

Personal-Liable Smartphones: Enterprise Mobility's New Reality

Consumers love the power a smartphone places in their hands. If you doubt that, consider these latest figures from IDC: a record 54.5 million smartphones shipped in the fourth-quarter 2009, 39% more than the 39.2 million shipped in the same quarter in 2008. Problem is, these days it's getting harder and harder to distinguish consumers from employees when it comes to smartphone use. Employees who are used to having e-mail, calendar and other applications at the ready on their personal devices want that same convenience while they work. Imagine the productivity gains, they say. Many enterprise IT executives are beginning to see the strategic advantage a company might gain in adopting personal-liable smartphone use. In these articles, *CIO* and its sister publications *Computerworld*, *InfoWorld* and *Network World* explore the latest thinking on personal-liable policies, examining the strategies and challenges, with a particular eye on security.

In this eGuide

Smartphones: Corporate Shackles or Tool for Work-Life Balance?

BlackBerrys, iPhones and other smart mobile devices are in demand by employees today. But who gets them, who pays for them and who controls them are questions with no easy answers

Who Should Own the Enterprise Handset?

I've changed my mind—personal handsets are the way to go

Shifting Mobile Cost to Employees? Think Twice

Employee-liable smartphone plans mean jumping over quarters to pick up nickels

Their Phone, Your Headache

Employees want IT to link their personal smartphones to e-mail and other corporate resources, but how do you secure devices that house a mix of personal and corporate information? And what happens when those employees quit?

Smartphones Need Smart Security Practices

Yes, it's 'blue and plays music,' but that cute smartphone is also a serious computer that must be secured

Security Manager's Journal: Woes Hang Up New Smartphone Policy

A global company is sure to have a lot of different kinds of mobile devices. And that's just the start of the problems

Analysis

Smartphones: Corporate Shackles or Tool for Work-Life Balance?

Thomas Wailgum • CIO

BlackBerrys, iPhones and other smart mobile devices are in demand by employees today. But who gets them, who pays for them and who controls them are questions with no easy answers

» Any and all executives or managers looking to get more productivity from their information workers—and, really, what company isn't shamelessly espousing a "more with less" philosophy these days?—might want to pay attention to the following strategy: Set your workers free from the office.

"Teleworking," or working from home/Starbucks/not-within-corporate-walls, of course, is nothing new. High-powered laptops, ubiquitous broadband and Wi-Fi con-

nections, and even-my-grandmother-has-one cell phones have all enabled a seamless virtual work-experience for the modern employee.

But new survey data from Forrester Research shows that tech-savvy information workers want to be connected to (yet untethered from) the office even more—they want smartphones. And they want them badly: Many are even ready, willing and able to foot all or part of the bill to

gain access to corporate e-mail and documents, as well as stay connected to their work lives—often at the expense of their personal lives.

Just 11% of U.S. information workers today use a smartphone at work, according to Forrester's 2009 Smartphones and Telecommuting: Workforce Technology Adoption 2009 report. (The Forrester survey fielded responses of 2,001 U.S. information workers who use a computer or terminal at their job and work at an organization with 100 or more employees.)

The information workers (or "iWorkers") surveyed want more flexible work hours (two-thirds of respondents said so) and a third want to work from home at least occasionally. In the past, info workers were forced or took the initiative (depending on your point of view) to use personal

Increasing the odds

“Giving information workers access to key corporate resources from any facility or from home and elsewhere raises the chances that they can find a key piece of information when it’s most valuable: at the point of decision-making.”

— Ted Schadler, principal analyst, Forrester

mobile devices to get their jobs done: A third of respondents in the survey report that they use their own mobile phones for work.

“The logic is clear,” writes principal analyst Ted Schadler in the report. “Smartphones and laptops unshackle work from location.”

Work-Life Imbalance

Two additional nuggets of survey data and Forrester analysis offer additional employer incentive to enable and encourage increased smartphone and laptop use: Teleworkers work, on average, two hours more per week than office workers. “Access to real applications from anywhere means more work in more places,” Schadler contends. “And that translates into higher productivity—or at least higher utilization of your IT investments,” such as collaboration, instant messaging and Web conferencing tools.

