PDA SECURITY

Incorporating Handhelds into the Enterprise

David Melnick
Mark Dinman
Alexander Muratov

Bob Elfanbaum
Elena Muratova
Darren Ruotolo
Doug Stephan

McGraw-Hill
New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

Library of Congress Cataloging-in-Publication Data

Melnick, David.
PDA security : incorporating handhelds into the enterprise / David Melnick.
p. cm.
ISBN 0-07-142490-3
1. Computer security. 2. Portable computers—Programming. 3. Mobile computing. I. Title.

QA76.9.A25M445 2003
005.8—dc21 2003052791

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7 6 5 4 3

ISBN 0-07-142490-3

The sponsoring editor for this book was Judy Bass, the production supervisor was Sherri Souffrance, and the art director for the cover was Anthony Landi. It was set in Fairfield by MacAllister Publishing Services, LLC.

Printed and bound by RR Donnelley.

This book is printed on recycled, acid-free paper containing a minimum of 50 percent recycled de-inked fiber.

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, McGraw-Hill, 2 Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.

CHAPTER FOUR

WHEN A HANDHELD BECOMES INFORMATION TECHNOLOGY'S PROBLEM

Assessing Your Corporate Risk Profile

Whether or not the IT group, senior management, or employees believe handhelds pose a risk that should be addressed, the reality is that the devices already in place have compromised strategic information assets. In many organizations today, IT has not assumed responsibility for corporate-owned handhelds, even within those organizations that directly purchased *personal digital assistants* (PDAs) for a specific business application or group. More importantly, IT has generally not assumed responsibility for how employees' personal PDAs interact with corporate PDAs.

INFORMATION TECHNOLOGY PROFESSIONALS PROBLEM

The IT professionals driving problem stems from both a security and management challenge. This problem leads to the conclusion that IT professionals must directly set standards and policies, and ultimately control the purchasing of handheld devices. This need to exercise control to address management and security challenges is a reaction to both the rapid proliferation of these devices, and to the increasingly important role they play in employees' information management tasks.

When PCs were introduced to Enterprises, the IT groups of most large organizations were primarily responsible for the management and development of large mainframe systems. Most IT groups, and many organizations for that matter, did not immediately recognize the impact PCs would have on giving individuals control over the automation of business processes and associated information. As a result, IT groups in many cases were not given the authority and budget to purchase and implement solutions using PCs. As discussed previously, they entered the Enterprise in an uncoordinated fashion.

Similar to the early era of PCs, handhelds from various manufacturers are used in Enterprises and run on different *operating system* (OS) platforms. Handhelds, for the most part, are not even coordinated by a department or group; they are still in large part individually purchased devices. Thus, standards for handheld use are rare, and little to no guidance is provided on how they may hook up to the corporate network. As employees try to get their own devices to work, they must each go through the same discovery process or get help from their coworkers, potentially affecting others' ability to get work accomplished. As a result, in addition to the security challenges driving IT management and control, a great deal of lost productivity and other inefficiencies occur.

Security and Management

The theme of security and management as related challenges will emerge in almost all organizations should be addressed as one problem. IT professional's ability to develop a standards-based management of devices within an organization is integrally connected to both the asset management and security challenge.

When PCs originally entered the corporate scene, it caused a tremendous change due to the new hardware and software that had to be managed. To avoid repeated efforts, this management challenge consolidated control into a coordinated and often centralized IT organization.

Handhelds today are in a similar state of change in the hardware and software area, with even more compressed product life cycles than PCs faced in the early 1980s. Without IT management, the rapid introduction of new handheld hardware and software into the Enterprise will not only affect productivity for the individual, but it will also dramatically increase the challenge of providing device management and security.

Enterprises experienced an often painful expansion of PC programs during the early 1980s. Over time, IT professionals were charged with managing the introduction and support of PCs in the organization to help coordinate that growth. Whether Enterprises end up buying handhelds for their employees, or they mingle the use of their personal PDAs with corporate resources, IT professionals must be responsible for the management of handhelds in order to do the following:

- Avoid costly time wasted in getting handheld technology working efficiently with desktops and networks.
- Bring economies of scale in the purchase of handheld hardware and software where applicable.
- Pool efforts to support handhelds in the Enterprise.

Handhelds Touch IT-Managed Assets

As we explore the security issues associated with handhelds, we find that risk primarily stems from the ease with which end-users can integrate devices with IT-managed PDAs that have access to strategic information. In short, PDAs are primarily designed to link to a user's desktop computer and download information. Handhelds can and, for the most part, do interact with many other areas for which IT is responsible. The major areas we'll look at include access to desktops or networks and the information stored on them.

