Secure USB Flash Drives

June 08

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

Secure USB Flash Drives

June 2008

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways.

The author wishes to acknowledge and thank Dror Todress of SanDisk and Louis Marinos of ENISA for the prompt support, valuable input and material provided for the compilation of this paper.

The author would also like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions and solutions. The content would be incomplete and incorrect without their help.

Contents

Executive summary

Over recent years, corporate end-users have increasingly needed to be fully mobile and connected, taking work home or out of the office to keep up their productivity. Staff needs to be able to synchronise files between a computer and the drive to allow key data to be backed up and available for use on the road or on other PCs ([1]). Thus, the use of mobile devices such as laptops, notebooks, universal serial bus (USB) flash drives, personal digital assistants (PDAs), advanced mobile phones and other mobile devices have proliferated in recent years ([2]).

In particular, personal storage devices such as USB flash drives have gained in capacity and have become ubiquitous in the enterprise environment ([3]). However, these devices are usually lacking in security, control and management tools and, in most cases, their use is not covered by a corporate policy foreseeing audit, backup, encryption or asset management.

Recent events have raised concern, leading organisations to understand that to secure corporate information stored on personal USB drives, new policies and technologies must be put in place ([4]). Often the measures organisations take to secure information stored on mobile devices are inadequate. Enterprises with highly regulated or sensitive data should consider controlling the use of plug-and-play devices. However, awareness of the risks and available safeguards is the first line of defence for security ([5]).

This document gives a brief outline of the corporate data which is susceptible to security breaches/incidents, and highlights potential risks associated with the innocent use of USB flash drives by employees of enterprises and also other less legitimate purposes such as smuggling information out of the company. Furthermore, it lists good practice guidelines which aim at helping readers to overcome obstacles within their organisations. The first step is to set clear security policies and make employees aware of them.

This paper targets IT departments, in particular IT managers and professionals, to ensure the ability to secure information on the network as well as the opportunity to manage data which enter and leave the company via these mobile devices. It also targets corporate end-users in general, to raise awareness of the risks related to the use of USB flash drives.

This document does not cover the associated legal aspects. Moreover, it should not be seen either as a comprehensive source of all risks associated with the use of personal USB flash drives for work-related purposes or a technical guideline to secure standards or solutions.

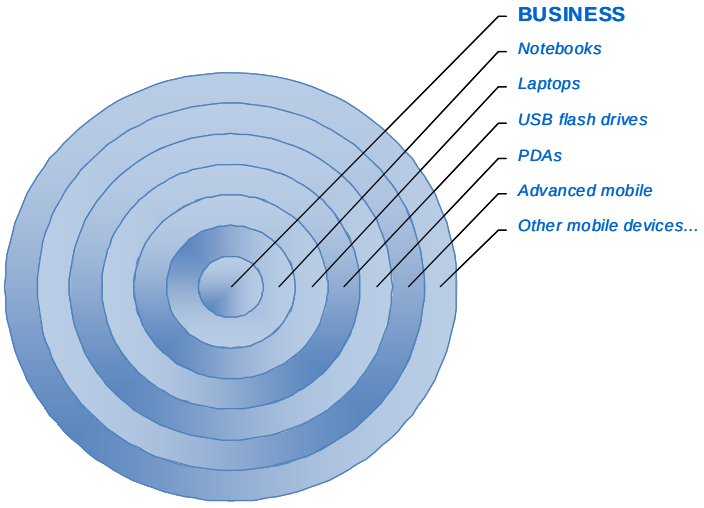
([1]) DataTraveler Secure and DataTraveler Secure — Privacy Edition White Paper, *Kingston Technology, Rev. 2.0, June 2007.*
([2]) Determine the appropriate level of ITAM controls for mobile assets, *Jack Heine, Gartner, 15 November 2005.*
([3]) Seven steps to secure USB drives, *SanDisk, July 2007.*
([4]) Seven steps to secure USB drives, *SanDisk, July 2007.*
([5]) A users' guide: how to raise information security awareness, *ENISA, June 2006.*

PART 1:

USB flash drives and related security implications

The use of mobile devices

In today's digital age where we live and work, corporate end-users need to travel light and be fully connected. As a result, an increased number of portable devices are used in business, such as laptops, notebooks, universal serial bus (USB) flash drives, personal digital assistants (PDAs), advanced mobile phones and other mobile devices.



With employees using mobile devices, travelling with data and taking work home, companies are constantly at risk from unprotected data on an unsecured USB flash drive. The consequence can be devastating: lost reputation, lost jobs, lost profits ([6]). Customer data, financial information, business plans, patient records and confidential information are only some examples of the data that are usually stored and transported. A considerable number of end-users are unaware of their exposure to security risks while doing so, as recent news incidents have highlighted ([7]).

For example, in the UK, a laptop with data of some 2 000 people with individual savings accounts (ISAs) was stolen from a HM Revenue & Customs employee; HM Revenue & Customs lost personal details of 6 500 private pension holders; nine NHS trusts lost patient records kept on disk; details of 1 500 students were lost in the post; details of three million British learner drivers were lost in the United States ([8]); a USB drive was stolen with names, grades and social security numbers of 6 500 former students ([9]); USB flash drives with US Army classified military information were up for sale at a bazaar outside Bagram, Afghanistan ([10]).

([6]) DataTraveler for Enterprise, *Kingston, 2008, available at* http://www.kingston.com/flash/DataTravelers_enterprise.asp *(last visited on 30 May 2008).*
([7]) McAfee encrypted USB — Data sheet, *McAfee.*
([8]) *'Timetable of missing data blunders'*, The Times, *20 February 2008; 'Disc listing foreign criminals lost for year'*, The Times, *20 February 2008.*

The potential for damage caused by the loss or stealing of sensitive corporate data grows exponentially every day, underlying the need for proper security measures that cover these hand-held mobile storage devices ([11]). Data loss is not just an IT or security problem; it is a business issue that reaches into many corners of an enterprise ([12]).

