IT@Intel White Paper

Intel Information Technology
Business Solutions
May 2010

Deploying Full Disk Encryption to Protect the Enterprise

Intel's success is based on our intellectual property. Information is the foundation of our company, and none of us can afford to make a mistake in how we manage it.

—Diane Bryant
Chief Information Officer
Intel Corporation

Rex Rountree
Encryption Service Manager, Intel IT

Carol Kasten
e-Discovery and Investigation
Team Manager, Intel IT

Michael Amirfathi
Engineering Information Protection and
Encryption Services Manager, Intel IT

Executive Overview

To help protect Intel's intellectual property and employees' personal information, in 2009 Intel IT began deploying full disk encryption on all corporate-owned laptops provided to employees. With this approach, the entire disk drive is encrypted, including data, applications, the OS, and free space, so that if a system is lost or stolen, malicious individuals cannot access data. Within 12 months, we have installed full disk encryption on more than 75 percent of all eligible corporate laptops.

We implemented a phased plan to help ensure smooth deployment of the encryption program. To minimize work disruption, we began "pull" deployment in early 2009, allowing employees to install the software at their convenience. Once we reached our goal of employees installing encryption on 70 percent of all corporate laptops, we switched to a "push" deployment to enforce installation on all remaining laptops.

We employed multiple strategies for managing our deployment, including:

- Establishing training, resources, and management infrastructure for operations and Service Desk staff prior to deployment.
- Developing automated client installation packages to make the installation process as simple as possible.
- Holding regularly scheduled meetings to keep executive and group management informed and to facilitate quick decision making to address issues as we progressed through the deployment.
- Tracking progress using metrics on the number of laptops encrypted and Service Desk call volume to carefully balance our adoption rate, scheduling goals, and burden on our support services.
- Promoting encryption adoption through training and resources for end users as well as through the use of targeted e-mails from executive management.

These and other strategies have helped us strike a balance between meeting an aggressive deployment schedule, minimizing disruption to employee productivity, and not overburdening our support services with resolving issues related to encryption deployment. We anticipate that through our final push deployment phase, we will meet our current goal to complete full disk encryption on all remaining laptops by mid-2010.

Contents

IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Industry trends show that security attacks have become more serious, more targeted, more financially driven, and better organized in recent years. An Intel IT internal risk analysis showed that one major security breach could cost Intel USD 5 million or more in direct costs alone.

In response to such growing threats and the costs related to lost or stolen data, in late 2008, Intel IT decided to deploy full disk encryption on all employee laptops. With full disk encryption, the entire disk drive is encrypted, including data, applications, the OS, and free space, so that if a system is lost or stolen, malicious individuals cannot access data. When properly implemented, full disk encryption provides a strong and automated security solution that does not depend on active employee participation. It is based on a mature technology, can be implemented across all laptops, and provides a foundational layer of security that can be integrated with other technologies.

In our planning process, we realized that implementing full disk encryption would entail considerable risk, since it involves the 80 percent of Intel employees who work on laptops. To mitigate this risk, we carefully planned our deployment strategies. We established requirements as outlined in Table 1, extensively evaluated products and suppliers, set up training, and established resources and management infrastructure before implementation.[1]

In our product evaluation process, we researched encryption products through analyst reports and third-party reviews, we tested products in the lab, and we conducted interviews with peer enterprises that had performed large-scale encryption deployments. This evaluation and interview process not only helped us make decisions, it also helped us learn about real-world pitfalls and best-known methods (BKMs) for deployment, which influenced how we planned our deployment. Table 2 shows the findings from our peer-company interviews.

SOLUTION

With careful planning and preparation, we began deploying our encryption solution in early 2009, with an aggressive target for encrypting all eligible laptops within a year. This timeframe minimized disruptions to employee productivity along with impacts to operations and Service Desk staff.

Planning Deployment

To help ensure a smooth installation process, we first established training, resources, and management infrastructure for operations and Service Desk staff. We also created targeted communications, resources, and training materials for end users.

OPERATIONS

We prepared our operations teams for the initial deployment and for later updates, laptop recovery, e-Discovery, monitoring, and auditing. Recovery and e-Discovery are particularly sensitive processes because they must meet legal and corporate requirements while still protecting end user privacy. Intel already had a comprehensive authorization framework in place for handling these processes, and that framework was extended to cover laptop encryption issues. As an example, authorization from appropriate legal, business, and technical managers is required for a laptop to be accessed if an employee is no longer with Intel.