For the purposes of this section, we'll simplify the classification of handhelds into two categories: wireless versus nonwireless. Most normal PDAs do not include wireless capabilities (excluding, for now, expansion cards or slots that make a nonwireless handheld a wireless one). These PDAs can easily be configured and synchronized with an employee's desktop or laptop.

IT employees are generally already responsible for maintaining polices or procedures on how to handle information that is classified as proprietary and may be synced. Most organizations have already established how classified electronic information should be marked and stored, and who has access to different levels of proprietary information. As soon as employees hook up their personal PDA to a desktop and syncs or downloads any information classified as proprietary, this creates a significant vulnerability in an organization's infrastructure. Whatever employees have access to on corporate networks or desktops can be easily downloaded and taken with them on their ultraportable PDAs.

Generally, however, it is easier for IT professionals to control the use of wireless devices, as they often manage standard network transports or "gateways" that have been implemented with security controls already. IT professionals must allow wireless devices to access corporate networks via *virtual private networks* (VPNs) or corporate email systems; employees can generally be prevented from establishing their own VPN or corporate email access using their wireless device. Although the

threat is seemingly greater for wireless devices, the more prevalent nonwireless devices pose the greatest risk. Just because of the sheer numbers, the pricing, and the availability of nonwireless devices, they introduce a far greater risk of allowing information to be compromised.

Because IT professionals are already responsible or accountable for desktop access, network access, and system security, they are increasingly compelled to control how PDAs access the existing infrastructure. As soon as an employee synchronizes their PDA and downloads any sort of corporate-associated data, suddenly a hole arises in the security of the Enterprise, for which IT is responsible. IT professionals are also accountable for the risk associated with a PDA that an employee brings in and hooks up to his or her desktop.

Even though IT employees are not formally responsible for the handheld budget, it is something for which they are held accountable. In many cases, handhelds are introduced to the organization by senior management employees, who turn to their IT specialist to help them effectively sync their new gadget with their desktop or laptop. Most IT specialists won't turn down this request, even if they are not formally charged with this type of support. Handheld devices are typically considered to be a companion device that are always used in conjunction with a desktop or laptop. Part of what makes them so appealing is how they can be used to seamlessly keep information in both places up-to-date.

With accountability already implied, IT departments recognize the need to ensure that security and management risks will be properly controlled as handheld devices' role in the organization expands. At this point, the organization must determine the nature of their security risk by focusing on the following questions:

- How are handhelds getting into their organization?
- What kind of information is at risk?
- Are there any projects in the works to deploy mission-critical applications that could expose information on handheld devices?

- Are external factors present, such as federal laws or regulations, that might require extra protection for information residing on handheld devices?

SECURITY RISK MANAGEMENT OF PDAs IN THE ENTERPRISE

What exactly is the risk that PDAs present to the Enterprise? Before you answer that question and start looking for solutions, you must go through a risk-management planning exercise. This exercise will help you assess what is at risk and what needs to be done to monitor and control the risk to your organization.

The following section examines assessing potential risks, discussing the following topics:

- Risk item identification.
- Risk analysis.
- Risk response planning, monitoring, and control.

It seems intuitive that due to the portable nature of PDAs, they can easily be lost or stolen. However, without going through some risk management, one cannot entirely understand how a lost PDA can threaten the Enterprise or its customers.

Risk Item Identification

The first step is to identify who is potentially exposing the Enterprise to risk. In the case of PDAs, the organization should get a handle on how PDAs are entering, what types of employees or groups are using them, and how they are using them. Key questions to study include:

- How are handhelds getting into your Enterprise?
- Are they coming in as personal devices, or are they part of corporate purchases and application deployments?

- What types of employees are using them? What are their roles and responsibilities?

These initial questions should be studied as you formulate strategies to address the risk that handheld devices might pose to your organization.

Risk Analysis

Once your organization understands how handhelds are coming into the Enterprise and who is using them, you can begin studying which type of information is at risk. In most cases, this consists of understanding how the various employees are using handhelds in their ongoing business activities. Is it primarily individuals who have purchased their own PDAs and are using them primarily for PIM applications? Or are groups deploying vertical applications on handhelds for mobile workers?

