

Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise

With safeguards in place to protect data and intellectual property, we are allowing employees to select the tools that suit their personal work styles and facilitate their job duties, improving employee productivity and job satisfaction.

Rob Evered

Information Security Specialist, Intel IT

Jerzy Rub

Information Risk & Security Manager, Intel IT

Executive Overview

Intel IT is actively integrating employee-owned hand-held devices into our enterprise environment. We have long recognized that the consumerization of IT—employees using their personal devices to access corporate data—is not a passing a workplace trend, so we worked closely with Intel’s Legal, Information Security, and Human Resources (HR) groups to enable a solution that aligns with our information security policy.

In January 2010, we implemented a new program allowing employees to use their own hand-held devices on the job. Employee response was overwhelmingly positive, with more than 3,000 employees signing up in the first month. As of September 2010, our computing environment included more than 20,000 hand-helds, and about 6,500 of these are employee-owned with access to corporate information. In July, we started a new program that allows personally owned tablets; we do not yet allow personally owned PCs, but are investigating that possibility for contract employees.

To reach this point, we engaged in activities on several fronts:

- We worked with Intel Legal and HR for more than a year to define and implement a personal device policy that meets Intel’s information security requirements.
- We used social media to engage in dialogue with employees over a period of six months

to understand their work styles and support needs.

- We developed technical solutions, such as new authentication methods and device management policies, that help safeguard corporate information and intellectual property.
- We provided training to users about information security and to IT Service Desk personnel about our personal device policy.

By taking control of the trend and the technology in our environment, we have been able to circumvent many of the security issues that might have occurred if we simply ignored the issue or prohibited employees from using their own devices to accomplish some of their job duties.

With safeguards in place to protect information and intellectual property, we are allowing employees to select the tools that suit their personal work styles and facilitate their job duties, improving employee productivity and job satisfaction.

Contents

Executive Overview.....	1
Business Challenge	2
The Case for Personal Devices in the Enterprise.....	2
Balancing User Demand and Information Security	3
Solution.....	3
Security Challenges	4
Designing a Security-conscious IT Consumerization Policy	4
Training Users and Service Desk Personnel.....	6
Technical Considerations	6
Results	7
Future Plans.....	8
Conclusion.....	8
Acronyms.....	8

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BUSINESS CHALLENGE

Like many enterprise IT organizations, Intel IT prohibited the use of personal hand-held devices in our environment. With the consumerization of IT, we face the daunting challenge of enabling employees' desire to access corporate information using an array of personal hand-held devices.

Ten years ago, Intel employees came to work to use great technology. Now, with the battery of consumer devices available, they often have better PCs and printers at home than they do at work. User expectations have also changed: We no longer need to provide basic computer and software training—users already have experience, often using platforms that we don't have—and the Internet has become accessible from more places than ever before.

The Case for Personal Devices in the Enterprise

Intel's highly mobile workforce wants to take advantage of the most up-to-date systems, services, and capabilities to do their jobs, typically using hand-held devices as companion devices to extend the usefulness of their corporate-owned mobile business PCs. This allows them to access information easily from home or on the road.

For example, many users want to synchronize their Intel calendars with a third-party web-based calendar utility so they can use their personal devices to access their work calendars from anywhere. They are motivated by the desire to get their jobs done in a manner that is easy, efficient, and most productive.

Employees often don't consider the information security issues raised by such a practice; however, for Intel IT, information security is critically important. We investigated the possibility of continuing our policy prohibiting all personal devices, but analysis showed that enforcing the policy would have consumed millions of dollars in software and support and would have negatively impacted users' productivity.

Such an approach would have required Intel IT to verify every application before allowing a user to install it—which alone would take away much flexibility from our highly technical, often specialized 80,000-user base. We also would have needed to significantly modify Intel culture and user expectations, deploy new lab networks, and install large amounts of new hardware and networking equipment.