According to the Datamonitor report commissioned by McAfee, 60 % of the 1 400 IT decision-makers surveyed across the globe said that they had experienced a data leak, and only 6 % could state with certainty that they had had no data leakage problems in the past two years. Furthermore, 61 % believe data leaks are the work of insiders ([13]).

USB drives

A definition

USB drives are solutions to store and manage enterprise data within and outside the enterprise environment. USB drives are also known as a keychain drive, flash drive or disk-on-key. They are plug-and-play portable storage devices that use flash memory and are lightweight enough to attach to a key chain. The first USB flash drive was sold in 2000.

USB drives are a powerful and popular tool for mobile professionals in enterprises or government agencies as they have:

- ✓ small size and light weight
- ✓ fast speed — 24MB/s
- ✓ big capacity
- ✓ low price
- ✓ plug-and-play functionality.

They continue to proliferate and see strong demand in terms of unit shipments. In 2006, Gartner forecasted the unit shipments to pass 114 million ([14]). In 2007, 85 million were sold but only a few of those buyers thought about the drives' security implications ([15]). A Gartner research found that 22 % of USB flash drives are sold to enterprises and about 80–90 % are not encrypted ([16]).

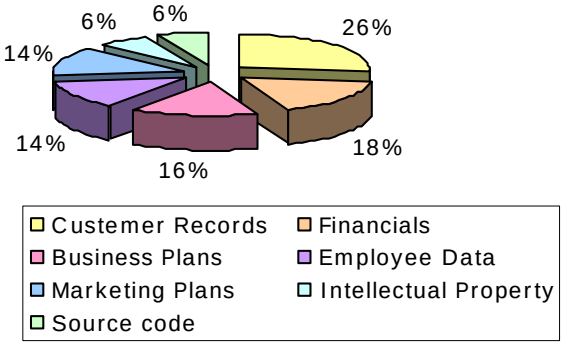
USB flash drives are a cheap and convenient way to move data off your computer — much easier than taking a laptop or hard disk drive ([17]). A recent study developed by SanDisk shows the

([9]) *'Small drives cause big problems', John Swarts,* USA Today*, 16 June 2006.*
([10]) *'US military secrets for sale at Afghanistan bazaar', Watson,* Los Angeles Times*, 10 April 2006.*
([11]) Seven steps to secure USB drives*, SanDisk, July 2007 and* Mobile device security in 2006*, Forrester, February 2006.*
([12]) Getting started with McAfee host data loss prevention*, McAfee, 2008.*
([13]) *'New report chronicles the cost of data leaks', Physorg.com, 2007, available at http://www.physorg.com/news96708147.html (last visited on 2 June 2008).*
([14]) Dataquest insight: USB flash drive market trends, worldwide, 2001–2010*, Joseph Unsworth, Gartner, 20 November 2006;* Forecast: USB flash drives, worldwide, 2001–2011*, Joseph Unsworth, Gartner, 24 September 2007.*
([15]) *'Thumb drives are too often the victims of convenience', John Zyskowski,* GCN*, 14 December 2006, available at chttp://www.gcn.com/online/vol1_no1/44136-1.html (last visited on 30 May 2008).*
([16]) *'Data breaches are "everyday incidents"', Matt Chapman, vnunet.com, 15 November 2007, available at http://www.vnunet.com/vnunet/news/2203540/security-breaches-everyday (last visited on 30 May 2008).*
([17]) *'The portable risk of high capacity USB drives', Allan Leinwand, GigaOM, 5 December 2007, available at http://gigaom.com/2007/12/05/the-portable-risk-of-high-capacity-usb-drives/ (last visited on 30 May 2008).*

following ([18]).

- ✓ The majority of corporate end-users (77 %) have used a personal USB flash drive for work-related purposes. They have reported that one out of five have little to no awareness about the risks involved with transporting corporate data on USB flash drives (21 %), revealing a significant potential for data loss.
- ✓ IT decision-makers anticipate that about 35 % of their workforce use personal USB flash drives to transport corporate data.
- ✓ About 41 % of IT decision-makers are not comfortable about the current level of USB flash drive usage in their organisation.

Corporate Data on USB Flash Drives



In a study conducted by the Ponemon Institute, it was found that more than half of employees report copying sensitive information to USB flash drives, even though 87 % of those companies had policies prohibiting the practice ([19]). This factor underlines that employee knowledge on corporate policies on USB usage is very limited. If we look at the training on policies around USB flash drive usage offered by the enterprises, we are convinced that there is a clear correlation. The SanDisk study shows that employees are trained either once per year on policies around USB drive usage (33%); that they are trained more than once per year (24 %); that employees receive training only once when they join the company (22 %); that they are trained on demand (17 %); and that they never train employees (3 %) ([20]). It is therefore crucial to underscore that education and awareness of the risks while using USB flash drives have a powerful effect on employee behaviour, since they promote a secure use in their day-to-day work.

Among recent incidents

The number of recent incidents goes on as USB flash drives get lost, misplaced, borrowed without permission or stolen ([21]). Below are reports of some of them ([22]).

- ✓ A misplaced USB flash drive found on a public computer was handed over to the Swedish armed forces. The drive contained two classified documents and was returned to the armed forces from an individual who discovered it at a public computer centre in Stockholm. An employee of the armed forces reported that the misplaced USB flash drive belonged to him. The drive contained both unclassified and classified information such as information

([18]) SanDisk endpoint security survey, *SanDisk, April 2008.*
([19]) Survey of US IT practitioners reveals data security policies not enforced, *Ponemon Institute and RedCannon Security, December 2007, available at http://www.ponemon.org/press/RC_PonemonSurvey_FINAL.pdf (last visited 2 June 2008).*
([20]) SanDisk Endpoint Security Survey, *SanDisk, April 2008.*
([21]) DataTraveler Secure and DataTraveler Secure — Privacy Edition White Paper, *Kingston Technology, Rev. 2.0, June 2007.*
([22]) *To read more on recent security incidents, please refer to 'Educational security incidents (ESI) — Sometimes the free flow of information is unintentional', available at http://www.adamdodge.com/esi/month/2008/01; 'Privacy and identity theft', Dave Jevans, IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008); and 'Thumb drives are too often the victims of convenience', John Zyskowski, GCN, 14 December 2006, available at http://www.gcn.com/online/vol1_no1/44136-1.html (last visited on 30 May 2008);* Plugging the leaks: best practices in endpoint security, *SanDisk, 2008.*

regarding IED and mine threats in Afghanistan ([23]).

