BEST PRACTICES

Encryption Technology

KASPERSKY lab

▶ ENCRYPTION MADE EASY

It's All About The Data

In the US alone, an estimated 12,000 laptops are lost or stolen every week. According to the Ponemon Institute, a laptop is stolen every 53 seconds. The figures for smartphones are no better — in 2011, 439 US organizations surveyed by Ponemon reported that, in the previous 12 months, 142,708 smartphones had been lost or stolen.

"Proactive data protection is a global imperative. Most of the world's major markets now require organizations of all sizes to implement data security and privacy initiatives. From PCI DSS to HIPAA, SOX or the UK's Data Protection Act, the global trend is towards authorities requiring that companies proactively protect sensitive data. In the UK, for example, the Information Commissioner (ICO) has said that data losses occurring "where encryption has not been used to protect the data" are likely to result in regulatory action."

If your first response to the above statistics is to consider the costs of replacing the hardware, you're focusing on the wrong problem. Hardware costs may be an issue for your organization, but in the event of a data loss incident, they're likely to be the least of your worries. When a laptop or device is lost or stolen, cleaning up the resulting data leakage mess accounts for more than 80 per cent of the associated costs, regardless of the size of the business.

Factor in the ever-increasing range of government fines for data breaches, reputational damage and impact on customer loyalty, and it's easy to see how the costs of a data breach spread well beyond hardware replacement. Eighty-five per cent of customers globally said they would take their business elsewhere if a business lost their personal information or was hacked; 47 per cent would take legal action.

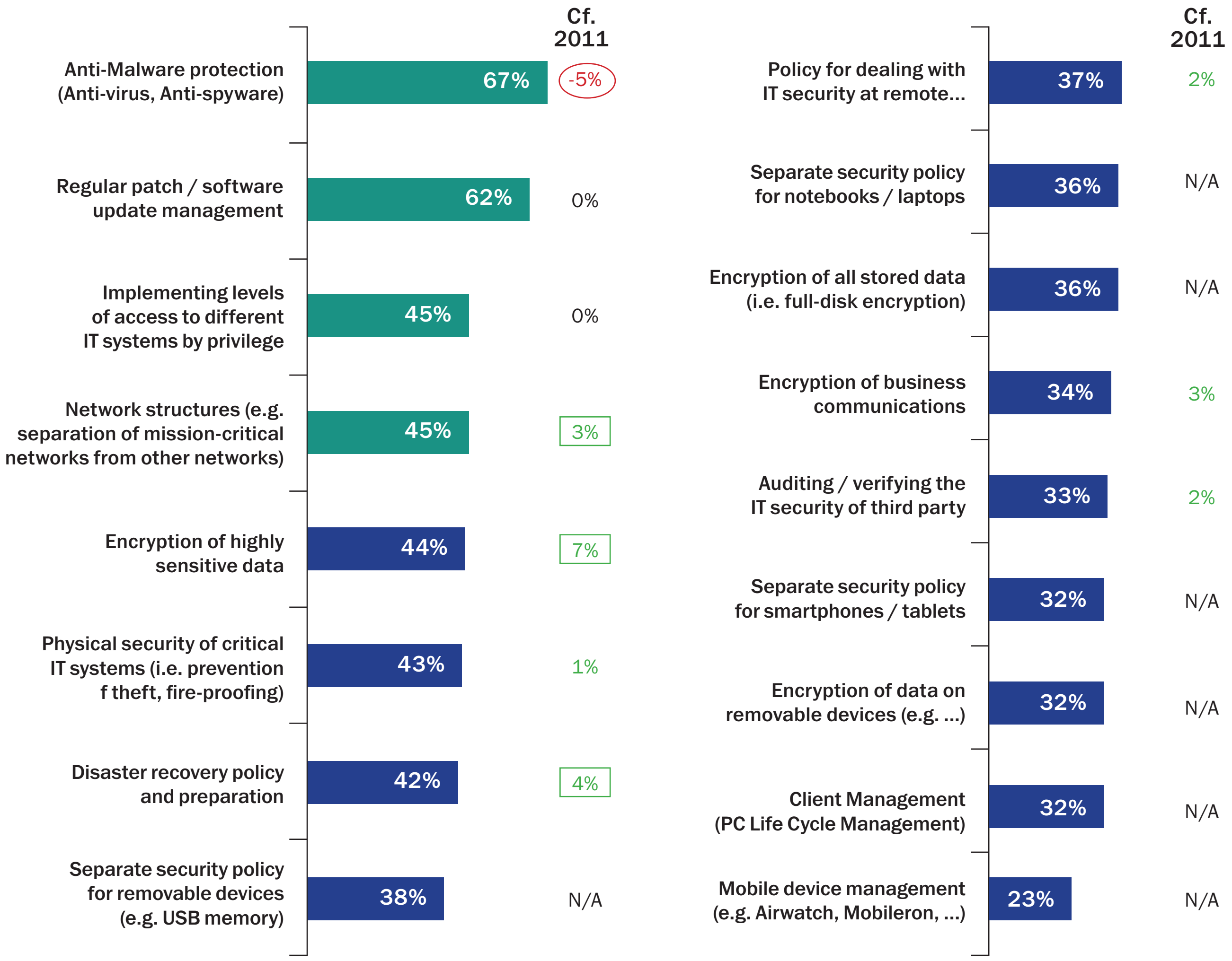
And you don't have to physically lose a device to lose sensitive data. Sensitive business information, intellectual property and trade secrets have become core targets of malware attacks.