And, adds Schadler, that nearly insatiable demand for a smartphone will allow companies to “offload costs and responsibility for devices and plans to their employees.” (For comparison, the report notes that one in three U.S. iWorkers has a laptop.)

All of this seems to be a win-win for companies that embrace this strategy. “Giving information workers access to key corporate resources from any facility or from home and elsewhere raises the chances that they can find a key piece of information when it’s most valuable: at the point of decision-making,” Schadler writes. “And that translates into higher team productivity.”

But what about the employees? It’s hard to deny that, on some level, they’re getting a raw deal: Not only are the employees allowing themselves to work longer hours (presumably without any pay increase), but some of them are actually going to have to pay out of their own pockets for

the “privilege” of work invading their private life, via that sleek smartphone that’s always on.

Smartphone users, in particular, “work from everywhere,” Schadler adds. “This data is definitive: iWorkers with smartphones use their devices everywhere—81% from home, 62% while traveling, even 64% while at their desks. And 29% of smartphone users spend three or more hours a day with the device.”

As the line between work and personal life blurs even more and the spread of mobile devices continues on its torrid pace, the question of who pays and how much will likely become more critical to corporate IT, finance and security departments.

“Telework is on the rise, poised to grow to 63 million U.S. iWorkers by 2016,” Schadler writes. “Regardless of its telework frequency, this group is technology-bound, more likely to use virtually every tool in the stable.” •

Opinion

Who Should Own the Enterprise Handset?

By Craig Mathias • Network World

I've changed my mind—personal handsets are the way to go

» Farpoint Group has historically taken the view that enterprise handsets, like all other elements of enterprise IT, should belong to the enterprise. This is based on the observation that one cannot manage what one cannot secure, and one cannot secure what one does not own. Security must be paramount in essentially every enterprise, but, let's face it:

- Most people want to use their personal cell phone as their only cell phone (and perhaps only phone altogether). Having to carry an additional enterprise-provided handset is in fact a burden in many cases, not a benefit. After all, the personal handset, plus accessories, travels regardless.

- The cost of handsets to the enterprise can be enormous, in terms of both capital and operational expense.
- There are numerous accounting and likely tax (both corporate and personal) issues associated with an enterprise-owned handset.
- Security, to return to my primary concern, is not just about encryption, VPNs, and authentication, but also about awareness, policies, and, today, mobile device management tools that automate both procedures and the cost accounting required to enable

the use of personal handsets in enterprise applications.

Besides, the use of personal handsets in business is happening whether the enterprise likes it or not. So, let's embrace what's become known as personal liability with respect to handsets, set up the automated accounting and reimbursement mechanisms required to cost-effectively enable enterprise use of a personal handset, put in place the additional mobile device management capabilities required, and educate and support users with respect to security, operations, acceptable use, etc.

This is a big change in my perspective—a 180, to be sure. But, unlike in the world of politics where “flip-flopping” is frowned upon (although, perhaps strangely, something I consider a sign of intelligence), we in IT should indeed flip

or flop when new technology so allows if the benefits are demonstrable—as is clearly the case here.

This is such a big topic that I've written a new Farpoint Group white paper on the subject, which you can find around the Web. Many thanks to Lyrix for a good deal of time spent discussing the many elements of personal

liability, and for a briefing on its product in this space, Mobiso 6.0.

I'm convinced—personal ownership of the delivery tools at the edge of the corporate network is going to become the standard operating procedure for enterprises of all sizes going forward. In some cases, sure, restricting ac-

cess to authorized devices will and should continue. But, for most organizations, the days of buying handsets (and perhaps even notebooks) are coming to an end. •

Mathias is a principal at Farpoint Group, a wireless advisory firm in Ashland, Mass.

Opinion

Shifting Mobile Cost to Employees? Think Twice

By Joanie Wexler • Network World

Employee-liable smartphone plans mean jumping over quarters to pick up nickels

» I've noticed a disturbing anecdotal trend in talking to enterprise customers lately, and some recent IDC numbers I just stumbled across seem to back it up. The unfortunate movement is away from corporate-liable mobile phone models and toward individual-liable setups, where employees procure their own wireless devices and services and may be reimbursed for their expenses by their employer.