- ✓ The UK National Health Service lost two unencrypted USB drives with patient record data of 148 patients. This followed on the heels of the UK Revenue & Customs service which lost an unencrypted CD-ROM with 25 million taxpayers' information on it ([24]).
- ✓ A loss of a USB flash drive containing hospital files of the Prince of Wales Hospital (PWH) Hong Kong took place in early May 2008. The stored files were mainly general working documents with personal data of patients, including name, ID number and laboratory test items. It has been estimated that around 10 000 records were involved ([25]).
- ✓ A USB flash drive with information on about 8 000 Texas A&M University Corpus Christi students was lost by a mathematics professor while on holiday in Madagascar. The USB flash drive held social security numbers and other information for students of all classifications and majors enrolled during the spring, summer and fall of 2006. The drive was owned by Department of Mathematics Chairman who took it with him on a two-week holiday and discovered it was missing as he was packing to go home ([26]),
- ✓ USB flash drives with US Army classified military information was up for sale at a bazaar outside Bagram, Afghanistan. The drives also included deployment rosters and other documents that identified nearly 700 US service members and their social security numbers, information that identity thieves could use to open credit card accounts in soldiers' names ([27]).
- ✓ About 13 000 employees at Pfizer Inc., including about 5 000 from Connecticut, had their personal information compromised when a company laptop and USB flash drive were stolen. The data breach, which occurred on 12 May 2008, was the second this year affecting Pfizer Inc. employees and the sixth made public in a one-year span dating back to May 2007. More than 65 000 data-breach notifications have been sent out by Pfizer over the past year, including more than 10 000 to employees from Connecticut. The company said that no social security numbers were on the laptop, but names, home addresses, home telephone numbers, employee ID numbers, positions and salaries were possibly compromised. Other information possibly lost included the department employees worked in, the Pfizer site where the employees worked, the name of employees, managers and descriptions of their jobs ([28]).
- ✓ A laptop computer containing the personal information of about 8 000 students was stolen from a Spring ISD employee's car. A testing coordinator's car was broken into when she made a quick stop on her way home from work. The car burglars made off with her school laptop and an external USB flash drive. The USB flash drive contained students' social security numbers, personal information, schools those students attend, as well as their grade level and birthdates. The drive also contained the Texas Assessment of Knowledge and Skills test results ([29]).
- ✓ The personal information of 6 500 current and former University of Kentucky students, including names, grades and social security numbers, was reported stolen 26 May 2006 after the theft of a professor's USB flash drive. The drive has not been recovered, and the

([23]) *'Privacy and identity theft', Dave Jevans, IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008).*
([24]) *'Privacy and identity theft', Dave Jevans, IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008).*
([25]) *'Prince of Wales Hospital announced an incident of loss of USB flash drive containing hospital files', Press releases, 6 May 2008, available at http://www.info.gov.hk/gia/general/200805/06/P200805060232.htm (last visited on 30 May 2008).*
([26]) *'TAMU Corpus Christi prof loses flash drive with 8 000 student records', Paul McCloskey,* Campus Technology, *18 August 2007, available at http://campustechnology.com/articles/48635 (last visited on 30 May 2008).*
([27]) *'Afghan market sells US military flash drives', Paul Watson,* Los Angeles Times, *18 April 2006, available at http://www.veteransforcommonsense.org/ArticleID/7120 (last visited on 28 May 2008).*
([28]) *'Another laptop stolen from Pfizer, employee information compromised', Lee Howard, 12 May 2008, available at http://attrition.org/dataloss/2008/05/pfizer01.html (last visited on 30 May 2008).*
([29]) *'Spring students' info at risk after laptop theft', KHOU.com staff report, 16 May, 2008, available at http://attrition.org/dataloss/2008/05/spring01.html (last visited on 30 May 2008).*

university is re-evaluating its use of USB flash drives ([30]).

- ✓ In October 2005, Wilcox Memorial Hospital in Lihue, Hawaii, informed 120 000 current and former patients that a USB flash drive containing their personal information (names, addresses, social security numbers and identifying medical record numbers) had been lost. It has yet to be recovered. The drives, in use only a few months, have been barred.

Though these incidents were different, the cause of each was the same: an insufficient awareness of the risks related to the use of USB flash drives while transporting sensitive data and a non-rigorous endpoint security policy.

Major dangers for USB drives

The uncontrolled use of USB drives is a major danger since it represents an unquantifiable yet significant threat to information confidentiality. Thus the following should be taken into consideration for securing USB drives assets.

- ✓ Storage: USB flash drives are usually put in bags, backpacks, laptop cases, jackets, trouser pockets or are left on unattended workstations.
- ✓ Usage: corporate data are stored on personal non-secure drives and move constantly. As USB drives gain wider acceptance among IT departments in organisations, the likelihood of security breaches and data loss increases. Many enterprises have strict management policies toward USB drives, and some companies ban them outright to minimise risk. Software solutions may help minimise risk by allowing corporations to record the interactions between the drive and the PC or server and record them in a centralised database ([31]).
- ✓ Costs: the average cost per breach ranges from less than USD 100 000 to about USD 2.5 million ([32]).
- ✓ Type of documents which are stored: public, internal, confidential, restricted and protected documents. According to the different industry sectors (bank, insurance etc.) The information which may be stored is different. Corporate end users most frequently copy customer data (25 %), followed by financial information (17 %), business plans (15 %), employee data (13 %), marketing plans (13 %), intellectual property (6 %), and source code (6 %) ([33]).