[1] For a detailed description of this process, see "Strengthening Enterprise Security through Notebook Encryption." Intel Corporation, December 2008.

Table 1. Intel IT Requirements for Full Disk Encryption Deployment

Requirement	Description
Security interoperability	Our solution had to be consistent and interoperable with Intel's existing laptop security solutions. It also needed to provide secure key storage on the laptop and support multi-factor authentication. Finally, to help ensure the solution met legal and regulatory requirements, the solution had to have standard certifications, such as Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST).
Enterprise manageability	To help ensure effective management, the solution had to be consistent with existing management tools and processes, including interoperability with Intel® vPro™ technology.
Minimal impact on laptop users	The solution had to be simple for laptop users in order to minimize disruption, training, and Service Desk requirements. Impact on laptop performance also had to be minimal. We did not want to interrupt employee workflow or otherwise decrease productivity.
Smooth deployment	The solution had to support automated deployment using Intel IT's existing laptop management infrastructure. It also had to provide tools for detecting and fixing deployment issues to avoid costly manual assistance for failed installations.
OS compatibility	The solution had to be fully compatible with all OSs and OS versions in Intel's laptop environment.
Laptop eligibility requirements	Only laptops with Intel® Core™2 Duo processors or newer were eligible for encryption. We made this decision after seeing significant performance delays when encryption was installed on laptops with older processors.

Table 2. Feedback from Peer-Company Interviews

Requirement	Specific Needs
Data losses	Our interviewees reported no data losses during their deployments, though in a few cases, laptop data had to be recovered using supplier tools.
Disk error scanning	Enterprises found it useful to run disk error scanning and defragmentation utilities on laptops prior to deployment. Those who did not experienced a 1 or 2 percent failure rate. In the past, hitting a bad sector on a hard drive during encryption would crash the system. However, today's leading solutions automatically halt the install when bad sectors are found. Disk error scanning can then be performed on these systems before retrying the install.
Deployment timelines	Deployment timelines varied greatly, from as few as 6,000 laptops in 18 months to as many as 15,000 laptops in three months. However, this seemed to depend more on the company and internal IT issues than on the selected encryption product.
Service Desk and service support call volume	All organizations experienced an increase in Service Desk and service support calls during initial deployment, but call volume returned to normal within a few weeks.
Recovery and e-Discovery	No problems were reported with recovery and e-Discovery tools and processes.

SERVICE DESK

We prepared support staff with training materials and scripts to help employees download, install, and provision the software, and to help with follow-up issues. Based on our research, we expected that users would require help primarily with creating and resetting passphrases. These passphrases are required for starting the encryption program and are set using multi-word, memorable phrases such as a sentence, with spaces between words. We decided to require passphrase authentication rather than single sign-on (SSO) authentication, because lengthier and more complex passphrases provide stronger security.

END USERS

Prior to deployment, we published and e-mailed employee communications to all laptop users. These communications explained the need for encryption and set expectations for deployment and use. In particular, users needed to understand new passphrase requirements and be prepared for some performance slowdown during the disk encryption process. E-mail communications also explained that, following full disk encryption, they would not notice any performance delays during normal use of the system. However, they would notice slight performance delays during start-up, shutdown, and while transitioning to and from hibernation. They could also expect somewhat longer performance delays following installation on laptops with solid-state drives (SSDs) due to their speed compared to that of hard disk drives (HDDs). For more information about these performance delays and how we resolved them, see the "Introduction of Solid State Drives" section. We also told employees they could expect newer laptops with faster processing speeds to have nearly negligible performance delays after installing the encryption program.

To make the installation process as simple as possible, we provided automated client installation packages on a Web site we created on the employee intranet. This Web site contained the downloadable encryption program as well as training materials such as high-level installation instructions, system eligibility requirements, materials promoting greater employee security awareness, a video from executive management stressing the importance of company-wide encryption, and frequently asked questions (FAQs).

Phased Deployment

To minimize impact on laptop user productivity, we implemented a "pull" deployment to allow employees to install and encrypt their hard drives at a time that fit their work schedules. From our download site, employees downloaded, installed, and provisioned the program at their convenience. After 70 percent of laptop users had downloaded the encryption program, we began enforcing compliance by "pushing" the encryption software to all remaining unencrypted laptops.

