of IP wireless phones	Medium	100%	100%	115%	105.0%
B5c	Installation and integration costs	High	100%	100%	125%	108.3%
B6b	Cost to support incremental calls to help desk	Medium	100%	100%	115%	105.0%
B7b	Cost of incremental monitoring of the wireless network	Medium	100%	100%	115%	105.0%

Source: Forrester Research, Inc.

Table 52: Benefit Category Risk Adjustments For Voice Services

Ref.	Risk to benefit	Risk level	Low	Most likely	High	Risk-adjusted
B9b	Cost avoidance of monthly cellular charges	High	50%	100%	100%	83.3%
B10d	Productivity gains for mobile workers	High	50%	100%	100%	83.3%

Source: Forrester Research, Inc.

Guest Access

The following tables show the values used to adjust for uncertainty in cost and benefit estimates for guest access.

Table 53: Cost Category Risk Adjustments For Guest Access

Ref.	Risk to cost	Risk level	Low	Most likely	High	Risk-adjusted
C1c	Cost of network design	Medium	100%	100%	115%	105.0%
C2c	Cost of access points	Low	98%	100%	105%	101.0%
C3b	Cost to install access points	Low	98%	100%	105%	101.0%
C4c	Implementation costs for guest access	Medium	100%	100%	115%	105.0%
C5b	Cost of incremental help desk support for visitors	Medium	100%	100%	115%	105.0%

Source: Forrester Research, Inc.

Table 54: Benefit Category Risk Adjustments For Guest Access

Ref.	Risk to benefit	Risk level	Low	Most likely	High	Risk-adjusted
C7d	Savings in time spent to deliver guest access	Medium	80%	100%	103%	94.3%

Source: Forrester Research, Inc.

Advanced Security

The following tables show the values used to adjust for uncertainty in cost and benefit estimates for advanced security.

Table 55: Cost Category Risk Adjustments For Advanced Security

Ref.	Risk to cost	Risk level	Low	Most likely	High	Risk-adjusted
D4d	Cost of IDS/IPS	High	100%	100%	125%	108.3%
D2k	Cost to deploy 802.1X on wireless/wired networks	High	100%	100%	125%	108.3%

Source: Forrester Research, Inc.

Table 56: Benefit Category Risk Adjustments For Advanced Security

Ref.	Risk to benefit	Risk level	Low	Most likely	High	Risk-adjusted
D4d	Savings from faster identification and containment of rogue access points	Medium	80%	100%	103%	94.3%
D5h	Savings from fewer junior IT staff required to support switches after 802.1X	High	50%	100%	100%	83.3%
D6c	Value of reduction in exposure to losses from unauthorized access with advanced security features	High	50%	100%	100%	83.3%
D6f	Value of reduction in exposure to losses from theft of proprietary information with advanced security features	High	50%	100%	100%	83.3%

Source: Forrester Research, Inc.

Appendix B: Total Economic Impact™ Overview

Total Economic Impact™ is a methodology developed by Forrester Research, Inc. that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI™ methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. For the purpose of this analysis, the impact of flexibility was not quantified.

Benefits

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the forms of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

Risk

Risk measures the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: the likelihood that the cost and benefit estimates will meet the original projections and the likelihood that the estimates will be measured and tracked over time. TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefit.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point in time. However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their organization to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total net present value of cash flows.

Payback period: The breakeven point for an investment. The point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A Note On Cash Flow Tables

The following is a note on the cash flow tables used in this study (see the Example Table below). The initial investment column contains costs incurred at “time 0” or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years one through three are discounted at the end of the year using the discount rate shown in Table 3. Present value (PV) calculations are calculated for each total cost and benefit estimate. Net present value (NPV) calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Example Table

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.