Type of documents

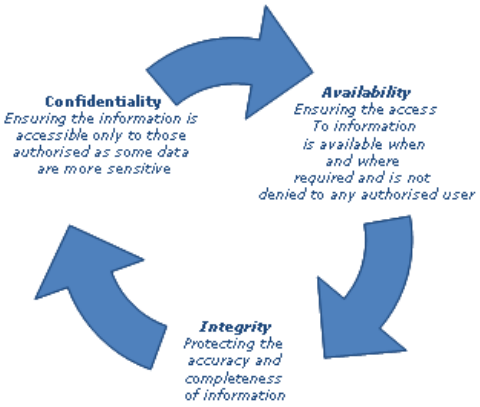
- ❖ *Public information: available to everyone*
- ❖ *Internal information: moves freely between the organisation*
- ❖ *Confidential information: moves between specific departments and/or business unit under a non-disclosure agreement (NDA)*
- ❖ *Restricted information: shared between selected employees of the enterprise*
- ❖ *Protected information: secured at all costs.*

([30]) *'Small drives cause big problems'*, *Jon Swartz* , USA Today, *16 August 2006, available at* http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm *(last visited on 27 May 2008).*
([31]) USB flash drive market trends, worldwide, 2001–2010, *Joseph Unsworth, November 2006, Gartner.*
([32]) SanDisk Endpoint Security Survey, *SanDisk, April 2008.*
([33]) SanDisk Endpoint Security Survey, *SanDisk, April 2008.*

Enterprise concerns

The following are some of the major enterprise concerns related to the use of USB flash drives ([34]).

- ✓ Data leakage: to limit data leakage, organisations should regulate the use of USB drives, eventually allowing the use of company-authorised USB flash drives only ([35]).
- ✓ Regulatory and security standards compliance challenges: having enterprises take care of secure USB flash drives usage will help in complying with the three aspects of security (i.e. confidentiality, availability and integrity) and some security standards and/or compliance framework (e.g. Sarbanes-Oxley, PCI data security standards etc.);



- ✓ Lost data and support costs: security policy could help enterprises recuperate stolen or lost data which occur even when security measures are in place, decreasing the costs of ownership and support.

Security implications

When enterprise information is stored on personal and non-secure USB flash drives, employees put their employer at risk both when they are inside or outside the company building. But the level of risk and threat which may occur is higher when sensitive information leaves the company as data may fall more easily into the wrong hands ([36]).

USB flash drives are a major security concern as more are lost or stolen. A survey, sponsored by the security firm Vontu, shows that more than half of the 484 tech professionals polled said that USB drives contain confidential information that is unprotected. At least one USB flash drive with data is lost at work each month, according to 20 % of those polled. Organisations are struggling to find out where the data is and where it is going. Furthermore, in most cases, employees do not report if USB flash drives go missing. An employee can download USD 25 million worth of

([34]) Seven steps to secure USB drives, *SanDisk, July 2007.*
([35]) USB flash drive protection, *Ron LaPedis, SanDisk, Disk Encryption Forum, 13 February 2007.*
([36]) Getting started with McAfee host data loss prevention, *McAfeee, 2008.*

information on a USB which can be bought for just USD 25 ([37]).
The security implications from personal storage devices can be classified as follows ([38]):

- ✓ data exposure due to device loss, theft or un-accurate usage;
- ✓ unauthorised data extraction;
- ✓ introduction of malicious code.

Risks and threats

Looking at the use of non-secure personal USB drives and the consequence of transferring and transporting corporate data, the number of risks and threats is almost infinite. The following can be identified.

- ✓ Data leakage ([39]): it is not possible to estimate the effects of valuable data leaking out of an organisation, but the problem is growing.
- ✓ Information loss: USB drives going missing or forgotten somewhere. It is most likely that other people seeing information (e.g. customer and/or employee data), eventually marked as confidential, keep the data for personal use and eventually reformat the device for personal use. This can possibly result in legal liability.
- ✓ Information confidentiality: when information falls into the wrong hands, the enterprise suffers a much greater loss than simply the replacement of the cost of the drive.
- ✓ Information integrity: when content is changed.
- ✓ Corruption of data: if the USB flash drive is closed to magnetic fields and/or is uncleanly dismounted. Usually the OS will attempt to handle unexpected disconnects as best it can, so corruption will not occur.
- ✓ Data security: smuggling information out of the enterprise.
- ✓ Damage to company business/reputation/image: when a USB drive is stolen and used to damage the business/reputation/image of the company.
- ✓ Market leadership loss.
- ✓ Virus transmissions/worms ([40]): when files are transmitted between two machines there is a risk that viral code or some other malware will be transmitted. In April 2008, a batch of HP USB drives was shipped with a virus.
- ✓ Spyware ([41]): when the host computer is compromised by spyware and other threats. In this case, the software-based security used in most consumer USB flash drives with password protection is less reliable than the hardware-based encryption because software-based protection relies on the host computer to perform security operations;
- ✓ Software vulnerabilities ([42]).
- ✓ Fraud/deception:
  - extortion;
  - identity theft;
  - theft of intellectual property, trade secrets, proprietary information.