We thoroughly tested our solution and processes through a series of small deployments. In each case, we documented technical and operational issues and developed appropriate fixes. We also coordinated these deployments with our planning process to optimize our infrastructure and training programs based on real-world results.

We defined four deployment phases, shown in Figure 1:

- Small evaluation. Deployment to about 20 end users, all peers and colleagues of the encryption team.
- Proof of concept. Deployment to a larger test group of 100 end users from various engineering and customer support groups. These individuals tend to be more computer-savvy than the average end user and are generally more proactive in resolving issues.
- Full production pilot. Deployment to 1,000 end users across a broad range of roles to simulate a full deployment. This group helped ensure that we could support all users effectively, yet still uncover the kinds of issues that were likely to arise in an enterprise-wide rollout.
- General rollout. Implementation of encryption across all remaining employee laptops. We began this phase with pull deployment and switched to push deployment after 70 percent of laptops were encrypted. We are currently in this general rollout phase, with more than 75 percent of all corporate laptops encrypted.

Tracking Progress

Throughout the deployment, we held regularly scheduled meetings to keep management informed and to facilitate quick decision making. These meetings helped us:

- Review project progress and discuss engineering challenges and deployment issues so that we could manage them as efficiently as possible.
- Better understand the business impacts of our deployment and respond in a timely and effective manner.
- Share progress and review issues and resolutions with executive management.

We set an aggressive scheduling goal, initially allowing one year for full deployment. We had to balance our scheduling goals against our goals to minimize impacts on both support services and employee productivity. We developed and tracked deployment metrics to monitor our progress and to help us adjust our strategies during the deployment:

- Overall deployment progress. We worked with executive and group management to define internal deployment goals. We used those goals to determine how we monitored deployment and to measure how we were tracking against schedules. This tracking was important in determining when to switch from pull to push deployment.
- Service Desk call volume. We tracked the number and reasons for calls related to encryption. If call volume exceeded our limit, we slowed the deployment implementation by reducing e-mail campaigns targeted to encourage employee participation.

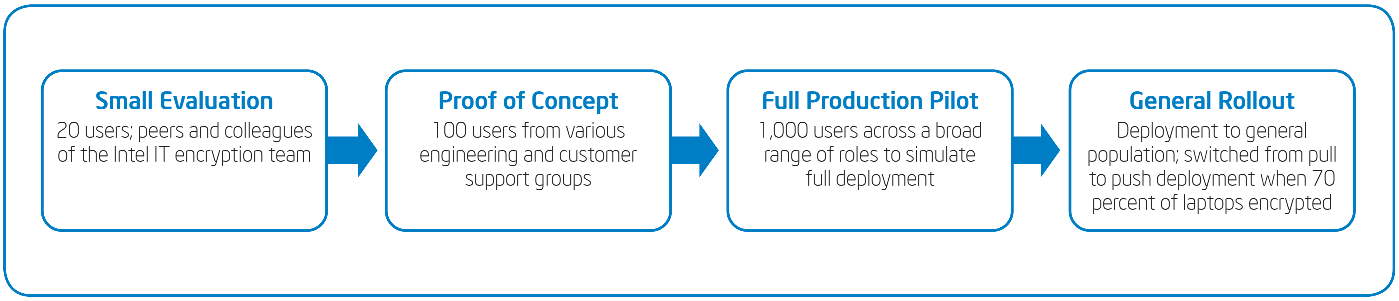
Small Evaluation
20 users; peers and colleagues of the Intel IT encryption team
Proof of Concept
100 users from various engineering and customer support groups
Full Production Pilot
1,000 users across a broad range of roles to simulate full deployment
General Rollout
Deployment to general population; switched from pull to push deployment when 70 percent of laptops encrypted

Figure 1. Intel IT deployed full disk encryption in four phases in order to test the solution thoroughly before general rollout.

Promoting Encryption Adoption

We decided to allow employees to schedule and perform their installations during the initial pull deployment phase based on our goal to reduce impact on employee productivity. However, this decision also caused many delays in the adoption of encryption. Employees postponed installation as they learned from peers and from Intel IT communications and training materials about installation time requirements and other issues.

Our installation instructions encouraged employees to enroll and download the encryption program while they were connected to the network at work, a process that took 10 minutes, and to start the encryption process during a time, such as at night or over the weekend, when they were not using the laptop. This was because this step took from two to four hours depending on the size and speed of the hard drive.