Since the use of personal devices was beginning to accelerate at Intel, our policy needed to change to accommodate it. We chose to embrace the consumerization of IT, recognizing that the trend offered significant potential benefits to both users and to IT:

- **Increased productivity.** Users can choose devices that fit their work styles and personal preferences—resulting in increased productivity and flexibility.
- **Greater manageability.** By offering a program that users can adopt, we are aware of what they are doing and can offer services that influence their behavior. This provides a clear understanding of our risk level so we can actively manage it.
- **Enhanced business continuity.** If a user's mobile business PC is nonfunctional, a personal hand-held device provides at least a partial backup, enabling the user to continue to work productively.
- **Loss prevention.** Internal data indicates that users tend to take better care of their own belongings and tend to lose personal devices less frequently than corporate-owned devices—which actually enhances information security.
- **Greater security.** Rather than ignore the consumerization of IT, we can increase information security by taking control of the trend and guiding it.

We challenged our organization to find a way to allow at least some form of IT consumerization while meeting Intel's information security and privacy requirements.

Balancing User Demand and Information Security

With each new generation of technology, Intel IT must develop ways to help keep information secure. The challenge is to develop a policy that maximizes both user demand and information security to the greatest extent possible.

In general, when users first adopt a new technology, we do not incur excessive support costs because security threats are minimal (see Figure 1). At the point where user demand peaks, the technology becomes expensive to support because security threats increase as more people gain experience with the technology and start to attack it. At that point, represented by point B in the figure, we need to allocate resources to secure the technology. The return on investment, however, is less than ideal because user demand for that technology begins to taper off, shown at point C, as other new technology becomes available.

We have found that adopting a technology at point A, where both user demand and information security are both relatively high, is the best approach.

SOLUTION

Recognizing the potential benefits of the consumerization of IT to both employees and to IT, about three years ago we began to identify the unique security challenges this workplace trend poses, investigate user behavior, and define the requirements of an IT consumerization policy.

These tasks involved close collaboration with Intel Legal and Human Resources (HR). We addressed some information security risks using technology, some by legal contract, and others with training designed to change behavior, empower users, and let them have responsibility for keeping current.

The foundation for the consumerization of IT was laid 20 years ago, with the advent of the Internet, e-mail, and the world-wide web. Figure 2 illustrates this process, culminating with our phased approach to embracing at least some personal devices in the enterprise.

We now have a policy in place that supports users' needs for mobility and flexibility by allowing personally owned hand-held devices in the enterprise and is capable of allowing other personally owned devices in the future.

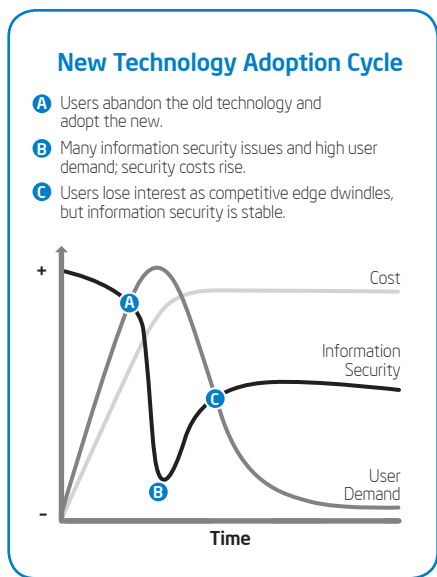


Figure 1. We have found it is best to adopt new technology at Point A, where user demand is still high but information security risk is still acceptable.