([37]) *'Small drives cause big problems'*, *Jon Swartz* , USA Today, *16 August 2006, available at* http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm *(last visited on 27 May 2008).*
([38]) Seven steps to secure USB drives, *SanDisk, July 2007.*
([39]) Understanding data leakage, *Jay Heiser, Gartner, 21 August 2007; 'Data-leak security proves to be too hard to use', Infoworld.com, available at* http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html *(last visited on 2 June 2008).*
([40]) *Viruses/worms have been identified as one of the top three security threats by IT decision-makers within the* SanDisk Endpoint Security Survey, *SanDisk, April 2008. See as well* McAfee®VirusScan® USB — proven security that protects your USB drive against viruses, *McAfee, 2006, available at* http://download.mcafee.com/products/manuals/en-us/vsusb_datasheet_2007.pdf *(last visited on 30 May 2008).*
([41]) *Spyware has been identified as one of the top three security threats by IT decision-makers within the* SanDisk Endpoint Security Survey, *SanDisk, April 2008.*
([42]) *Software vulnerabilities have been identified as one of the top three security threats by IT decision-makers within the* SanDisk Endpoint Security Survey, *SanDisk, April 2008. See as well* New attacks: device vulnerabilities stand out, *Avivah Litan, Don Dixon, Greg Young, Gartner, 21 June 2005.*

PART 2:

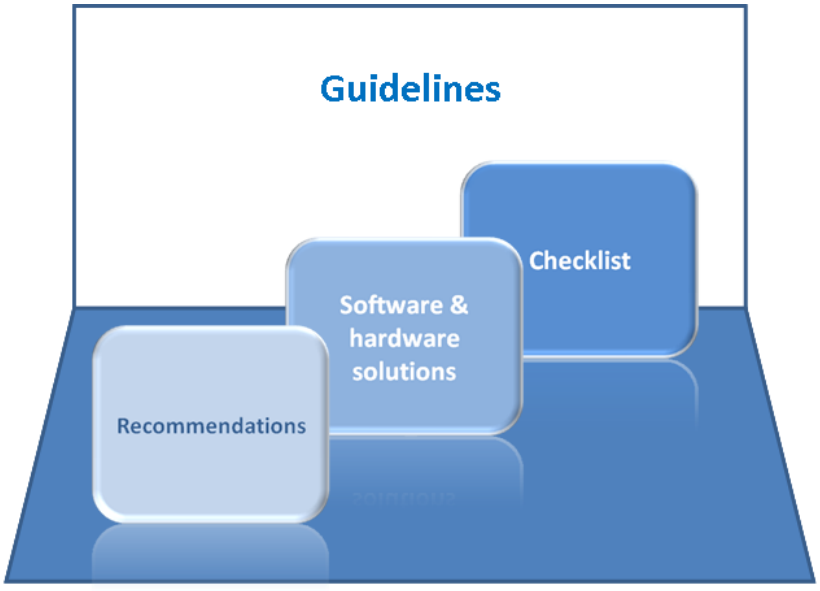
Guidelines for good practice

Our guidelines

Based on the data gathered and their analysis, this document provides good practice guidelines that can help readers and their organisations mitigate risks while dealing with USB security matters.

The good practice guidelines comprise of three components:

- ✓ recommendations;
- ✓ possible software and hardware solutions;
- ✓ a checklist.



Recommendations and possible software and hardware solutions

There are a number of recommendations and software and hardware solutions to ensure the secure use of USB flash drives.

- ✓ Implement a risk assessment methodology to ensure the correct controls to minimise risks throughout the lifecycle of the devices ([43]). A risk assessment will allow for understanding in detail the risks related to the use of USB flash drives and costs providing the basis to develop a strategy for closing these gaps ([44]);
- ✓ Implement security policies/guidelines around the use of USB drives and storing of corporate data on to a personal USB flash drive. Most measures are reactive, launched in response to a data loss incident. A recent survey shows that 67 % of organisations have implemented or are implementing policies as a result of a data or security breach in their organisation ([45]). Implement security policies before any data/security breach happens. Develop a company security policy which has every employee signing an agreement for not connecting their personal USB drive to the network and transport data. Eventually allow the use of corporate

([43]) Determine the appropriate level of ITAM controls for mobile assets, *Jack Heine, Gartner, 15 November 2005.*
([44]) *To read more on risk management/risk assessment methods and tools see* http://www.enisa.europa.eu/rmra/rm_ra_methods.html *and* http://www.enisa.europa.eu/rmra/rm_ra_tools.html
([45]) SanDisk Endpoint Security Survey, *SanDisk, April 2008.*

USB flash drives, specifying employee responsibilities and rules for safe use ([46]) and blocking devices that have no valid business use ([47]). Thus define what types of hardware are allowed to access the network.

Corporate policies should be comprehensive but not so restrictive as to impede employee productivity. This is why many large organisations choose to monitor and log access to sensitive files rather than block them outright ([48]). These rules will vary depending on the roles and responsibilities of each employee.

- ✓ Introduce a procedure to assess the loss and/or damage of a corporate asset, such as USB flash drive. Use forms to collect and analyse information from personnel involved as appropriate.
- ✓ Implement a centralised endpoint security policy through a dedicated solution. Deploying and managing portable storage devices across an organisation can be complex and expensive. A centralised management enables organisations to overcome these challenges by:
  - managing and eventually blocking ports — encryption and identity management software will not make USB drives 100 % secure. Monitor every port on every workstation and lock out unauthorised devices. Furthermore, it is also possible to audit port and record what devices are in use or be set to allow only specific devices, such as encrypted drive issued to particular employees ([49]);
  - looking for a system that allows tracking offline usage of USB flash drives — comparing mobile data files against the originals to determine if they have been opened, altered or copied to another device;
  - recovering user passwords centrally, using a challenge response mechanism;
  - managing the corporate USB flash drives centrally ;
  - demonstrating compliance with security standards;
  - protecting assets and brand by demonstrating that devices were encrypted at the time of loss or stolen with an extensive auditing;
- ✓ Audit and enforce policies: once policies are in place ensure that they are followed. The audits can range from the physical inspection of employee workstations (e.g. monitor the use of USB flash drive in your organisation eventually limiting the use of USB drives to company-authorised devices) to virtual audits using network-based applications that follow data as it moves though an organisation ([50]). Simply establishing corporate policies without any means of enforcing the rules or detecting violations is useless ([51]).
- ✓ Asset management: assess/identify all hardware and portable devices used to access the network. Eventually use software to identify every device that has ever been connected to the network. You will need this information to define your policies around the type of devices that can be used in the organisation, including USB flash drives, the employees who will allow using them and the type of protection required.
- ✓ Assess company's readiness for cases of loss of data if USB flash drives are lost or stolen.