IDC has reported that it expects worldwide shipments of individual-liable business-use devices to grow by nearly 18% to reach 56.7 million units by 2013. The researcher also expects that in the same year, more than 56% of corporate mobile devices will be individual-liable devices.

Please think at least twice before going this route.

There are a couple seemingly obvious reasons to offload mobile expenses to employees, and they have to do with the perception of sparing budget and reducing corporate liability. One driver is the U.S. Internal Revenue Service's current categorization of cell phones as "listed property" that puts mobile phones on a par with a corporate car and PC. These items are considered taxable employment benefits because they can easily be used for personal use as well as for corporate use.

Note, however, that two identical bills to remove cell phones from the listed property category—one from the House and one from the Senate—have been languishing since January 2009. So, while it's taking time, the IRS risk could ease up any day.

The IRS issue must be behind the individual-liable move-

ment in corporate America, according to Kevin Dilallo, a partner at telecom law firm Levine, Blaszak, Block & Boothby LLP in Washington, D.C. The reason?

"If companies think they are saving money [using the reimbursement method], they are out of their minds. And from a security standpoint, individual liability is suicide," he says.

Banning corporate-liable phones does solve the IRS problem, he acknowledges. But he indicates that these gains are shortsighted. They are far outweighed by the risk of giving up IT control over the devices (any handset with Microsoft ActiveSync can sync to your Exchange server and you wouldn't necessarily know it, for example).

And banning smartphones at work altogether, while being done in some companies, "is just nuts," he says. •

Wexler is an independent networking technology writer/editor in Silicon Valley.

Opinion

Their Phone, Your Headache

By Ojas Rege • Network World

Employees want IT to link their personal smartphones to e-mail and other corporate resources, but how do you secure devices that house a mix of personal and corporate information? And what happens when those employees quit?

» For years analysts have encouraged the consumerization of IT to enhance collaboration and productivity. It began with adoption of consumer instant messaging applications and continued with Web 2.0 technologies such as wikis and social networking. Now, as employees start bringing their smartphones to work and request IT to provide access to e-mail and other corporate applications, we are seeing the consumerization of not just an application but an entire computing platform.

At first glance this looks like a great idea. IT increases employee satisfaction, reduces opex costs by having employees foot part of the wireless bill, and cuts capex costs

by ducking the cost of the pricey phones. What's more, employees with smartphones devote more personal time to work so there is a productivity gain.

Early data from the Aberdeen Group shows that 20% of companies surveyed allow their employees to use personal devices for work.

But securing employee-owned smartphones is not the same as securing corporate-owned devices. In the corporate model, if an employee leaves the company, standard procedure is to retrieve the phone and "brick" it, wiping it clean of all data and resetting it to factory defaults. In the new model, when an employee leaves the company the phone goes

too, packed as it is with personal pictures, videos, contacts, applications, music and confidential corporate information. Is it fair to wipe all personal information from a phone just because an employee tried to be more productive for the company? At the same time, is it damaging to the company's business to compromise security levels just because that employee happens to own the phone?

Enterprise Data Boundary

The way to address this issue is to start by adopting a framework that provides visibility into corporate data on an employee's smartphone and allows administrators to set boundaries around this data. This doesn't have to be something as fancy as tagging or fingerprinting mobile files. It can start with simply drawing a line between media files on one side and xls, doc, ppt, and pdf documents on the other.

The key is that however this enterprise data boundary is drawn, if an employee leaves the company, he or she

should be able to take the phone with personal data intact, while IT should be able to ensure that any corporate information has been safely removed. The process should be simple and transparent to all.

In addition to segmenting personal information from corporate, IT must have an honest dialogue with employees about the trade-offs that exist when attaching a personal smartphone to the enterprise. For instance, regulatory compliance policies may mandate that corporate communications be archived for e-discovery purposes. These communications can include SMS messages, therefore, the employee must weigh the privacy concerns of having SMS archived in the same manner as corporate e-mail.

IT will likely find that different policies will apply be-

tween corporate-owned and employee-owned phones, so it's crucial for the policy enforcement framework to delineate between phones based on ownership.

Finally, the overall governance structure for mobility must move from one of command-and-control to one of partnership. Employees and IT must take responsibility for the corporate data on employee phones. IT cannot be the sole policing function; accountability and responsibility have to move to the employee.