Ponemon Institute suggests that the average value of a lost laptop is $49,246, with only 2 per cent accounting for the hardware replacement costs. Encryption can, on average, reduce the cost of a laptop by over $20,000. Whether you're faced with a stolen laptop, lost storage device or data stealing malware, encryption means your sensitive data is useless to criminals or unauthorized viewers.

So what's the best way to go about it?

BEST PRACTICE APPROACHES

There was a time when encryption was viewed as the sole preserve of government agencies or large corporations with even bigger budgets. Technology has moved on, however. Today, organizations of all sizes can afford to implement resource-efficient, easy-to-manage encryption solutions.



Encryption is increasingly being used as a tool in the fight against data loss.

Here are some best practice approaches you can take to ensure that your business adopts an effective encryption strategy.

1. POLICY FIRST, TECHNOLOGY SECOND

As with so many security strategies, best practice for encryption begins with establishing strong policies: Are you going to encrypt entire disk drives? Removable storage devices? Or just certain kinds of data, files and folders? Maybe you want certain documents to be unreadable to some users but not to others? How about a little bit of both?

For most businesses, making information accessible to the right people at the right time is a priority — good policies, coupled with the right technologies will get you there without compromising on security.

Some good places to start include:

- Include all relevant stakeholders — IT management, operations, finance. They'll help you to identify the kinds of information that need extra protection.
- Access control — If everyone's got a key, there's no point in locking the door. Work with stakeholders to identify who needs access to what kind of information. And when. As an extra precaution, audit access controls regularly to keep them relevant.
- Know your compliance needs — PCI DSS, HIPAA, GLBA, DPA… You might not be familiar with the growing number of data protection regulations out there, but many of your co-workers are. Identify the regulations, laws, guidelines and other external factors that govern the way data is secured or exchanged in the organization. Set policies to work with these — for example automatic encryption of customer credit card data or employee social security numbers.
- All in or all out — Put your policy in writing, have senior management endorse it and communicate it to your end users — including any third parties that handle your sensitive data. If they don't like it, that's fine — but they can't have access to your data.
- Back it up — best practice always involves backing up your data before installing any new software. Encryption is no different — make sure you back up all your end-user's data before proceeding with your encryption program.

2. FULL DISK ENCRYPTION OR FILE LEVEL ENCRYPTION?

The simple answer is: Both. Encryption solutions typically come in two key varieties — Full Disk Encryption (FDE) and File Level Encryption (FLE), each of which has its own set of benefits:

BENEFITS OF FULL DISK ENCRYPTION (FDE):

- FDE protects “data at rest” at the level as close to the hardware as possible — i.e. every single sector of the drive is encrypted. The means that all the data on your hard drive is encrypted, including file content, metadata, filesystem information and directories structure. Only authenticated users can access data on the encrypted drive. In addition to hard drives, FDE technology can be applied to removable media, such as USB drives or hard drives in a USB enclosure.