([46]) Toolkit sample template: a sample employee agreement for the use of personal digital devices, *Jay Heiser, Gartner, 1 February 2008. SANS proposes a sample of a policy which control the use of mobile computing and storage devices, including flash drive. The policy sample is available at* http://www.sans.org/resources/policies/Remote_Access.doc *(last visited on 30 May 2008).*

([47]) Getting started with McAfee host data loss prevention, *McAfeee, 2008.*

([48]) *'Data-leak security proves to be too hard to use', Infoworld.com, available at* http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html *(last visited on 2 June 2008).*

([49]) *'Closed doors policy', Daniel Tynan,* FedTech Magazine, *August 2007, available at* http://fedtechmagazine.com/article.asp?item_id=352 *(last visited on 30 May 2008); 'Thumb drives are too often the victims of convenience', John Zyskowski,* GCN, *14 December 2006, available at* http://www.gcn.com/online/vol1_no1/44136-1.html *(last visited on 30 May 2008);* USB flash drive protection, *Ron LaPedis, SanDisk, Disk Encryption Forum, 13 February 2007.*

([50]) *'Closed doors policy', Daniel Tynan,* FedTech Magazine, *August 2007, available at* http://fedtechmagazine.com/article.asp?item_id=352 *(last visited on 30 May 2008).*

([51]) Plugging the leaks: best practices in endpoint security, *SanDisk, 2008.*

Assessment

- *Do you know the sensitivity classification scheme applied to content?*
- *Do you know what sensitive business information and core Information assets to protect?*
- *Do you know the users/business units who can access that information, how and with what frequency?*
- *Do you know who can use USB flash drive to copy and transport information? Moreover, do you know the employees who received a corporate USB drive?*
- *Do you have written security policies or guidelines which cover the use of USB flash drives?*
- *Do you educate users and how frequently?*
- *Do you backup information residing on USB flash drives?*
- *Do you have the support of key stakeholders?*

- ✓ Limit access: limit the access to certain types and amount of sensitive data to certain employees. In a more complex organisation, establish data usage rules specifying the personnel who can be authorised to get access to sensitive data files, what kind of data files can be portable and how they should be treated. Look for software that can automate this process by scanning files on network drives and client machines, checking for key words ([52]).
- ✓ Attach USB drives to key chains/lanyards to avoid loss of media: the reduced size of USB flash drives makes these devices easier to lose or be stolen and higher storage capacity increases the potential amount of data at risk for unauthorised access.
- ✓ Invite users to put the USB flash drive in read-only mode to avoid virus transmission: some USB flash drives include a physical switch to put the drive in a read-only mode to avoid the host computer from writing or modifying the data on the drive.
- ✓ Scan USB flash drive after copying files from an untrusted machine to avoid virus transmission.
- ✓ Require users to authenticate: prevent unauthorised access to data with a mechanism that requires users to authenticate using a password and/or fingerprint. Set a maximum number of password or biometric authentication retries to counter attacks.
- ✓ Use of encryption, performed either by software or hardware means, whereby data is altered in order to make it inaccessible without proper key to decrypt the data ([53]). In this way data will be useless without the required key and will remain always secure wherever it travels. A solution is to require sensitive data to be stored only on encrypted storage devices such as enterprises-grade USB flash drives with mandatory password protection for all files. Another solution, which is widely acknowledged as one of the best, is to use hardware-based encrypted devices which perform the encryption on-board inside the USB flash drive. The major advantage of hardware-based encryption keys is that they never leave the USB flash

([52]) Plugging the leaks: best practices in endpoint security, *SanDisk, 2008.*

([53]) Use the three laws of encryption to properly protect data, *Rich Mogull, Gartner, 24 August 2005; 'Thumb drives are too often the victims of convenience', John Zyskowski,* GCN, *14 December 2006, available at* http://www.gcn.com/online/vol1_no1/44136-1.html *(last visited on 30 May 2008);* Seven steps to secure USB drives, *SanDisk, July 2007* and Assessing the security of hardware-based vs. software-based encryption on USB flash drive, *SanDisk, May 2008.*

drives, are not susceptible to any outside attacks and virtually don't cause performance loss ([54]). Finally, encryption is a powerful security technology but is a tool which can be used. It should be used when data moves and access controls rights are not specific enough ([55]). Evaluate third-party data encryption tools with appropriate defences for all high-risk systems, those that contain sensitive data or are likely to be stolen and use for corporate espionage ([56]).

- ✓ Protect your infrastructure from malicious codes: use of antivirus protection to ([57]):
  - stop viruses: block, clean and remove viruses and trojans from USB flash drive;
  - protect PCs: prevent your USB flash drive from acting as a carrier of viruses that can be transmitted when you plug into a PC.
- ✓ Backup information: be able to recover data residing on USB flash drives.
- ✓ Train your workforce: train employees on policies around technology usage to make them aware of the risk involved with storing and transporting corporate data on USB flash drives; explain how to avoid data leaks and remind them to report those that happen. Keep them informed of possible changes in policies and ensure they follow guidelines in their daily work. User education, awareness and acceptance are critical for the success of any security policy or implemented technical solution.
- ✓ Run a survey to check if users are familiar with their organisation's policies regarding USB flash drive usage.
- ✓ Start at the top: start with senior management and personnel who travel with sensitive data before moving on to the rest of the organisation. The best defence against data leaks is an educated workforce.
- ✓ Collect feedback to further fine-tune enforced solutions and policies for maximum accuracy and understand the patterns that increase the risk of data loss.