To improve installation rates, we handled issues as quickly as possible, improved our installation instructions to help employees avoid common pitfalls, and initiated communications to encourage adoption:

- We placed posters in Service Desk centers describing the importance of encryption so that anyone bringing a laptop in for service could read these posters.
- Intel's CEO and CIO sent e-mails explaining the importance of encryption and encouraging employees to install the encryption program. After the CEO's e-mail, we saw an 8x increase in encryption installation, shown in Figure 2. Getting the support of senior management was critical to successful deployment of our encryption program.
- We prioritized deployment to high-risk groups of laptops containing the most sensitive data, such as human resources data, for earliest deployment. We targeted our e-mail campaigns and prioritized PC refreshes to the highest risk groups to help ensure that adoption occurred in those groups more rapidly.
- We tied our e-mail communications campaign to call volume related to encryption issues received by the Service Desk. When calls fell below a pre-defined threshold, we increased our e-mail communications campaign, which encouraged more employees to install the encryption program. As Service Desk and service support call volume rose above a pre-defined threshold, we eased back on the e-mail campaign.

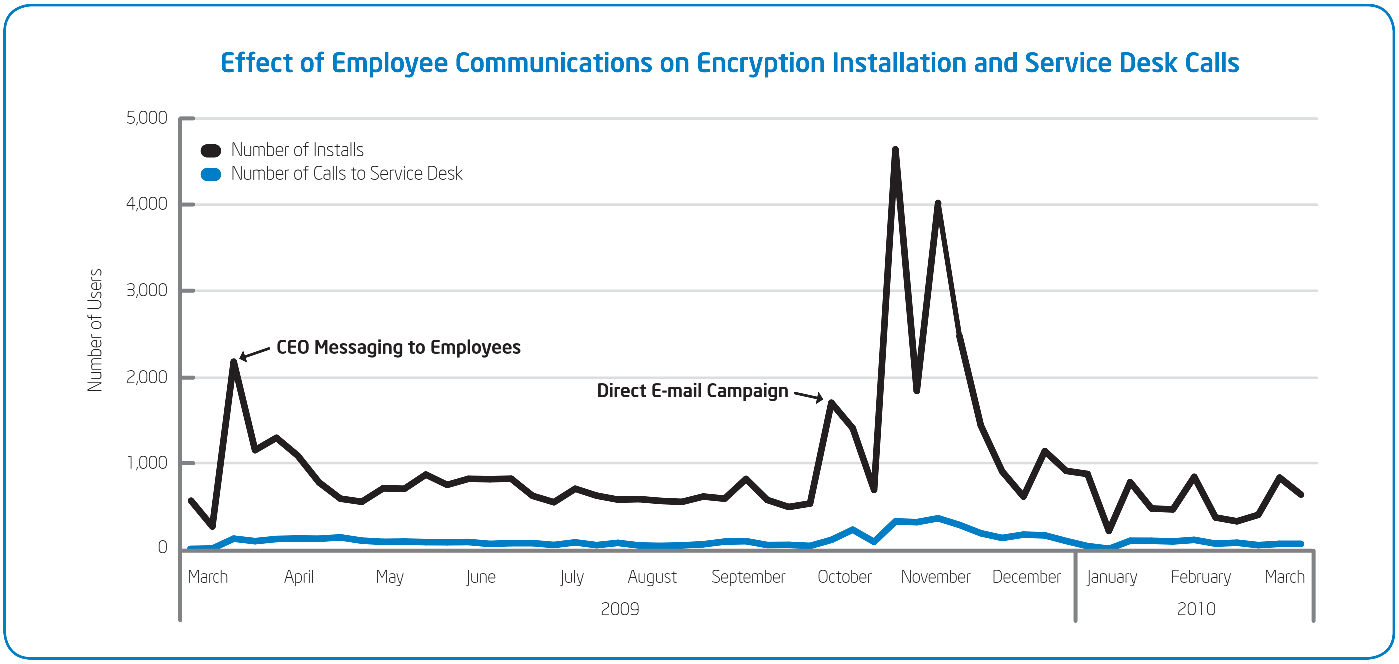

Figure 2. Intel executive e-mail communications and Intel IT's direct e-mail campaign to employees increased encryption program installations and Service Desk call volume. If call volume exceeded our limit, we slowed deployment by reducing these communications.