- Look for pre-boot authentication — this requires users to successful pass through an authentication process before the operating system will even launch, giving you an additional layer of security in the event that a laptop is lost or stolen — nothing can be read directly from the drive surface by thieves, nor can the OS be started.

- Best practice for FDE also includes a ‘set and forget’ policy, removing end-user choice from the equation; make access via a single sign-on (SSO) and your end users will be none the wiser.

- FDE’s greatest advantage is that it eliminates user error as a point of risk — it simply encrypts everything. On the down side, it cannot protect data in transit, including information shared between devices. If you’re following best practice, and have chosen a solution that also offers File Level Encryption, this won’t be a problem for you.

BENEFITS OF FILE LEVEL ENCRYPTION (FLE):

Operating at the file system level, FLE not only enables ‘data at rest’ protection, but also secures ‘data in use.’ Using FLE, specific files and folders on any given device can be encrypted. Best-in-class solutions allow encrypted files to remain encrypted, even when copied through the network. This makes selected information unreadable to unauthorized viewers, regardless of where it’s stored or copied to. FLE allows administrators to automatically encrypt files based on attributes such as location (e.g. all files in My Documents folder), file type (e.g. all text files, all Excel spreadsheets etc) or the name of the application that writes the file — for example, a best-in-class solution will support the encryption of data written by, say, Microsoft Word, independently of the folder or disk.

- FLE offers great flexibility to businesses seeking to apply granular information access policies — only data defined as sensitive (according to administrator-set policies) is encrypted, supporting mixed data usage scenarios.

- FLE also facilitates easy and secure systems maintenance — encrypted file data can remain secure while software or systems files are open to facilitate updates or other maintenance. For example, if you’re a CFO who wants to keep confidential business information out of sight of a systems administrator, FLE supports this.

- FLE supports effective application privilege control, allowing administrators to set clear encryption rules for specific applications and usage scenarios. Through application privilege control, administrators decide when to provide encrypted data in its encrypted form, or even complete block access to encrypted data for specified applications, for example:

  - Simplify secure backups by ensuring encrypted data remains encrypted during transfer, storage and restoration, regardless of the policy settings at the endpoint to which the data is restored.

  - Prevent exchange of encrypted files over IM or Skype, without restricting legitimate message exchange.

By adopting a combined FDE/FLE approach to encryption, businesses can take a best-of-both-worlds approach — you might, for example, choose file encryption only for desktop PCs, while enforcing full disk encryption on all laptops.

3. ENFORCE REMOVABLE MEDIA ENCRYPTION

USB flash drives can now hold 100GB+ of data, while portable drives smaller than your hand can hold terabytes of data — that’s a lot of potentially business-critical information being left in jacket pockets at the dry cleaners, left behind in the security tray at the airport or simply falling out of your pocket.

You can’t control user carelessness of accidents, but you can control the consequences. Effective encryption strategies include device encryption as standard. Ensure that every time sensitive data is transferred from an endpoint to a removable device, it is encrypted. You can do this by applying FDE or FLE policies to all devices, thereby ensuring that even when they are lost or stolen, your sensitive data is secure.

When working with sensitive information both inside and outside the perimeter, so-called ‘portable mode’ should be adopted. For example, you’re making a presentation at a conference and have to use a flash drive to transfer your data to a public computer that doesn’t have encryption software installed. You need to ensure that your data remains secure, even while it’s travelling from your laptop to the presentation system — best-in-class solutions offer ‘portable mode’, allowing you to do this. It enables transparent use and transfer of data on encrypted removable media, even on computers where encryption software is not installed.