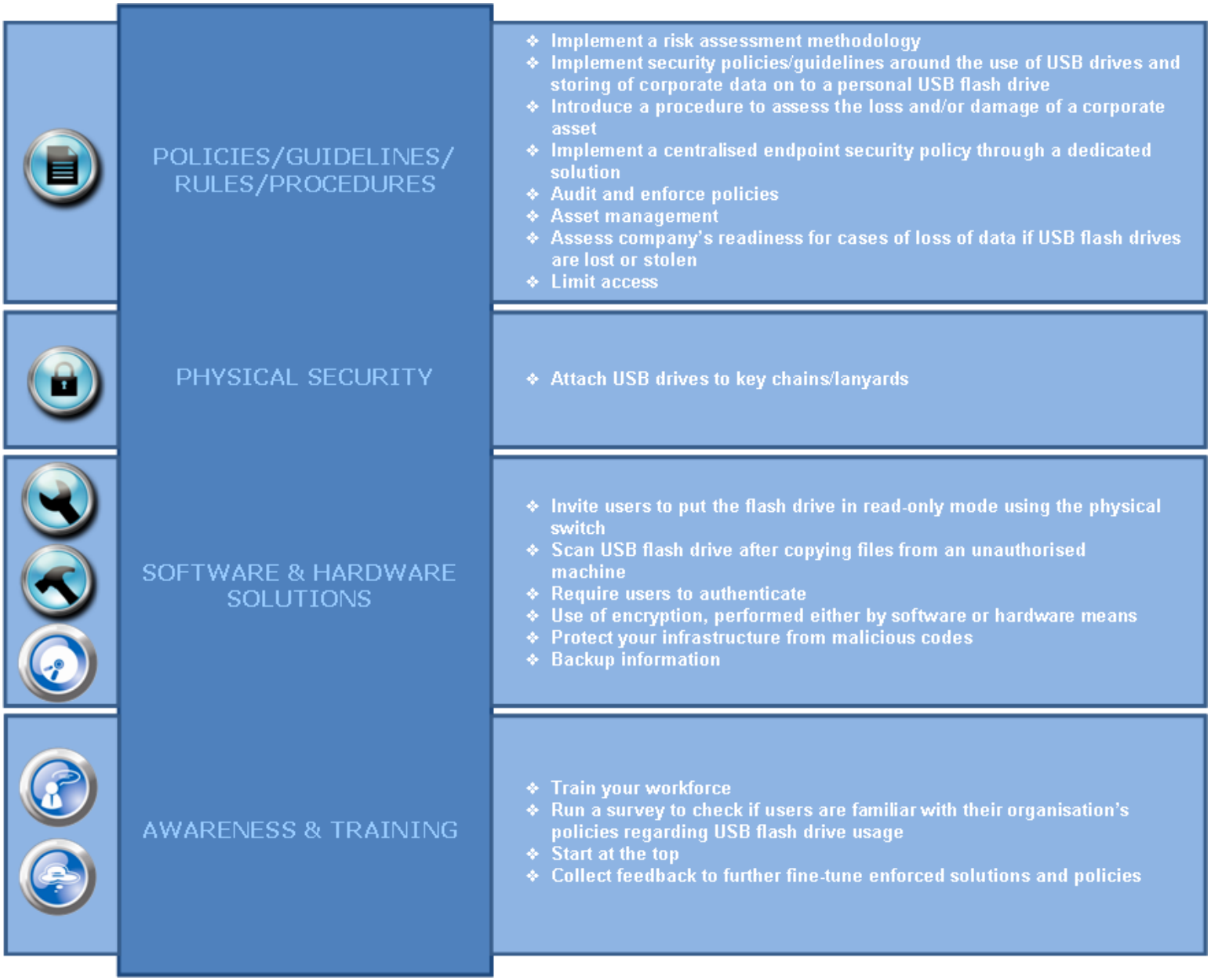
The table below summarises the recommendations and software and hardware solutions described above:

([54]) Assessing the security of hardware-based vs. software-based encryption on USB flash drive, *SanDisk, May 2008.*

([55]) Use the three laws of encryption to properly protect data, *Rich Mogull, Gartner, 24 August 2005 and* Prepare for DRAM threat to encrypted data storage, *John Girard, Ray Wagner, Eric Ouellet, Gartner, 25 February 2008.*

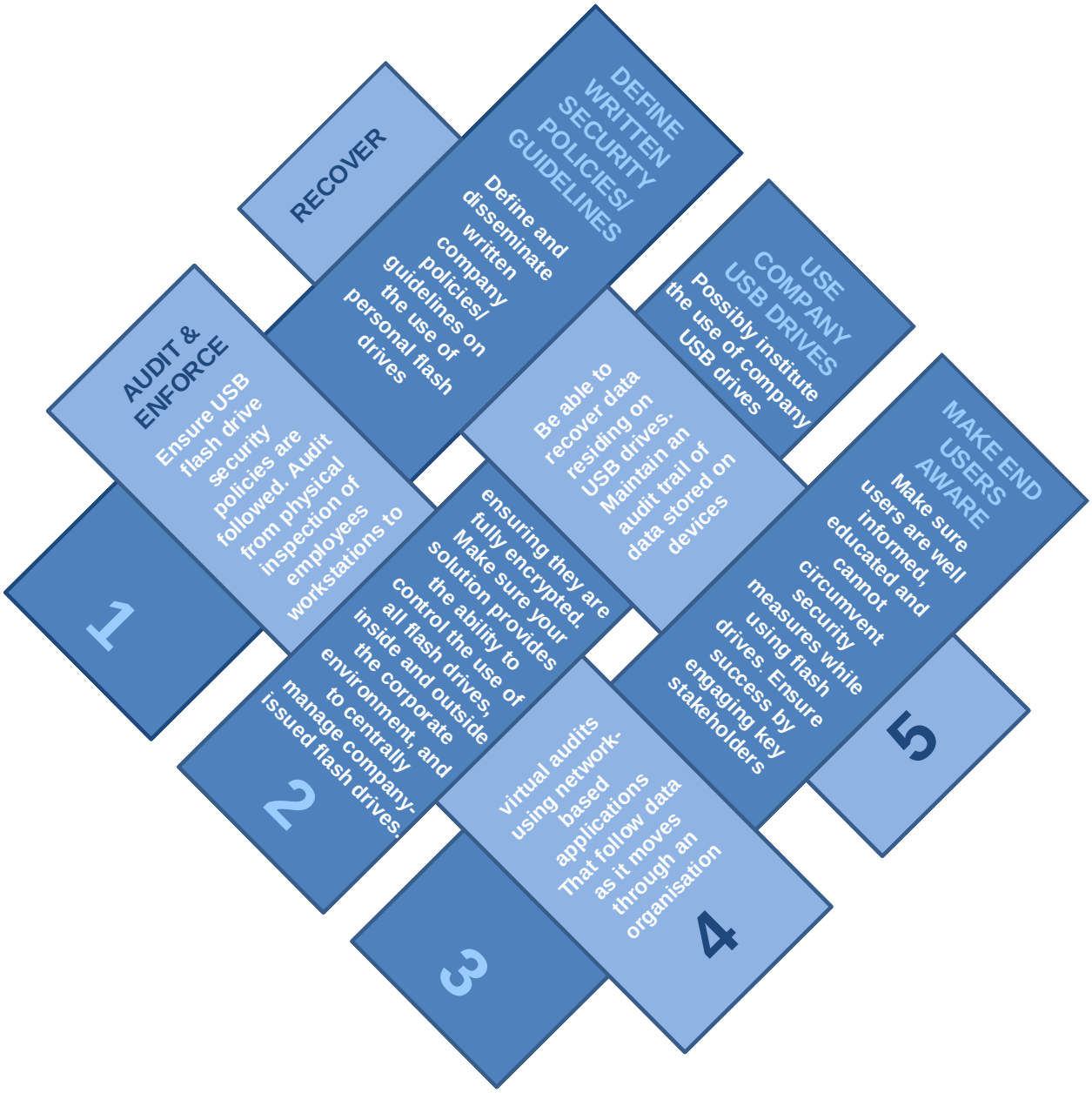
([56]) *Cyber espionage now ranks third on the SANS Institute's list of the top 10 cyber menaces for 2008. For more details see* Top 10 cyber menaces for 2008, *SANS Institute, available at http://www.sans.org/2008menaces/ (lat visited on 2 June 2008).*

