Five Ways to Ensure Encryption is More Effective and Manageable

And how a managed security service provider can protect your data better while lowering costs

Key Takeaways:

- Encryption is now the widely accepted best practice for securing data.
- Effective encryption is not straightforward. IT staff must consider not only technical requirements, but also management, support and usability issues.
- Effective encryption should be strong encryption, should not visibly affect employees, be cost-effective and should be integrated with backup and recovery.
- A managed security service provider can bring ultimate control over encrypted endpoints with tools, expertise and around-the-clock support infrastructure.

Encrypting data on laptops, notebooks and tablet computers is now widely accepted as a best practice for any organization that works with customer and employee data, financial information and intellectual property. Indeed, it is an obligation for most industries that have any form of regulatory or association oversight with compliance requirements.

But effective encryption is harder to achieve than most people imagine. IT managers must consider not only technical requirements, but also management, support and usability issues. And because encryption is part of the bigger objective of protecting information, they must also consider how the technology interacts with data backup and recovery.

In this paper, we will outline why laptop encryption is so important, and look at five ways to make encryption more effective and manageable. We will also describe how a managed security services provider can make encryption reliable, easy and affordable.
Why Encrypting Data on Laptops Is Critical

Today, companies and government agencies must assume that a certain number of their laptops, notebooks and tablets will be lost or stolen. In a recent survey, one out of eight Canadian business owners reported that they had experienced the loss or theft of a laptop. Another study estimates that 7% of laptops used for business are lost or stolen over their useful life — 46% of which contain confidential data (and 71% of which are not backed up).\(^1\)

Lost and stolen laptops can be very costly in terms of internal expenses (such as replacement hardware and software, detection, support, forensics activities and loss of employee productivity) and external costs (such as loss of revenue and customer goodwill, data breach notification costs and fines, legal fees and loss of intellectual property). One research firm estimated the cost as high as $56,165 USD per unencrypted laptop lost.\(^2\)

Many Canadian firms also face government and industry regulatory requirements. For example:

- The Personal Information Protection and Electronic Documents Act (PIPEDA) mandates that “security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification” and states that “methods of protection should include … technological measures, for example, the use of passwords and encryption.”

- A series of rulings from the Office of the Information and Privacy Commissioner of Ontario essentially demands the encryption of personal health information (PHI) on laptops and desktop computers — one of the rulings was actually published with the completely unambiguous title, “Encrypt Your Mobile Devices: Do It Now.”

- The Payment Card Industry Data Security Standard (PCI DSS) requires that all companies handling payment card information “develop and maintain secure systems and applications.” The statement is generally interpreted to include a requirement to encrypt all payment card information stored on laptops, desktop computers and servers.

In all of these cases, companies that can prove that lost data was encrypted are not subject to penalties. For example, in one ruling, the Ontario commissioner states that “to the extent that personal health information on a mobile computing device has been encrypted to protect it from unauthorized access, I would not consider the theft or loss of that device to be a loss or theft of PHI. … The custodian would not be required to notify individuals [of a data breach] under [PIPEDA].”\(^3\)

In addition to avoiding the scrutiny of regulatory bodies, fines and search-and-destroy expenses, companies that comply with requirements for encrypting data are spared the brand damage and public embarrassment entailed in publicly disclosing the loss of devices containing customer and company data.

\(^1\) For simplicity’s sake, we will use laptops to refer to laptops, notebooks and tablets. Data on Canadian laptops lost or stolen is available at [http://www.nopaniccomputing.com/npc-infographic-risky-business.pdf](http://www.nopaniccomputing.com/npc-infographic-risky-business.pdf). For data on missing laptops in the U.S., see “The Billion Dollar Lost Laptop Problem,” Ponemon Institute, October 2010.

\(^2\) “Cost of a Lost Laptop,” Ponemon Institute, April 2009.

\(^3\) PIPEDA, Section 4.7. PHIPA Orders HO-004, HO-007 and HO-008. PCI DSS standards are available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). The quotation is from PHIPA Order HO-004.
Requirement No. 1: **Strong Data Encryption**

The first requirement for effective encryption of laptops is “strong data encryption,” a set of functional requirements that ensures that unauthorized people will be unable to access confidential data even if they have complete control of the laptop.