At the core of your analysis will be a handheld risk classification document, which will be illustrated as we sum up how to assess overall vulnerability. The classification, similar to a data classification exercise, allows an organization to build a matrix including categories such as device types and information assets in order to understand the related risk factors determining an organization's overall vulnerability.

Some additional questions include the following:

- What information are those handheld users carrying on those devices?
- What unintended information are those handheld users carrying on those devices?
- Does your organization have a process in place to classify which information is proprietary and should be actively protected?
- Do employees access any corporate-proprietary information solely on site, or do they have access to it off site?
- Regardless of need, what proprietary information are they accessing off site?

- Do you have plans to deploy mission-critical applications on a handheld platform? If so, do these applications include access or the generation of proprietary data?
- Have you reviewed your business processes recently to identify the impact of handhelds?

Risk Response Planning, Monitoring, and Control

Once an Enterprise has an understanding of how PDAs are entering the organization, who is using them, and what proprietary data is accessed, it can begin looking at risk-response strategies on how to safeguard the information residing on the handheld devices. Some of the questions to address in this process are as follows:

- How tightly does the organization want to control the use of corporate-owned devices?
- What type of policy will the organization adopt for controlling the use of devices owned by individual employees?

Depending on the nature of the proprietary information involved, some organizations may be forced to take a hard-line approach in which no personal handhelds can be used on site or that company-proprietary information cannot be stored on them. Chapter 5 discusses the steps IT groups can take to monitor and control the risk that handhelds present to the organization.

RISK ITEM IDENTIFICATION: WHO IS BRINGING HANDHELDS INTO YOUR ORGANIZATION?

The first step in looking at your Enterprise's risk is to determine exactly how handhelds are entering your organization and where

they are coming in contact with your organization's infrastructure. Although a number of companies have begun to implement specific mission-critical applications for handheld devices, most have not actively brought handhelds into their business. However, with at least 20 million devices manufactured and sold by Palm, Inc. alone, a large number of handhelds have been purchased by consumers, many of whom are employees in organizations.

According to the *International Data Corporation* (IDC), roughly 20 percent of purchased devices in 2002 were bought directly by organizations. That number is expected to grow to 29 percent in 2003. Although this is a substantial expansion with more corporate purchasing expected, the vast majority of devices still belong to individuals.[1]

As a result, many of these devices are finding their way into organizations through a "backdoor" without the direct knowledge or sanction of corporate IT departments. Looking at the two major categories of handhelds (wireless and nonwireless), most employees are more than likely using nonwireless devices because of the relatively low cost. Also, most of these devices are being purchased for basic personal information management capabilities; that is, the ability to have schedules, contacts, and notes at their fingertips. For this reason, it is likely that most of these users would attempt to sync their handhelds to their PCs in the workplace.

Far fewer wireless handheld devices enter your organization through the backdoor than nonwireless devices. Unless IT professionals sanction the use of corporate email on wireless devices, most of these devices will touch the corporate network primarily in the same way as the nonwireless devices. Because of the relatively high price point and corporate support required to hook them up to the organization's infrastructure, you will generally be much more aware of the use of wireless devices used.

---

[1]Gaudin, Sharon. "IT Expected to Push Enterprise Handheld Adoption." *Datamation*, 25 June, 2002.

Although a number of organizations are beginning to purchase PDAs either for employees or for specific business areas, the majority of them are personally owned by employees. Most of the Enterprise PDA managers have begun to look at the issue of security. However, many of them are struggling with how to apply policies and impose security requirements on handheld devices that are personal assets of employees.

Although a few organizations are beginning to outfit large groups of employees, such as sales departments, with PDAs, corporate-issue PDAs are the exception today. The majority of PDAs coming into your Enterprise will be through the backdoor, without the support or sanction of corporate IT groups. This backdoor entry of personal devices requires a risk item identification process to focus on who is bringing handhelds into the organization and for what purpose.

Employee Backdoor: The Profile of Employees Who Are Likely to Bring a PDA to the Office

Examining which types of employees are most likely to use a PDA as part of their daily work can be done in a number of ways. We will take three different views of employees:

- *Technogeeks* Those who gravitate toward new technology on their own.
- *Job function* Those employees whose personal productivity could benefit from a PDA.
- *Organization or industry function* What the organization produces or the services it provides.

Technogeeks A definite set of early consumers exists in almost every organization. They don't all have to be the first to purchase something, but they will often be among the first to use it on a regular basis long before the mainstream consumer. With PDAs, a core set of avid users existed when the first handhelds were commercially available in the mid-1990s. However, within five years, that core set of avid users increased to hun-

dreds of thousands as the number of total PDAs sold reached into the millions by the year 2000.