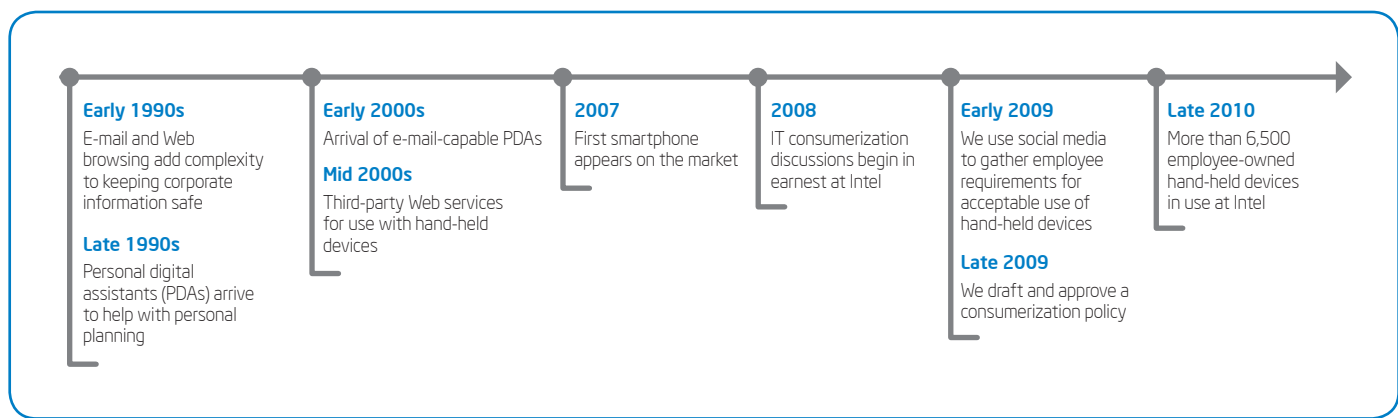


Figure 2. Responding to a 20-year trend toward the consumerization of IT, we broke the development of our policy into stages; the entire effort took more than 18 months.

Security Challenges

It is relatively easy to verify and enforce which applications are running on corporate-owned hand-held devices. With personal devices, this process is not so straightforward because employees have the right to install any applications they choose. However, we have identified certain minimum security specifications for hand-held devices that provide a level of

Mobile Business PCs or Thin Clients?

At Intel, we have standardized on mobile business PCs, complemented by hand-held devices such as smartphones and tablets—corporate- or employee-owned. This solution enhances employee productivity without compromising information security.

We have not found that the thin client computing model, which centrally stores information and allows access to that information only from specific devices, is a foolproof way to protect corporate information.

Although thin clients are appropriate for certain limited applications, in general we feel they limit user mobility, productivity, and creativity. Also, many of the perceived security enhancements associated with thin clients need to be viewed with caution. At Intel, we found that many of the information security risks merely moved—they didn't disappear. For example, thin clients usually don't include the same level of information security protection as mobile business PCs, yet they can still connect to the Internet and export information, putting that information at risk. Therefore, the loss of productivity that came with using thin clients was for little or no gain.

information security that allows us to test, control, update, disconnect, remote wipe, and enforce policy:

- Two-factor authentication required to push e-mail
- Secure storage using encryption
- Security policy setting and restrictions
- Secure information transmittal to and from Intel
- Remote wipe capability
- Some firewall and Intrusion Detection System (IDS) capabilities on the server side of the connection
- Patch management and enforcement software for security rules
- The ability to check for viruses from the server side of the connection, although the device itself may not have anti-virus software

In the case of anti-virus software, we analyzed virus attacks on Intel mobile devices and found that very few targeted corporate information—most either sent text messages or attacked the user's phone book. Although we do expect malware incidents to increase over time, the current threat level to actual corporate information is low.

We also provide guidance for configuring software installed on the personal device, as well as a standard set of application installations.

Designing a Security-conscious IT Consumerization Policy

In designing a policy that would allow personal hand-held devices to access corporate information, we first needed to know how employees were already using personal devices, why they were using them, and what they expected from Intel IT. We then worked with Intel Legal and HR to address their legitimate concerns about allowing personal hand-helds to access

corporate information. Once we crafted our policy, we needed to train our Service Desk personnel and employees on how to comply with the policy.