Security systems have traditionally focused on inbound reporting of exceptions to IT and security staffs. Mobile management systems have to be just as focused on outbound reporting of exceptions to employees so they can do something about it. Employees must be engaged, un-

derstand their role in the partnership, and have the tools to live up to their part of this cooperative security bargain.

While shifts in enterprise security models have often led to battles between employees and IT staffs, the adoption of employee-owned smartphones may be an exception. Here, employees have an incentive to securely operate their personal smartphones because they genuinely want to use them for both work and life. What IT needs to do is provide these employees the tools to be able to strike that balance without compromising enterprise security or personal usage. •

Rege is vice president of products and marketing for MobileIron.

In-Depth

Smartphones Need Smart Security Practices

By **Mary Brandel** • Computerworld

Yes, it's 'blue and plays music,' but that cute smartphone is also a serious computer that must be secured

»» As vice president of IT at Windsor Foods in Houston, Stephan Henze has to stay one step ahead of the latest IT trends. That's why he's spending a lot of time thinking about securing and deploying smartphones enterprisewide. The company had only a few-dozen smartphones just a short time ago, but IT now manages about 100 of them, and Henze foresees substantial growth in the near future.

The task of securing smartphones keeps getting hairier, Henze says, while the company's need for mobile communications grows stronger, even on the shop floor, where maintenance engineers will soon receive automatic SMS alerts on their phones.

He's not sure he can continue to enforce the company policy of supporting only Windows Mobile-based phones, yet nonstandard devices will complicate his security efforts. He is well aware that for some people, a smartphone is a fashion statement. "With PCs, I was able to tell them we're not a Mac environment, but I'm not sure I can do that with phones down the road," he says.

Henze is among a growing number of IT and security leaders grappling with the challenge of securing these increasingly popular devices. The primary concern, of course, is the risk of exposing sensitive data if a phone or removable memory card is lost or stolen. Data also can

be exposed if a phone is sold or sent in for repairs without its memory first being erased.

There's also the risk that VPN-connected devices could expose corporate networks to hacker and malware intrusions. And there's a growing potential for viruses to attack the phones themselves through SMS hacks and other exploits. "If I take your device and muck around with it, what if the VPN is set up on it?" asks Philippe Winthrop, an analyst at consultancy Strategy Analytics Inc. "It's a huge risk not being dealt with enough today."

Complicating matters, users are apt to view smartphones as their own personal gadgets, not something IT should control. "There's a deep underlying current of 'This is my mobile device,'" says John Girard, an analyst at Gartner. A user will often see his smartphone as something that's "blue and plays music," not as an asset that needs to be secured, he says.

Smartphones' multimedia capabilities raise other concerns, Girard says. For instance, company policy might prohibit moving corporate documents to external media, but is there a policy that governs using a smartphone to take photographs in the office or record meetings?

Many companies try to take control by purchasing standard phones for employees—a move that at least enables them to support just a single operating system. But even then, users may adhere to the standard only loosely, says Paul DeBeasi, an analyst at Burton Group. “I see employees who have the company phone in their left pocket and their personal phone in their right,” he says.

Indeed, in a recent study of 300 companies in the U.S. and Europe by Good Technology, a vendor of mobile security and management tools, nearly 80% of the respondents reported an increase in the number of employees who wanted to bring their own devices into the workplace in the past six to 12 months, and 28% reported a data breach because of an unauthorized device.

Despite all of the security risks, “two out of three organizations are struggling in terms of not only defining but enforcing IT and business policies around mobility,” Winthrop says.

Lax Smartphone Security

Only 23%
of smartphone owners
use the security software installed on the devices.

Source: Trend Micro Inc. survey of 1,016 U.S. smartphone users, June 2009

Girard concurs that companies have been slow to realize the implications of a phone-related data breach. “If clients do call and ask about phones, they’re asking me to render an opinion that reduces their liability for employees using smartphones, [rather than] trying to do something to improve security,” he says. “I’m waiting for the level of concern to grow up and match what exists for PCs.”

And it should. Whether companies buy smartphones for employees or just allow their use, it’s the company that’s liable if data gets exposed, Winthrop says.