The number of users and their relative enthusiasm can be gauged by the web sites or communities that support handheld enthusiasts. A brief list of a few of the most common sites is as follows:

- www.brighthand.com
- www.palminfocenter.com
- www.pdageek.com
- www.pdabuzz.com
- www.pdastreet.com

Many of these sites offer news articles on the handheld industry, product reviews, technology conference reports, and so on. Many of them also provide not only links to price comparison and search engines, but they sell the products themselves in their attempt to be a one-stop shop for PDA enthusiasts. One of the most important aspects these sites provide is a forum where enthusiasts can compare notes and offer advice to newbies. One of the most active web sites is brighthand.com[2], where visitors must register with the site in order to post comments or questions with the other 15,000 registered users. They can post to dozens of forums to talk about hardware, software, and industry news, or pose questions. Frequently, many consumers doing research or trying to decide which type of handheld hardware or software to purchase will post questions to get a number of experienced users' views.

The technogeeks are generally comfortable with using technology, especially new technology. They aren't afraid of stumbling through learning how to use the new devices effectively. Unfortunately, this can also affect the organization where the

[2]www.alexa.com reports that Brighthand has the largest reach and traffic of all of the other handheld sites. It has 40,000 registered members, 50,000 posts a month in 100 forums, 4–5 million page views, and 200,000 unique visitors from over 120 countries.

individual's productivity might suffer. But once they are up-to-speed with the new technology, they will often become proponents of PDAs, as they will be more than happy to spread the knowledge and provide informal support to other users in the corporation. This has its advantages in that the use of handhelds can increase without any official training or support provided by the Enterprise. Of course, this is also a disadvantage, as the organization does not control how the technology is being implemented, which returns to the potential security threat.

Job Functions The second category of employee likely to bring in his or her own handheld device is someone whose personal job performance would immediately benefit from the use of a PDA. These types of employees are as follows:

- Executives using PDAs for immediate access to summarized reporting of vital key information.
- Salespeople or mobile workers requiring product data or *customer relationship management* (CRM) system access.
- Account managers and project managers leveraging PDAs for strong project management.

Although these employees are probably motivated to excel in their jobs (which most would be, or they wouldn't be holding their positions for very long), they do not necessarily have to be technogeeks. Of course, the two categories are not mutually exclusive! A number of senior managers and sales executives were the first to purchase PDAs as soon as they were available, because they like to experiment with the latest technology in handheld devices. Although some obvious crossover between these two categories can be noticed, we will assume for now that the majority of employees who have their own PDAs are doing it because they perceive it will help them with their job and career.

For many, the basic PIM functionality is reason enough. Any of the previously mentioned employees can benefit from having

all their contacts, their schedule, and other pieces of information at their fingertips at all times. However, many of these employees can also excel by taking advantage of the benefits that wireless handheld devices offer. In fact, it is generally senior management employees who sponsor (or push for) a pilot program for handheld usage, particularly wireless handhelds, within their group. As a result, handhelds that come into the organization from the most visible employee groups are not always via the backdoor. However, as we'll discuss later, this only increases the need for IT professionals to have plans and policies in place to handle the various implementation and security issues.

Organization Type The third means for bringing PDAs into the Enterprise via the backdoor is related to the function of the organization or group within the Enterprise. One example is a law firm where an individual's time represents the corporate product, and specialized skills must be accessible at any time. For this reason, lawyers, who historically have not adopted technology quickly, have rapidly adopted the BlackBerry devices providing always-on email access. Although we will discuss industry examples at a later point, such as healthcare and patient privacy laws, lawyers exchanging confidential information via email clearly illustrate why IT professionals must understand PDA use to mitigate any substantial risks.

When and Why an Organization Buys Devices for Its Employees

In addition to PDAs entering the Enterprise via the backdoor of personal purchases, certain organizations are purchasing handhelds for specific groups. This is being done for a number of different reasons. Here are some examples:

- CRM applications increase sales information mobility.
- Productivity applications reduce expenses by automating business processes.

- Various other killer applications are being used in categories including executive information reporting, email, and more every day.

In general, the corporate purchasing of devices is driven by applications that offer some organizations a compelling case. However, some sectors that have shown uneven adoption of these applications. Two particular areas or groups in which corporate purchasing has been more widespread includes sales (with CRM-related applications) and executives (with quick access to information and email). From an industry perspective, healthcare, government, and financial services have been rapid adopters, among others.