FINDING OUT WHAT USERS WANT

It quickly became evident that only users themselves know the answers to questions about preferences and behaviors. We decided to engage with employees directly through social computing—a blog—to openly discuss the creation of Intel IT's consumerization policy. We met with resistance from Intel Legal and HR because they understandably felt that discussing policy in an unconstrained environment like a blog might allow any responses to be perceived as policy itself. We needed to set clear expectations in all our communications that Intel IT was not making promises or firm statements about policy. Rather than letting this carry a negative tone, we were conversational and honest, as illustrated by the following example:

"Over the next month we will be posting questions about how you believe Intel should handle the consumerization issue. NOTE: This is an experiment—Intel has never opened up policy development discussions directly with employees. So be kind. Or be brutal, we can take it.

Your feedback will be read by experts and decision-makers and may inform a future consumerization policy. Then again, it might be ignored altogether, no offense. ☺"

When designing the blog, we engaged a communications specialist to help write the questions with user behavior in mind. It was important to craft questions in a way that would elicit meaningful responses. A sampling of the high-level questions we asked included:

- Why do you want to use your own device(s) for work?
- What would you give up to use your device for work?

- What does your personal device do that helps you work?
- Would you increase security habits for more device freedom? More paranoia, please?

Many of our questions sought similar kinds of information from employees. Asking which applications people need for work and what functionality they need might seem redundant, but people interpret these two questions differently and provide different responses—which helped create a broad picture of usage patterns and preferences. In this particular example, applications allude to functionality but also reveal very specific solutions, while functionality confirms the overall preference or perceived need for a general task like calendaring or e-mail.

Participation in this dialogue underscored users' desire to use personal devices to perform their jobs: More than 8,000 employees responded. In fact, user response was so enthusiastic and informative that we extended the lifespan of the blog from one month to six months.

Sometimes users' responses to our questions shed new light on assumptions we had made about how people worked. For example, two sales representatives, with essentially the same job responsibilities, had very different device preferences. One was adamant that he needed a device that could download applications, allow him to check e-mail, and show locations of airport lounges and wireless hotspots. His counterpart complained about having to use a device with too many extraneous features—he simply wanted a mobile phone that could make calls and had long battery life.

GETTING SUPPORT FROM INTEL LEGAL AND HUMAN RESOURCES

Developing an IT consumerization policy required support from Intel Legal and HR. Their concerns included policy validation and enforcement, e-Discovery, and audits and investigations.

Because of these concerns, they monitored the blog closely, and we incorporated their feedback into our interactions with users. We took this opportunity to educate Legal and HR about the reality of IT consumerization and the potential benefits—as well as the potential risks—it posed for Intel. Collaboration allowed us to align our goals and solutions, and share the very positive user response to the concept of allowing personal hand-helds in the enterprise environment.

CRAFTING AN END-USER LICENSE AGREEMENT (EULA)

The result of our policy development activities is an end-user license agreement (EULA) that addresses information security through policy. In reality, it is not a new policy at all—rather, it aligns the use of personal assets for business purposes to our existing terms and conditions of employment so that users can anticipate common policies.

The EULA gives users clear instructions on what they can and can't do with a device. For example, the section on data storage and backup states:

“Pursuant to the Intel Code of Conduct, you have the responsibility to ensure that the Intel Data in your possession is managed and protected. This means that you may be required to install encryption solutions and are not allowed to give non-Intel employees unlocked access to the device. Where any Intel Data resides on your device, you should only back it up to an Intel owned device.”

Currently, our policy allows only personally owned hand-held devices, such as smartphones and tablets, as well as USB sticks for mass storage and some devices owned by business partners. However, we tried to make the EULA general enough that it would serve for virtually any type of personally owned device, even though the use of some of these, such as home PCs, are not yet allowed at Intel.

After two years of development and modification, we now have one EULA that covers both personal and corporate devices, is not limited to specific applications, and is able to accommodate future developments for at least six months. We review the EULA each quarter to make sure that, as the technology and demands from users change, the legal protection provided by the EULA remains up to date. Users re-sign the EULA when they move to new technology.

Of the more than 6,500 Intel employees who asked to use personally owned hand-held devices, only about 50 refused to sign the EULA. This reaction underscores the need for employee training and communication, because these employees wouldn't have been signing anything new at all. Employees who do not sign the EULA cannot use personal devices to access corporate information.