Technology to centrally secure and manage smartphones, whether via a third-party platform or from smartphone vendors themselves, does exist. Most analysts agree that,

among smartphone vendors, BlackBerry maker Research In Motion (RIM) and Microsoft, with its latest version of Windows Mobile, provide the best management platforms.

For other devices—or for companies that support phones from multiple vendors—there are a variety of options, including management software from vendors such as Credant Technologies, Good Technology, Sybase, Trust Digital, Trend Micro and MobileIron, among others. Key capabilities offered by such platforms include centralized control of the following:

- Password management.
- Authentication authorization.
- Strong encryption.
- Inactivity timeout, in which users are logged out of an application session after a specified period of inactivity and are prompted for a password to restart.
- Remote wiping of memory if a device is lost or stolen or if the user enters his authentication credentials incorrectly a given number of times.

Central control

At Robinson Lerer & Montgomery, CIO Jeff Saper has approached the security challenge by standardizing on the

Do you want that data to go, sir?

“Our biggest concern with any smartphone is [that] it acts as a storage device. Users can plug it into the USB, download company files and walk out the door with them.”

— Christopher Barber, CIO, Wescorp

BlackBerry, which is issued to all employees at the New York-based strategic communications firm. Saper uses several of the 450 wireless IT policies and commands provided by BlackBerry Enterprise Server. The firm has also used Good Technology’s platform to handle Palm and Treo devices, but Saper turned exclusively to BlackBerries when he decided to keep things consistent on a single platform.

Security measures include inactivity timeouts after 10 minutes of nonuse, and remote wiping of the devices if there is any fear of data compromise following a loss or theft, or if the password is entered incorrectly more than 10 times. “Even if someone could hack the password, it’s safe,” Saper says.

Most important, he says, users can’t disable any of the security functions.

With remote wiping, it’s important that data is backed up to the BlackBerry server so that it can be restored, Saper says. He can restore message history too, because

the server ties into Microsoft Exchange. Such backups can make clear what data is on a device and hence what would be vulnerable if the phone were stolen, Girard points out.

While other platforms can perform remote wipes, the BlackBerry server also provides confirmation that the wipe was accomplished, which would give a company a stronger position if a case involving a smartphone data breach ended up in court, he says. “If you can’t prove you did the wipe, it doesn’t sound good,” he adds.

Girard also believes it’s important to set devices to time out after periods of inactivity. He recommends setting inactivity timeouts at one to five minutes for devices with high-value information, no more than 10 minutes for those with medium-value data and no longer than 15 minutes for those with low-value information. To resume using the device, employees should have to re-authenticate by entering a strong password.

That’s easier said than done. “Because it’s mobile, people think it’s supposed to be easy, and they resist having to type in a seven- or 12-digit code,” Girard says. “But you can’t just have a four-digit code, because there’s a very real chance of someone observing you typing it in.”

Girard has also had clients who allow more than 10 password retries before deactivating a device. That’s a highly questionable policy. “Even if you’re drunk, you should be able to get in after that many tries,” he says.

Christopher Barber, CIO at San Dimas, Calif.-based Western Corporate Federal Credit Union (Wescorp), supports two devices, the BlackBerry and Apple’s iPhone 3G. The iPhone runs e-mail and a relationship management application used by salespeople. To secure the iPhones, Barber set up a standard security profile that includes all the safeguards he wanted, with Microsoft Exchange Server pushing it out to the devices.

Nice, but not overly so

“... even if organizations want to cater to every user’s desire, they need to take into account the need to manage the devices and the information that passes through or is stored on them.”

— Philippe Winthrop, analyst, Strategy Analytics

He uses RIM’s Enterprise Server for the BlackBerries. Security features include strong password protection, encryption and remote kill capabilities.

Data out the door

“Our biggest concern with any smartphone is [that] it acts as a storage device,” Barber says. “Users can plug it into the USB, download company files and walk out the door with them.” With the global profile, however, he can enforce password strength and encryption, so even if users do put sensitive data on a portable device, there is a reduced chance of someone else accessing it if the phone is misplaced or stolen.

Taking a centralized approach to encryption is key, Girard says. All the well-known vendors have an encryption feature for their phones, “but unless the company takes enterprise control, it’s strictly optional,” he says.