Healthcare Numerous examples of handheld deployment can be found in the healthcare field. The portable nature of handhelds, combined with the need for workers to be able to move from patient to patient quickly, makes handheld device deployment a natural fit for numerous applications in the healthcare field.

Let's look at an example from Palm, Inc. The Naval Medical Center in Portsmouth, New Hampshire, is the oldest, continuously running hospital for the U.S. Navy.[3] It delivers state-of-the-art healthcare to naval personnel and their families. Physicians at the Naval Medical Center at Portsmouth needed to find a better way to communicate patient information for personnel on various shifts.

The Naval Medical Center developed and implemented an application running on Palm devices that gives physicians easy access to information from patient files as well as reference information, contact information, and other notes and data. The system replaced handwritten notes on cards, thereby reducing the chance for errors from unreadable notes. It also saved time, allowing for easier and quicker access to information. The

[3]Palm Solutions Group. "Palm Success Stories." 2002, http://www.palm.com/enterprise/studies/.

implementation also made the transition between shifts more efficient. Physicians can easily synchronize patient information and case histories so that staff have the information they need literally at their fingertips. In addition to the primary benefits of increasing worker productivity, the organization also benefited from being able to provide a higher quality of service to their patients.

Government Handhelds have proven to be an effective tool for federal, state, and local government entities. Two examples of PDA implementations from Palm's "Success Stories" include the U.S. Navy and the Alabama Department of Transportation.

The quick and efficient capture of critical data is a must in the U.S. Navy. One example where handhelds greatly facilitate the capture of accurate data is on the flight decks of aircraft carriers. Using Palm devices, Navy personnel aboard the *USS Constellation* and *USS Abraham Lincoln* grade aircraft landings. The previous system required personnel to quickly record landing grades and comments in notebooks. This made accurate record-keeping difficult, and correcting mistakes distracted one from the next landing, particularly when it was hard to see at night.

Two Navy commanders developed a handheld application that enabled personnel to quickly record grades and enter comments for each landing. Errors were reduced and corrected more easily on the backlit PDA devices. The personnel were also able to quickly synchronize the data they captured during their shift, reducing errors from the previous process.

In another example, field inspectors for the Alabama Department of Transportation were using a construction management application to automate the record-keeping processes for their projects. Unfortunately, because the application only ran on a desktop or laptop computer, they were forced to take their notes manually in the field and bring them back to the office to key in later.

The field inspectors and officials from other states asked the manufacturer of the construction management application to create a handheld component that would enable field inspec-

tors to use the software in the field and work in an integrated fashion with their office computers. The handheld application allowed inspectors to download the appropriate information into their handheld, where they could record data throughout their day. This information was synchronized at the end of the shift on the desktop. This made data collection much more accurate and efficient, and it eliminated the inaccuracies of handwritten notes and data entry mistakes. Additionally, the built-in PIM and other productivity tools (such as calculators) in the handhelds reduced the number of other devices that inspectors had to carry with them in the potentially hazardous construction environment.

Financial Services Handhelds are also utilized by a number of Enterprises to help give them a competitive advantage. An example from Palm's "Success Stories" is Sun Life Financial. Sun Life is an international financial service organization that provides a variety of wealth protection products and services to individuals and corporate customers.

Among Sun Life's products are variable life insurance products. Rapidly changing market information makes staying informed of the latest news a significant challenge. Sun Life wanted to provide its brokers with a mobile solution that could provide immediate and detailed product information that could be updated periodically. This would help their brokers provide more accurate and profitable products and services to their customers.

Sun Life provided Palm devices to a group of their brokers so they could easily access a variety of funds and product information. Updates could be stored and distributed via *Secure Digital* (SD) cards containing quarterly fund performance information. The handhelds provided Sun's brokers with the most up-to-date product information, allowing them to better serve their customers. The PIM applications built into the handhelds also allowed the brokers to have quick and easy access to contact information that could also be kept current with SD cards.

RISK ANALYSIS: WHEN DOES THIS THREAT REQUIRE ACTION?

In the previous section, we looked at identifying handhelds' risks in the Enterprise. Specifically, we discussed how handheld devices enter the organization, who is most likely to use them, and how. The next step in the risk assessment and management process is to gain a better understanding of the impact of risk on the handheld devices. In this section, we will explore:

- What kinds of information can get on PDAs.
- How PDAs interface with various parts of the Enterprise infrastructure.