In addition to addressing what is and is not allowed, the EULA accommodates Legal and HR issues.

Privacy Concerns

Working with Intel Legal required us to define of the terms “corporate information,” “employee-owned data,” and “personal data.”

- Corporate information is data or intellectual property owned by Intel.
- Employee-owned data is data the employee owns, such as a to-do list or a collection of recipes.
- Personal data is data controlled by privacy legislation, such as home address, medical data, and so on.

We try to eliminate the commingling of personal and corporate information whenever possible, but often the technology does not support this effort. For example, personal and corporate information may intersect on calendar applications. Because users' personal data is often mixed with corporate data on hand-held devices, users need to understand that, in the case of an investigation, we may confiscate their device and may see their personal data.

HR Concerns

It is important that workers be compensated for their time spent working. Our EULA specifically addresses this issue:

“Non-exempt employees who check their work e-mails outside of regular working hours are performing compensable work and must report this work time on their time cards. Non-exempt employees may not elect to work and not report their time. If a non-exempt employee believes that he/she is not being properly compensated for time worked, or believes that he/she is being pressured to perform work without reporting the time, this should be immediately reported to HR Legal or through the Intel Ethics reporting website.”

eDiscovery Issues

We expected eDiscovery to be a challenge, but it ended up being a fairly easy issue to address. As long as we don't introduce local applications that generate data on the devices, the only connection between hand-held devices and the company is e-mail. Therefore, we can perform all eDiscovery on our e-mail servers.

We did learn that employees create content in unique ways; for example, they might snap a photo of a white board and send it to colleagues in an e-mail message. We are able to capture this information on the e-mail server. Where information is located and what copies are on the devices is mostly controlled by policy and auditing.

Collecting corporate information from devices that we don't own can create challenges. We do not allow corporate information on devices that has not been synchronized elsewhere. We also added a clause to the EULA that informed users that they were subject to legal hold.

“When placed on legal hold, you must surrender your device if requested to do so. All files on your device may need to be copied, and relevant files may be used in an Intel legal matter. By participating in this program, you agree to allow Intel Legal to review and copy information on your device at any time Intel Legal determines it is necessary.

Employees subject to a Legal Event Hold Notice may have restrictions on which services they are able to use. It's your responsibility to understand from the IT eDiscovery team what services you are allowed to have on your device.”

Investigation and Audit Changes

Users agree in the EULA that Intel can investigate their personal device. However, with the advent of personal devices in the enterprise, our investigations team needed to work differently. Compared to investigating a corporate-owned device, it is much more difficult to investigate a personal device without the user being aware of the investigation. Therefore, we carefully defined what actions would necessitate us confiscating and investigating a personal device, and we try to package and release services in such a way that we won't ever need to investigate the device.

Training Users and Service Desk Personnel

Simply developing a policy is not enough. We found that we needed to train users about what the policy means and how to protect information on their devices.

For example, during our conversation with users on the blog, we learned that only about a third of them would decline to loan a personal device to a family member—even

though the device had Intel information stored on it. Educating users about the risks such behavior poses to corporate information has the potential to enhance information security through behavior modification.

We also discovered that IT Service Desk personnel required training to adequately answer users' questions about the EULA, so that they don't accidentally invalidate parts of it by giving the wrong answers. For example, if a user has a question about what form of monitoring Intel IT is performing on personal devices, Service Desk personnel must be careful not to give a response that could legally hamper Intel's decision to monitor personal devices in the future. Frequently asked questions (FAQs) provide this type of training for our Service Desk employees and end users.

Technical Considerations

One of the biggest technical challenges to implementing our policy involved firewall authentication. With IT-managed systems, authentication uses two factors: something you know—a password—and something you have—a registered mobile business PC. But when the device is unknown, you are left with only one authentication criterion.