But Barber says that securing smartphones is a matter of managing risks, not covering every base. He says he recently saw a YouTube video of someone who used a hacking program to break into an iPhone that was password-protected and encrypted. He also says the iPhone’s removable SIM card is a vulnerability, because if a thief removes the card, the phone won’t be able to receive a remote kill command because it won’t be able to connect to the corporate network.

To offset this risk, Barber relies on a combination of policy and education.

“We train everyone not to put sensitive data on the iPhone,” he says. In the future, he hopes to back that up with data loss prevention technology, which would monitor data being moved into an e-mail attachment or USB drive. “We’re as comfortable as we can be, but there’s always risk.”

At Windsor Foods, Henze has also gone the centralized

management route, using MobileIron’s Virtual Smartphone Platform. The decision was based on his desire to manage not just security from one platform, but also carrier contracts and deployment. In addition, while he has standardized on Windows Mobile devices, he wanted to be sure he wasn’t locked into that decision. MobileIron supports BlackBerries and iPhones and plans to support Symbian and Android devices.

Henze started with the basics, such as password management, auto-disable and remote wipe, but is adding centralized encryption. The platform also backs up applications and data on the phones and reports on configuration and memory utilization, which speeds troubleshooting. It also takes inventory of applications stored on the phones and disables any that aren’t approved.

Henze also notes that the help desk manages the smartphones rather than a senior network engineer. In fact, a

portal enables users to check on their phone usage and even perform tasks such as remote wipes and configuration themselves. “The [MobileIron] appliance makes it easier from an IT perspective,” he says.

For Henze, the work of smartphone security has just begun. For instance, he’s considering integrating digital rights management with the smartphone management platform.

“Let’s say a person working with us has a laptop full of confidential information, and he gets terminated,” Henze says. “With digital rights management, the device would check in with the authentication server to see if he’s still a legitimate user, and if he isn’t, he wouldn’t be able to read those files anymore.” This works better than remote wipe, he says, because if files are stored on a removable card, there is no way to delete them.

There have been concerns from some users about the Big Brother aspect of having IT monitor their phones. However, this concern is outweighed by the fact that IT can provide better service when it comes to new phone deployments, replacements and remote troubleshooting, Henze says. For instance, IT will be able to configure a new phone right after it’s purchased, rather than taking three or four days. “They’ll be up and running in no time,

10 Smartphone Security Risks

Here’s a look at 10 common smartphone security risks, with tips for dealing with them from Gartner analyst John Girard:

1. No configuration management plan.

Tip: Responsibility for managing smartphones should be given to the same staffers who provision and manage PCs.

2. No power-on password, or a weak password policy.

Tip: Several vendors’ device management consoles allow you to configure password complexity rules and password reset questions and answers.

3. No inactivity timeout/auto-lock.

Tip: Timeout policies should be enforced over the air through your device management console, so that the enterprise can maintain near-real-time control.

4. No auto-destruct/data-wiping plans.

Tip: Two methods should be used: over-the-air commands and locally initiated wipes. The latter should occur after a password has been entered incorrectly a certain number of times or when a device has been off the network for a predefined amount of time.

5. No memory encryption rules.

Tip: Major enterprise smartphone operating systems provide settings for enforcing encryption.

6. No master plan for backup and synchronization.

Tip: Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization.

7. No e-mail-forwarding barriers.

Tip: Forwarding of e-mail and attachments can be regulated with server-side settings of a corporate e-mail system, and additional filtering is available through commercial data loss prevention filters.

8. No application certification rules.

Tip: Private keys can be used to restrict which applications are allowed to install or execute.

9. No default browser permission rules.

Tip: Choose browser default settings that comply with company policy when phones are provisioned, to avoid providing an entry point for malicious code.

10. No plan for dealing with smartphone diversity.

Tip: Set a policy that defines what levels of support different devices will receive. Assign smartphone support to a single IT group.

and when that happens, they'll appreciate it," Henze says.

In the end, there's no single means of maintaining security as more and more smartphones enter the enterprise, whether they're issued by the company or brought in by employees. But what's certain, says Winthrop, is that you can't just give employees free rein. It's not uncommon for IT to allow individuals to be responsible for their own devices, or even encourage the idea. But in the end, he says, it's the employer that's liable if data gets leaked.