What Information Is on Those Things?

As discussed previously, the majority of devices within an organization have been purchased by employees who are using primarily nonwireless devices and PIM applications. They want quick access to contact information, calendars, and other information at their fingertips. As a result, a great deal of the information stored on these devices is personal in nature. This could include information such as:

- Personal addresses and phone numbers.
- Financial information such as credit card and bank accounts.
- Web site account and password information.

Personal Information Although the corporation doesn't have any direct responsibility for employee's personal and financial information, some unintended consequences could occur if that employee loses his or her device. For instance, contact information for the employee's colleagues and coworkers could be stored on the device. If the PDA falls into the hands of a com-

petitor or recruiter, he or she could have instant access to a number of people in your organization if the data on the device is not secure.

Also, just because much of the information an employee keeps on his or her personal device is personal in nature does not mean that *all* of it is. A quick survey will generally uncover the following:

- Business or coworker contact information.
- Customer or partner contact information.
- Company benefits and financial information.
- Internal web site access addresses.
- Business-related web site accounts.
- Business and personal passwords.

The lines between personal and business PIM information can become quickly blurred. The notion of completely segregating personal from business information essentially flies in face of being able to use the PDA and PIM applications effectively. Although it is possible to ask or expect employees to keep two separate PDAs—one for personal and one for business information—in the increasing effort at reducing number of devices (such as phone, pager, and PDA), separate devices may prove to be an impractical solution.

Corporate Information Most organizations would like their employees to be as effective and productive as possible. Thus, having one device that carries both personal and business-related information seems to make sense. As a result, corporate information will undoubtedly make its way onto the device, whether it is personal or corporate-owned. Some examples of corporate data you wouldn't want to have floating around insecure include the following:

- Customer lists and contact information.
- Direct report personnel information (for managers).

- Strategic partner or vendor contact information.
- Pricing and proposal information.
- Corporate web site account and password information.
- Network or VPN account and password data.

Depending on the responsibilities an employee has, any amount of sensitive information could be stored on a personal device. Thus, it should be an area of concern that this information is being stored, in the majority of cases, on an employee's personal device. As a result, a device being lost or stolen would have a significant impact.

Beyond the PIM use of the device, the increasing array of business applications is driving the purchasing of handheld devices. Applications such as *Executive Information Services* (EIS) and mobility versions of CRM systems are causing the migration of mission-critical data from Enterprise-based computers to handheld devices. This data often has generally understood risks associated with its loss, including operational as well as confidentiality risks.

How Are They Interfacing With My Infrastructure?

In addition to identifying which types of corporate-proprietary information is potentially stored on handheld devices, the organization needs to understand, influence, and, if possible, control who, what, when, and how the data is transferred or synced to the handheld device. Several options are available:

- Direct cable or cradle connections between the handheld device and the employee's corporate laptop or desktop computer.
- Cable or cradle connection between the handheld device and the corporate network, arbitrated by the desktop but managed by a server service.

- Dial-up access between the handheld device and data stored on the corporate network.
- Wireless access between the handheld device and data stored on the corporate network and in email accounts.

Whatever information an employee has access to from his or her desktop or via corporate network connections can be easily synced to a handheld device for quick and easy access.

How to Assess Your Vulnerability

We recommend an exercise to develop a *security risk classification* (SRC) document to evaluate and assess your vulnerabilities. The exercise is based on making assessments of your exposure in the four areas described below. With a focus on the handheld device, this exercise will provide you with a basis and aid in developing a multidimensional approach to assessing your exposure. The SRC is composed of four discreet matrices or tables for each of the following:

- *Industry* Legal requirements or other industry-specific issues.
- *Organization* Cultural norms and usage patterns specific to your Enterprise.
- *Access medium* The range of devices and their capabilities and limitations.
- *Information assets* Confidentiality, operational risk of loss, and life expectancy.

Each area should be broken down into elements that are specific or relevant to your organization. For example, Table 4-2 displays six different types of Information Assets. Your organization could have 10 more relevant information assets. For each element you can add a row in the matrix or table and assess a value for the Information Classifications in each column. Table 4-1 displays the information classifications and sample values for each classification.