Therefore, one of the interesting challenges of allowing personal devices in the enterprise is how to use information on the device to authenticate to the network, without that information belonging to the user. If the employee owns the piece of information used to authenticate to the network, we would have no grounds for disciplinary action if the user chooses to move his or her data to a different device to get access to the network. For example, the International Mobile Equipment Identity (IMEI) number on a mobile device belongs to the user if they

own the hardware, so we cannot use that to authenticate the device.

To address this issue, we now send a text message to a predefined phone number, and that text message becomes the user's password. In this scenario, the phone number is the "must-have" authentication factor, and the text message is the "must-know" authentication factor.

Device management also poses challenges, because one solution doesn't fit all devices and applications. We have designed our device management policy with the expectation that a device will be lost or stolen. Therefore, we expect it to be able to protect itself in a hostile attack. This means that the device is encrypted, can self-wipe with a number of wrong password attempts, and we can remotely wipe the device. Our personal device

policy requires users to have controls in place prior to any loss.

Also, some services need greater levels of security than others. For example, the system for booking a conference room doesn't need the high level of security required by the sales database. Therefore, the room booking system can reside on a device over which we have less management control. We developed a tiered management system, which is illustrated in Figure 3.

Results

Our policy of allowing personally owned hand-held devices in the enterprise has been in effect for about a year. Three thousand Intel employees signed up for the program in the first month; to date, the Intel environment includes more than 20,000 hand-helds, 6,500 of which are personally owned by Intel employees. In July

2010, we started a new program that allows personally owned tablets.

We have been able to achieve these results using a three-pronged approach:

- The EULA enumerates exactly what employees can and cannot do with a personally owned device, in language they can understand.
- Technical solutions, such as new authentication methods, help safeguard information.
- Training users about information security has helped improve the way they use personal devices, such as not letting family members or friends borrow a device that can access corporate information.

This approach has allowed us to successfully accommodate personally owned hand-held devices in our infrastructure without compromising our information security standards.