Typical characteristics of strong data encryption include:

- An advanced encryption algorithm such as Advanced Encryption Standard (AES) 256-bit.
- Compliance with FIPS 140-2 cryptography implementation standards.
- Secure management of encryption keys.
- Secure authentication of users through complex passwords or biometrics.
- “Encryption by default,” which occurs automatically, with no user action required.

One topic that is often overlooked is biometric authentication tools, such as fingerprint readers (FPR). Advanced implementations of these create an encrypted “vault” on the laptop that stores complex passwords for users’ data and login credentials, online services, virtual private networks and applications. Authorized employees can easily access encrypted material and logins by swiping a finger over the fingerprint reader, but if laptops are lost or stolen, outside parties will have greater difficulty cracking the passwords with dictionary or brute-force attacks, as the FPR makes using very-difficult-to-crack passwords practical in everyday use. This layered approach is convenient for employees and eliminates the all-too-common problem of people writing down passwords and leaving them stuck to the computer or in the carrying case. It also encourages employees to use longer and stronger passwords, since passwords have to be entered only once, after which the employees can authenticate through the fingerprint reader.

Requirement No. 2: **No Visible Impact on Employees**

Information security does not operate in a vacuum. Security measures that are intrusive or perceived to have a negative impact on productivity often cause a backlash among employees.

In some cases, the backlash may be limited to grumbling or minor ill will toward the IT department. But in other cases, the consequences may be more severe, leading employees to evade or disable the security solution. This can negate the value of the defense and leave the organization vulnerable to data loss.

And employees feel they are not entirely wrong to resist intrusive software and slow performance, since these problems affect productivity.

To be consistently effective, laptop encryption solutions should:

- Operate behind the scenes, without needing employee actions to initiate (or troubleshoot) encryption.
- Be “system-wide” to protect all relevant files, without requiring users to store data in special areas on the device.
- Encrypt files on the fly, without causing a notable slowdown in laptop performance.

---

4 “Health-Care Requirement for Strong Encryption,” a fact sheet published by the Ontario Information and Privacy commissioner, provides a good overview of strong encryption.

5 System-wide refers to the comprehensive protection of proprietary information. It does not mean full disk encryption, which often creates issues related to usability and performance and can significantly increase support costs.
Requirement No. 3: **Full Encryption Lifecycle Management**

Encryption is not a “set and forget” kind of technology. On each laptop, encryption has a lifecycle that includes deployment, updates, ongoing monitoring, performance management and decommissioning. Each of these processes involves effort and specialized expertise.

Unfortunately, deployment can be an extremely error-prone process, as illustrated by several real-world examples:

- PHIPA Order HO-008 revolved around a case where an automated process to install encryption on a laptop failed. The IT administrator and the laptop user both failed to notice a “Disk is not encrypted” error message. When the laptop was stolen, more than 20,000 patient records were exposed.  

- U.S. Government Accountability Office (GAO) auditors found that reliably installing encryption on laptops was beyond the competence of even rocket scientists (or, more precisely, the IT staff at NASA). According to their report, “[NASA’s] encryption software had been installed on 27 of 29 laptop computers. Although the agency asserted that it had installed it on all 29 laptops, officials explained that they did not have a mechanism to detect whether the encryption product was successfully installed and functioning.”

- The GAO found similar problems at the U.S. Department of Agriculture, where 10% of supposedly encrypted laptops turned out not to be encrypted, and “the agency had no mechanism in place to monitor whether the installed product was functioning properly.”

Another key component of encryption management is a reliable mechanism to update and monitor systems at remote locations. Special tools are available to ensure that encryption is deployed and fully functional, and to provide ongoing management through status alerts and casual monitoring.

Finally, decommissioning and “scrubbing” are needed to ensure that confidential data cannot be recovered after the systems are sold or discarded and encryption is no longer being managed.

Requirement No. 4: **Qualified Support**

Laptop encryption solutions can require fairly extensive remote support.

Work can come to a standstill if encryption keys become “scrambled” or corrupt, blocking access to data or entire devices. That means expert support personnel need to be available around the clock to respond to employee issues related to forgotten passwords and remote elimination and restoration of encryption keys.