TABLE 4-1. Information Risk Classification Matrix Setup

Information	Classifications	
Class A	Confidentiality	
	100	Highest level of confidentiality
	50	Private and sensitive information about Enterprise/client/vendor
	25	Private information about client/vendor
	1	Publicly accessible
Class B	Operational Risk of Loss	
	100	Critical to business operation: Enterprise cannot function if lost
	80	Critical to business operation: Enterprise's ability to operate seriously impaired if lost
	60	Critical to business operation: Client/vendor's ability to operate seriously impaired if lost
	40	Important to business operation: Enterprise/client/vendor negatively affected if lost
	20	General value to Enterprise/client/vendor
	1	Of no material business consequence if lost
Class C	Retention/Access Requirements	
	100	Real-time access, no expiration
	80	Real-time access for 9 months, 48-hour retrieval for 7 years
	65	Real-time access for 6 months, 48-hour retrieval for 7 years
	50	Real-time access for 1 day, 48-hour retrieval for 7 years
	30	Real-time access for 9 months, no retrieval after expiration
	20	Real-time access for 6 months, no retrieval after expiration
	10	Real-time access for 3 months, no retrieval after expiration
	1	Real-time access for 1 day, no retrieval after expiration

TABLE 4-2. Risk Classification Matrix Measuring Six Information Types

Information Assets	Class A	Class B	Class C	Total
Employee contact information	100	40	1	141
Customer contact information	100	80	50	230
Vendor contact information	100	100	20	220
Customer sales data	100	60	20	180
Network passwords	100	100	100	300
Corporate financial data	100	100	50	250

How to Develop the Classification Framework The set of matrices will be used to set the objective levels of risk that any PDA can be measured against. Once the specific PDA and its associated industry, organization, access mediums, and information assets are defined, the PDA will be assigned an overall risk classification. The numeric score assigned to each PDA will represent its risk across a number of dimensions, or values within the matrix. Security response policies will need to be developed to assign to PDAs based on the resulting numeric score. These policies that are assigned based on the numeric scores will result in some PDAs with relatively slight security measures and others with substantial security precautions.

The overall security exercise can be implemented with a wide spectrum of complexity. It can range from a simple, single-dimensional matrix with a cumulative numeric assessment, as illustrated in Table 4-1, or as an Enterprise-wide multidimensional approach to security policy implementation, requiring multiple matrixes such as those illustrated in Table 4-2.

The following section illustrates how this process, much like the development of a standard data classification document, is dependent on establishing the right values and models for its success. In order to illustrate the use of this framework, Table 4-1 uses the information matrix with the following three key values for evaluation: Operational Risk of Information Loss;

Confidentiality of Information; and Retention Requirements for the Information. In Table 4-1, higher scores representing greater risks are established for each dimension or value. The cumulative score for all values of a particular information asset represents its overall information risk as defined by the matrix.

Once your values are assigned to the matrix and a scoring model has been assigned to each value, each asset can be measured by the matrix. In this case, the assets would include the types of information. The next step requires the development of a comprehensive categorizing of the information assets you expect to be on the PDAs. The following implementation of the information matrix defined in Table 4-1 is illustrated in Table 4-2. Table 4-2 demonstrates the results of an evaluation of six types of information using the matrix.

The score results can be used to assign policies to various PDAs based on their level of risk as defined by the matrix. In this example, the PDAs containing information, which has a score at various numeric thresholds, can be required to implement various policies, the enforcement of which we will illustrate in Chapter 6. In general, a set of increasingly strong security measures can be developed as a response strategy. You can use this framework for scoring and then assign the threat level to a particular user's PDA based on the information assets expected to reside on that particular PDA.

Although we have focused solely on the information assets area in our example matrix (Table 4-2), a complete SRC should also consider the other areas. For instance, access mediums, which refers to the range of ways that handheld devices come in contact with an organization's data, must be included in any Enterprises' assessment. Collectively, we increasingly need to address the network-enabled applications that can run on devices, such as Microsoft's Terminal Services Client on network-aware PocketPC devices. The ability to reset a password or to change user permissions should be factored into your risk assessment and can be included as elements in a matrix addressing the range and degree of vulnerabilities for the access mediums area.

Understanding How to Address Industry-Level Issues Part of assessing your Enterprise's risk is recognizing which internal and external factors affect your business. For certain industries, regulatory considerations must be covered. Some industries, as we will illustrate, have specific requirements to meet regarding information security, while others face a less regulated environment with lower overall risks. However, generally speaking, all businesses face some level of obligation to provide basic levels of protection for their client and employee information.