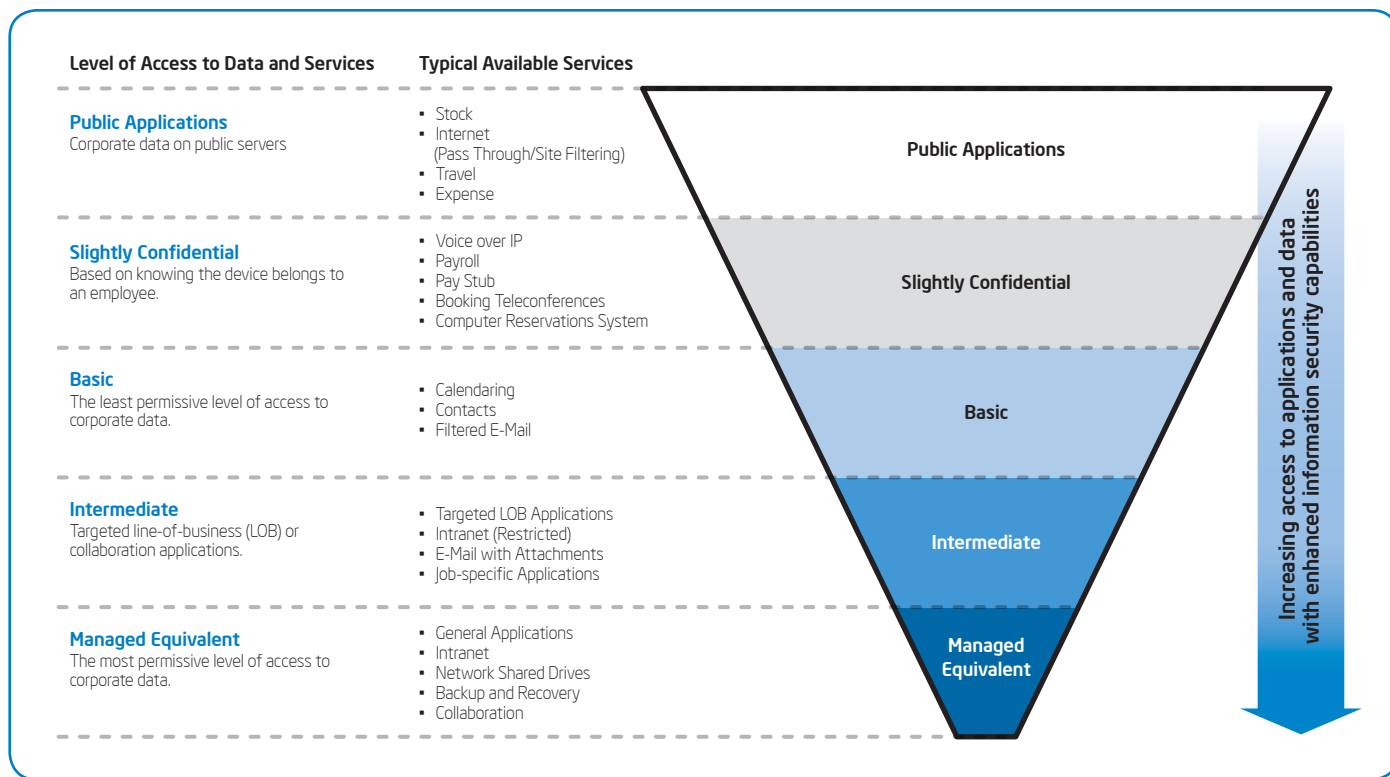


Figure 3. A tiered approach to device management lets us match the required level of management to the sensitivity of the information and application.

We have seen a significant increase in productivity, measured by number of e-mail messages sent from a personal device and “time back” reports. We have also experienced a significant reduction in unauthorized devices on our network—currently, less than 0.5 percent—because we are enabling more devices with a sufficient level of security enforcement.

Future Plans

Although they are companion devices and in no way replace our employees’ mobile business PCs, hand-held devices comprise a significant part of Intel’s IT infrastructure. We are funded to deliver more user capability and more device management capability, so personal devices will be managed just like a laptop.

Our manageability team is working on a new management console, which will feature improved reporting and security controls. We anticipate installing this new management system by the end of 2010.

Through pilot projects, we are investigating several usage and support models for hand-held devices, both corporate- and employee-owned:

- Use a corporate device and push e-mail from the supplier.
- Use a low-cost device, either corporate-owned or personal, and push e-mail from Intel IT servers.
- Allow any device, using a portal for connectivity, with no offline information allowed.

We also have a team that is improving access to applications from hand-held devices. For example, we will soon provide access to Intel’s intranet through personally owned hand-held devices. We are also investigating allowing employees to use popular social media applications to find and contact other Intel employees, as they have indicated they prefer this method to using Intel’s internal employee directory.

CONCLUSION

The consumerization of IT is a significant workplace trend Intel IT has been actively investigating for three years. We have established a comprehensive information security policy, trained users and Service Desk personnel about that policy, and developed technical solutions that meet our information security requirements. These accomplishments enable Intel IT to take advantage of the benefits of IT consumerization without putting our corporate data at risk.

For us to successfully accommodate employees’ desire to use personal devices in the enterprise, it was important that we proactively anticipated the trend instead of ignoring it. In our dialogues with other companies, we found that many of them lost control of their environments by simply doing nothing. Our success also hinges on

an even-handed approach to developing policy, where each instance of personal device usage is treated consistently; it would be difficult to take action if one employee did something if that thing is common practice.

Now, our highly mobile users can use either their own or a corporate-owned hand-held device as a companion to their mobile business PC. Because employees with similar responsibilities have different preferences, allowing them to use the hand-held devices that best suit their work styles increases productivity and job satisfaction.

For more information on Intel IT best practices, visit www.intel.com/it.

ACRONYMS

EULA	end-user license agreement
FAQ	frequently asked question
HR	human resources
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
LOB	line-of-business
PDA	personal digital assistant


This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

1110/IPKA/KC/PDF

 Please Recycle
323956-001US