4. CHOOSE INDUSTRY PROVEN SECURE CRYPTOGRAPHY

Your encryption strategy is only as good as the technology that underlies it. Easily cracked encryption algorithms are worthless. Advanced Encryption Standard (AES) with 256 bit key length is considered the ‘gold standard’ of encryption techniques. It’s used by the U.S. government and is industry-standard worldwide. Don’t underestimate the importance of keys — your encryption algorithm is only as good as the key needed to unlock it. Easily hacked keys make your entire encryption program worthless. Similarly, effective key management is a vital component of effective encryption — there’s no point in having the world’s best lock on the door if you put the key under the mat.

5. DON’T FORGET ANTI-MALWARE PROTECTION

Laptops that aren’t lost or stolen can still be at risk for data loss. Cybercriminals are increasingly targeting sensitive information on business devices, writing malicious code that can steal information from laptops without the user’s knowledge.

No encryption best practice strategy is complete without integrated malware protection capable of targeting malicious code designed to siphon off valuable information from your laptop. Best practice calls for anti-malware updates and scanning capabilities that can be performed automatically, without end-user interference.

6. FORGOT YOUR PASSWORD?

Users forget their passwords almost as often as they lose their USB keys or smartphones. Sometimes even the best hardware or operating system can fail, leaving users without access to vital information. Keep encryption keys in a centralized storage location/escrow — this makes it a lot easier for you to decrypt data in emergency situations.

A quality encryption solution should provide administrators with tools for straightforward data recovery in the following cases:

- When the end user requires it (e.g. forgotten password)
- When the administrator needs it for maintenance, or in case of a technical issue, such as an OS that won’t load or a hard drive has physical damage that must be repaired.

When a user forgets their password, alternative authentication can be achieved by requiring them to give the correct response to a series of alternative questions.

7. KEEP IT SIMPLE, KEEP IT CENTRAL

Traditionally, a common complaint from businesses seeking to deploy encryption has been that it’s too complicated to implement and manage. Many older solutions are provided separately from anti-malware, for example, adding an extra layer of complexity. Managing diverse solutions — anti-malware, endpoint control, encryption — even from a single vendor (never mind multi-vendor environments!) is not only expensive, it’s time consuming at all phases of the solution adoption cycle: Purchasing, staff education, provisioning, policy management, maintenance and upgrade all need to be treated as separate projects for each component. An integrated approach not only saves time and money, but makes the software adoption process as easy and painless as possible.

Easy to manage solutions are more effective. Choose one that enables single-console, single-policy management from day one, reducing investment and eliminating compatibility issues between numerous components, all being managed separately.
It’s good practice to apply endpoint encryption settings under the same policy as anti-malware protection, device control and all other endpoint security settings. This enables the best practice approach of integrated, coherent policies — for example, IT can not only allow approved removable media to connect to a laptop, but can also enforce encryption policies to the device. A closely integrated technology platform has the added benefit of improving overall system performance.

KASPERSKY LAB — MAKING BEST PRACTICE A REALITY

Kaspersky Endpoint Security for Business can help make encryption best practice a reality for organizations of all sizes. Combining gold-standard encryption technology with Kaspersky's industry-leading anti-malware and endpoint control technologies, our integrated platform helps protect sensitive data from the risks associated with device loss or theft while keeping information safe from data-stealing malware.

Granular controls and rich functionality are easily deployed from a single, centralized management console, offering administrators a genuinely 'single pane of glass' view over their security landscape — whether it's virtual machines, physical or mobile/ removable devices.

Unlike many traditional data protection offerings, Kaspersky Endpoint Security for Business enables a ground-up approach to single policy management: Encryption policies are set within the same overall policies for anti-malware protection, device control, application control and all other endpoint security settings. This ground-up approach is possible because of Kaspersky's unified code base — our developers create software and technologies that interact seamlessly, giving users a security platform rather than a disjointed suite. Close integration of essential security components such as anti-malware, encryption, application and device control simplifies management and monitoring while delivering stability, integrated policies, reporting and intuitive tools. One vendor, one cost, one installation, **complete security**.

[1] **Newspoll survey**, November 2011.

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

© 2012 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Mac and Mac OS are registered trademarks of Apple Inc. Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. IBM, Lotus, Notes and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, Windows Server and Forefront are registered trademarks of Microsoft Corporation in the United States and other countries. Android™ is a trademark of Google, Inc. The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.