Healthcare Looking at the healthcare field, the obvious regulations affecting the flow and processing of electronic information is the *Health Insurance Portability and Accountability Act* (HIPAA). HIPAA was passed in 1996 and in August of 2002 it had its final regulations approved, further implementing the act. This law addresses the responsibility of healthcare organizations to safeguard patient information, which they fundamentally do not own but rather hold in trust on behalf of the patient. The law outlines a number of objectives that must be enforced whether the information resides on a mainframe system or on a PDA.

In addition to addressing the responsibility of healthcare organizations to safeguard patient information, HIPAA also requires the US Department of Heath and Human Services (HHS) to develop standards for the maintenance and transmission of information (also referred to as Administrative Simplification). HIPAA is not simply an IT concern, but an Enterprise issue. The protection and security of electronic health information is just one aspect that must be addressed in the context of the entire Enterprise. Looking simply at how handhelds are secured is an important but small piece of the overall puzzle. For instance, securing the data on a handheld device is no good if the processes for how handhelds are used and how confidential information is accessed are not analyzed in relation to the rest of the healthcare organization's processes. As a result, unfortunately, the implementation of PDA security in this context often requires cross-department efforts.

Many Industries Introducing Regulation Like healthcare, the financial services field currently has to interpret and implement requirements associated with Gramm-Leach-Blily[4]. Even the much broader requirements under the recent Sarbanes-Oxley Act could affect how businesses address the question of PDA security. However, looking beyond the specific industry examples, most Enterprises need to consider their overall exposure to the loss of information or breach of access on handheld devices. As described in the other numerous examples, it is easy to acquire some of this confidential information on handhelds, but it is not so easy to determine exactly what is or isn't secure if the organization has no comprehensive approach or set of policies.

RISK RESPONSE PLANNING AND CONTROL: WHAT IS A MEASURED IT RESPONSE

In preparing for the next chapter, let's take an inventory of our current level of organizational readiness. You have to walk before you can run, and if your organization has only a limited approach to implementing security requirements, you might need to prepare before moving forward.

After determining which kinds of information and functionality constitute a risk, and which external factors would necessitate a comprehensive security approach for handheld devices, the next step is to examine the user access controls and privileges that must be extended to handheld devices. Addressing a measured response to handheld security risk management

[4]The GLB Act was signed into law in November, 1999, and repeals the Glass-Steagall Act which prohibited banks, securities firms, and insurance companies from affiliating. One of the key provisions of GLB is the requirement of all financial institutions to disclose to customers their policies and practices for protecting the privacy of non-public personal information.

is the focus of the next chapter, but in preparation review the following questions:

- *Information classification* Do you understand your information security requirements and what data must be protected?
- *User controls* Do you have strong user- and group-level controls for roles and privileges?
- *Business process understanding* Has your Enterprise established a clear process for obtaining information?
- *Overall security requirements* Does the organization have strong security criteria in place that can or should incorporate the use of handhelds?

If your organization has a strong security approach as part of the general IT network and asset-management areas, many of these questions will already have been answered and a set of handheld policies can be developed. However, if your organization has had a limited approach to security, you find that once you go beyond your user-password policies, you will be working from scratch. At this point, assess your organization's readiness to incorporate handheld security criteria into current security practices.

Information Classification

Below are some examples of questions that you can review for your organization before you begin to formulate and finalize your measured response to handheld device security risk issues.

- Does your organization have defined classes of information that define what is confidential and what is nonconfidential?
- Has your organization established a process to classify information?

- Are there any guidelines to determine how the different classes of information should be handled?
- Who has access to various classes of information?

User Controls

- What kind of information do users have access to?
- How volatile is the data on your user's devices?
- Do users have the right to take information with them when they are not in the workplace?
- Can users identify what information is considered proprietary or confidential, and what they should do to protect it?
- Which user classes exist and how varied are their access rights?

Business Process Understanding

- Which business processes require proprietary information to be accessed outside the office?
- Which level of information volatility or frequency of change do current processes require? For example, do devices contain read-only data or do they update master databases or sources?
- Do automated business processes currently require that information leave the office (either electronically via handheld/laptop computers or on paper)?

Overall Security Requirements

- Do you have written security policies in place?
- Does your organization have security policies for your systems (desktop, laptop, networks, server/mainframes, and so on)?

- Do you have policies defined for how employee access, transmit, or send and receive information?
- Do you perform any audits or checks to see how well to which policies are adhered?
- Do you have any policies established for handheld computers?
- How do you tackle putting controls on devices used by individual employees?