"There's a fascinating issue here, in that employees

don't think too long or hard about which laptop they're going to get," Winthrop says. "But they're absolutely going to ask 'Why did or didn't they give me a BlackBerry?' or 'Why can't I bring in my iPhone?' or 'I wonder if I can get a [Palm] Pre?'" But even if organizations want to cater to every user's desire, he says, they need to take into account the need to manage the devices and the information that passes through or is stored on them.

In fact, smartphones should be viewed not as phones, but as PCs that happen to make phone calls, Winthrop says.

According to Henze, that notion has turned the world inside out. "In the old days, there was the Internet, the intranet and the internal corporate network," and each was distinct from the other. But today, with miniature yet powerful mobile devices carrying data wherever a person can go, "the egg is scrambled," Henze says. "Data sits wherever, and it's much more difficult to get ahead of it." •

Brandel is a Computerworld contributing writer. You can contact her at marybrandel@verizon.net.

Lessons Learned

Security Manager's Journal: Woes Hang Up New Smartphone Policy

By Mathias Thurman • Computerworld

A global company is sure to have a lot of different kinds of mobile devices. And that's just the start of the problems

>> Over the past seven months, I have led a team of IT representatives in making sure that all mobile devices are aligned with our new security policy. I thought this was going to be straightforward—a few mouse clicks to check off some boxes, and our policy would be in effect on our entire inventory of mobile devices.

But because months have gone by since our previous CIO signed off on our security policy, you can probably guess that things weren't as easy as I expected.

The policy is pretty simple. It states that all mobile devices that are used to connect directly to our network or

that otherwise synchronize data with the network must have four-digit passwords, must time out after 30 minutes of inactivity, must wipe themselves of all data after 10 unsuccessful log-on attempts, and must be capable of being controlled by our IT department and of being remotely wiped if lost or stolen.

The first problem is variety: We use something like 25 or 30 different kinds of phones worldwide. While most of them are BlackBerries, iPhones or Windows smartphones, there are plenty of variations. Nokia, Samsung, Motorola, LG, HTC and PCD are just some of the vendors we use.

That diversity makes it pretty much impossible to fully test every phone with every operating system.

On the other hand, there are only two methods by which mobile phones can connect to our internal network: one for BlackBerries, and one for every other device. The latter uses Microsoft ActiveSync. One of the major differences is that ActiveSync passwords can't be reset. If a user forgets his password, he must wipe the device to the factory default setting. Ouch! That was a factor in one notable complication we encountered as we began testing some widely used devices.

Nokia phones that some employees were using in Singapore had come preconfigured with default passwords. The passwords weren't activated but were nonetheless bound to the devices. When we pushed the ActiveSync policy to those phones, they locked, and the users thought that they were

supposed to create new passwords. Many of them ended up trying to input a password 10 times; guess what happened.

Starting Over

After many trials and tribulations during our limited tests (the Nokia situation is only one example), I suddenly found myself back at square one. That's because our previous CIO had procrastinated on approving an executive communication authorizing us to deploy the mobile device policy to a handful of BlackBerry-using executives before undertaking a global rollout. (We've had no problems with BlackBerries.) He probably didn't care to get involved in the issue because he knew he would be leaving soon.

When I approached our new CIO, he began to ques-

Trouble Ticket

AT ISSUE: It has taken months to implement a new security policy for mobile devices, and meanwhile a new CIO has arrived.

ACTION PLAN: Start by helping the new CIO understand the value of passwords.

tion me on the need for passwords for mobile phones. He wasn't reacting to our deployment woes; he simply didn't see the need for such a policy. I had to explain about the risks involved should an unprotected BlackBerry phone

fall into the wrong hands.

To underscore the potential for theft of intellectual property, I used my BlackBerry to browse to an unprotected, internal Web site that is loaded with sensitive materials that it is my job to protect. Without passwords, I said, a competitor who came into possession of one of our BlackBerry phones would have unimpeded access to all such sites and the information that they contain.

Sometimes a security manager just has to conjure up some scary scenarios to make a point. I'm pretty sure he got it. •

This journal is written by a real security manager, "Mathias Thurman," whose name and employer have been disguised for obvious reasons.