Better Security through Enhanced Management

Securing employee laptops requires more than data encryption. It also requires effective client management to maintain security-hardened configurations. To help us manage employee laptops (and desktops) more effectively, and at significantly lower cost, Intel IT is currently in the middle of a multi-year process that will upgrade our client systems and support infrastructure to take advantage of Intel® vPro™ technology. By the end of 2009, we had deployed and provisioned about 50,000 PCs with Intel vPro technology.

Client systems that are enabled with Intel vPro technology include built-in, hardware-based capabilities that help to improve security, maintenance, and asset tracking. These PCs can be accessed over wired and wireless networks by authorized management applications and support staff, even when the system is off, the OS is unresponsive, software agents are disabled, or the hard drive has failed.

We developed several use case scenarios for Intel vPro technology that increase productivity and reduce support costs. One scenario includes helping users to remotely reset their passphrases. The Service Desk can take control of the PC and remotely enter the passphrase recovery token in a matter of minutes. The passphrase recovery token is a 26- to 32-character alphanumeric string; entering this string remotely can save time and reduce errors resulting from miscommunication between Service Desk staff and the user. To learn more about this and other use cases related to the remote management capabilities of Intel vPro technology, see the video "3 Use Cases with Intel vPro technology" at http://communities.intel.com/docs/DOC-4165.

Implementing New Support Processes

Our early trial deployments confirmed that the main Service Desk issue for our encryption deployment involved providing laptop users with guidance for creating new passphrases. Employees previously had to enter two passwords before using their laptops: a hard drive authentication password required to start the system and OS logon password. After each employee's hard drive was fully encrypted, we retired the hard drive authentication password and replaced it with a laptop encryption passphrase.

However, in deploying the new encryption solution, we felt it was important to increase password length and strength requirements. Though employees continued to use their existing OS logon passwords, everyone had to create a new passphrase for the encryption solution to meet the new requirements.

Many employees were confused by the concept of passphrases, which are set using multi-word memorable phrases (like a sentence) with spaces between words. Many employees instead entered a long, complex string of characters (like a lengthy password with no spaces) that they often forgot, resulting in calls to the Service Desk.

To help reduce the confusion, we improved the encryption program installation instructions to clarify installation steps and to clear up misunderstandings about how to set strong passphrases. We provided guidance through e-mail and Intel's employee intranet portal, and prepared Service Desk staff to assist with passphrase issues. We also trained Service Desk staff to use the supplier tools provided for remotely resetting encryption passphrases. Eventually, employees who had already installed encryption began to teach their peers about how to set memorable, secure passphrases.

MITIGATING RECOVERY FAILURES RELATED TO FORGOTTEN PASSPHRASES

When employees called the Service Desk after forgetting their passphrases, Service Desk staff gave them a temporary recovery token valid for one-time use. After using the token to get past the passphrase request to log on again, some employees would neglect to change their passphrase before logging out. This resulted in system rebuilds with data recovery from backup. After initial discovery of this issue, we modified the support process to make sure that our Service Desk staff not only helped employees log on to their laptops with the recovery token, but also helped them immediately reset their passphrases. Service Desk staff explained the process to the user over the phone, which took from 15 to 20 minutes. Alternately, if the laptop had Intel vPro technology enabled, service support staff could remotely perform the same process within 3 to 5 minutes. (See the sidebar "Better Security through Enhanced Management.")

ACCESSING HARD DISKS FOR E-DISCOVERY

In cases where employees had separated from Intel, Service Desk staff needed to assist e-Discovery with gaining access to laptop data. We established a process whereby, with proper authorization, Service Desk staff helped e-Discovery staff log back on to returned laptops using a temporary recovery token, and then helped them to immediately reset the passphrase to gain access to laptop data.

Addressing Deployment Challenges

Throughout our deployment process, we dealt with numerous challenges.

ENTERPRISE DATA BACKUP

Pre-deployment discussions with other companies confirmed the need for an enterprise-wide backup process for data recovery. Because the encryption process touches every sector of a HDD, if the HDD hits a bad sector during the encryption process, the system may crash and permanent data loss could result.

As a precautionary measure, we required HDD backup before employees installed the encryption program. We found that some Intel locations lacked the capability or capacity for all systems to be backed up. This forced us to stop encryption deployment in some areas until those locations remediated this situation. However, requiring backups before encryption program deployment had an extra benefit: A higher percentage of employees are now able to back up their data at Intel.