Another important support function is the ability to monitor devices for suspicious activity. For example, a support representative alerted to repeated failed password attempts or fingerprint reader activity can contact the laptop user and confirm that the user is still in possession of the device, help troubleshoot why the user can’t access the system, and reset the password or fingerprint credentials.

A final support feature is the ability to block access to encrypted files if a laptop is believed to be lost, and to “wipe” the files if the loss or theft is confirmed. Providing this capability consistently is critical for protecting data from exposure and all its associated consequences.

---

6 PHIPA Order HO-008.
Requirement No. 5: **Integrated Backup and Recovery**

Encryption is one of several technologies needed to provide data protection and should be able to work effectively with related technologies, particularly backup and recovery.

If a laptop is lost or stolen, it is critical to protect the data on it from attackers, but it is also very important to recover that data and make it available to the employee again as fast as possible. That requires:

- Backup that is consistent and reliable.
- Mechanisms to quickly recover not only encrypted files, but also the encryption keys needed to access them.
- Multiple versions of backed-up data, in case the first-level backup suffers from malware corruption, active data corruption or similar problems.

To accomplish these goals, the encryption solution and the backup and recovery solution need to work hand in hand. Care must be taken so that the use of encryption on the device and in the backup never thwarts the availability of any version of the backed-up data.

**Managed Services: An Alternative to the Risks of Implementing and Managing Device Encryption**

Encrypting data on laptops is critically important, but it can be risky, difficult and costly. And with threats becoming more sophisticated, it doesn’t look like it will get easier any time soon.

A managed security service provider like NPC can provide the tools, expertise and around-the-clock support infrastructure to offload encryption challenges from the enterprise.

**Strong data encryption:** NPC’s integrated data protection service includes laptop encryption that meets FIPS 140-2 standards, uses AES-256 encryption, and provides for the secure remote management of encryption keys. It supports complex password policies and biometric authentication such as fingerprint readers. It enables encryption by default, providing encryption without any user action. The service exceeds the encryption-related recommendations described in the three PHIPA orders discussed earlier.

**No visible impact on employees:** The NPC service operates entirely behind the scenes, without intruding on employees. It also uses file-by-file encryption and other methods so that employees do not see a slowdown in their laptops or experience any loss of productivity.

**Full encryption lifecycle management:** The NPC operations center has the tools to deploy encryption remotely to new laptops, update the software and monitor continuously to make sure the encryption software is configured properly at all times. The service also includes decommissioning of laptops at the end of their life.

**Cost-effective support:** NPC provides around-the-clock support with highly trained security experts. They help employees anywhere and at any time remotely reset passwords, restore encryption keys, monitor laptops for suspicious activity, and block and wipe data remotely if a laptop is lost or stolen.
**Integrated backup and recovery:** NPC’s Managed Security Services include backup and recovery, integrated with encryption. Backups of both encrypted and unencrypted system files are performed on a regular schedule without disturbing employees. If files are lost or corrupted, they can be recovered directly over a secure internet connection to an existing laptop, or NPC can send a new laptop with all of the user files and keys needed to minimize downtime and resume operations quickly.

In short, NPC has the expertise and economies of scale to provide endpoint encryption that is extremely effective and meets compliance requirements. The company also oversees deployment, management, monitoring and support functions. The same service includes not only encryption and backup, but also intrusion and malware detection, 4G wireless services, secure decommissioning and other services that promote security and efficiency.

Contact NPC today at 1 (855) NO PANIC (667-2642), or visit [www.nopaniccomputing.com/free-quote](http://www.nopaniccomputing.com/free-quote) for a quote.
About NPC

NPC offers secure, professionally managed computers featuring a suite of backup, wireless, security and customer support services, controlled and supported by a sophisticated cloud-services strategy, all for one low monthly payment.

Every NPC device features biometric access with professionally managed encryption and is automatically backed up each day. All systems are constantly monitored for security and backup compliance, malware attacks, physical unauthorized intrusion attempts and system performance. Lost, stolen or defective systems are replaced within 48 hours, with data and applications restored.

NPC provides the benefits of infrastructure without a large financial investment, and keeps pace with rapidly changing privacy and compliance demands, security threats and industry trends to provide certainty and control of confidential information.

For more information, visit www.nopaniccomputing.com, email nopanic@npcmail.net or call 1-855-667-2642.