UPDATING ASSET INVENTORY

To contact employees to install the encryption program, we needed a complete list of all laptops and the employees who use them. However, we discovered outdated information in our asset inventory system. This led to improvements in the system to provide more accurate accounting.

DISTINGUISHING OLD FROM NEW LAPTOPS

We saw significant performance delays when encryption was installed on older laptops. To address this issue, we decided to encrypt only laptops with Intel® Core™2 Duo processors or newer. We also equipped all new laptops with encryption during our regularly scheduled two- to four-year PC refresh cycles.

IDENTIFYING CONFIGURATION INCOMPATIBILITIES

About 10 percent of laptops across Intel had unique configurations to address specialized business needs, deviating from our standard builds. These configurations required custom fixes during deployment. We needed a way to easily identify these unique configurations before we asked users to deploy encryption to avoid installation issues and productivity loss.

We developed an application to help determine differences between unique and standard platform builds so that we could provide employees with steps to deal with their unique configurations during installation. If a laptop had an incompatible or alternative encryption program installed, we told employees how to remove it before installing the new one. For laptops with multiple builds and other system variations—such as multiple boot systems, multiple partitions, or multiple virtual environments—we told employees how to manage those variations during installation.

INTRODUCTION OF SOLID STATE DRIVES

Following an evaluation that showed significant benefits of using Intel® SSDs—including reductions in IT support costs and improvements in user productivity—we began deploying laptops with SSDs as part of our standard IT build. This decision occurred midway into our encryption deployment. Because SSDs provide much faster data access rates than HDDs, we initially saw a higher percentage of degradation in drive performance of SSDs compared to HDDs after encryption was installed.

To resolve this issue, we worked with our supplier to help redesign the encryption program to comprehend SSDs. The supplier improved code performance, provided an option to deploy either 256-bit or 128-bit encryption, and took advantage of Intel® dual-core technology and Intel® Hyper-Threading Technology available on newer laptops with Intel® Core™ i5 processors. This encryption program redesign resulted in a 2x performance improvement.

Results

To date, more than 75 percent of Intel's eligible laptops have been encrypted and push deployment is well underway. We have extended our schedule for encryption program deployment from our original estimate of one year to 18 months. This will help us provide better support to Intel's end users and help ensure support staff is not overburdened. We expect that all remaining corporate laptops will be encrypted by mid-2010.

Next Steps

We plan to work with our supplier to take advantage of significant performance gains achieved by laptops with Intel Core i5 processors and Intel® Core™ i7 processors in the next release of their encryption product. We also expect the next release will take advantage of new software optimized for Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). These instructions, built into these processors, enable both faster and more secure data encryption and decryption. We anticipate faster installation of the encryption program and significant performance improvements for start-up, shutdown, and transitions to and from hibernation.

CONCLUSION

Throughout our deployment of full disk encryption, we took steps to resolve challenges using numerous strategies. Our most successful strategies involved employee training, communication with executive and group management, modifications to support processes, resolving technical and operational issues, and collaboration with our supplier to boost encryption program performance and resolve other technical issues.

By early 2010, Intel employees had successfully installed the full disk encryption program on 70 percent of all eligible corporate laptops, which was our goal for switching from pull to push deployment. We then began implementing enforced push deployment of the encryption program to help ensure installation on remaining laptops. We anticipate that all remaining corporate laptops will be encrypted by mid-2010.

Near the end of our encryption program deployment, after we have push deployed all Intel IT-managed laptops, our team of encryption experts will manually encrypt all remaining laptops that require special attention because they are not Intel IT-managed.

As the risks and costs associated with serious attacks and laptop losses continue to rise each year, we have learned that our enterprise security strategies must become more vigilant. Intel IT's continued deployment of full disk encryption is an important part of those strategies.

FOR MORE INFORMATION

Find additional IT@Intel white papers at www.intel.com/IT.

- "Strengthening Enterprise Security through Notebook Encryption." Intel Corporation, December 2008.
- "Enterprise-wide Deployment of Notebook PCs with Solid-State Drives." Intel Corporation, August 2009.

ACRONYMS

BKM	best-known methods
FAQ	frequently asked question
FIPS	Federal Information Processing Standard
HDD	hard disk drive
Intel® AES-NI	Intel® Advanced Encryption Standard New Instructions
NIST	National Institute of Standards and Technology
SSO	single sign-on
SSD	solid-state drive

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.

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.

Printed in USA
0510/JLG/KC/PDF

♻ Please Recycle
323002-001US