([57]) McAfee®VirusScan® USB — proven security that protects your USB drive against viruses, *McAfee, 2006, available at http://download.mcafee.com/products/manuals/en-us/vsusb_datasheet_2007.pdf (last visited on 30 May 2008).*


POLICIES/GUIDELINES/ RULES/PROCEDURES
Implement a risk assessment methodology
Implement security policies/guidelines around the use of USB drives and storing of corporate data on to a personal USB flash drive
Introduce a procedure to assess the loss and/or damage of a corporate asset
Implement a centralised endpoint security policy through a dedicated solution
Audit and enforce policies
Asset management
Assess company's readiness for cases of loss of data if USB flash drives are lost or stolen
Limit access
PHYSICAL SECURITY
Attach USB drives to key chains/lanyards
SOFTWARE & HARDWARE SOLUTIONS
Invite users to put the flash drive in read-only mode using the physical switch
Scan USB flash drive after copying files from an unauthorised machine
Require users to authenticate
Use of encryption, performed either by software or hardware means
Protect your infrastructure from malicious codes
Backup information
AWARENESS & TRAINING
Train your workforce
Run a survey to check if users are familiar with their organisation's policies regarding USB flash drive usage
Start at the top
Collect feedback to further fine-tune enforced solutions and policies

Checklist

Checklist items can be used as guidance for the main steps to undertake when running any activity related to the secure usage of USB flash drives by an organisation. Once the enterprise has recognised the importance of protecting corporate data and classifies the data, the following main steps should be followed:



PART 3:

Safety tips and corporate benefits

Practical tips to prevent USB flash drive theft

Practical tips

- *Ensure employees report cases of lost of stolen USB flash drives to the IT department*
- *Conduct a damage assessment for every USB flash drive that goes missing*
- *Establish how and where they went missing*
- *Review your policies/guidelines to ensure major sources of loss are covered*
- *Highlight potential risks associated with the innocent use of USB flash drives by employees and for other less legitimate purposes such as smuggling information out of the company*
- *Take special measures for business units/departments which are handling sensitive data*
- *Monitor and report incidents on a regular basis*
- *Train and send out reminders to employees*
- *Benchmark your performance against other similar enterprises*
- *Collect feedback to further fine-tune the enforced solutions and policies for maximum accuracy and understand the patterns that increase the risk of data loss*

Benefits

An overview of the many benefits linked to a secure use of USB flash drives will help and lead the enterprises to better decide about this matter. The following benefits were identified.

- ✓ Enhance and boost employee productivity through mobility and remote connectivity.
- ✓ Flexible and secure solutions will:
  - protect corporate assets,
  - reduce total cost of ownership,
  - prove that devices were encrypted when stolen or lost.
- ✓ Defend enterprises from data leakage.
- ✓ Enforce mandatory company-wide security policies.
- ✓ Sanitise any PC, anywhere. Allow connection to PC by authorised devices.
- ✓ Extend security policy beyond the perimeter:
  - track all activity on USB flash drives.
- ✓ Comply with the three pillars or classifications of information security — confidentiality, availability and integrity — and security standards.

Conclusions

In today's organisations, sensitive data is stored and accessed on a variety of mobile devices, including USB flash drives. The storage capacity, size, low price and plug-and-play functionality are some of the reasons why their use has increased enormously. USB flash drives are often handling corporate information, such as financial information, forms, employee documents and customer data. These mobile devices remain largely unprotected and uncontrolled by IT departments, leaving business susceptible to consequences which may be devastating such as lost reputation, jobs and profits.

Loss of company information is the result of employee ignorance about the risks associated with the use of USB flash drives or their willingness to skirt policies in order to work more productively. Thus most of the actions are not intentional or malicious but accidental and unintended.

Although there is increasing awareness of the risks and costs related to the insecure usage of USB flash drives, there is still a significant amount of work to do. It is therefore crucial that IT asset managers prepare themselves and their organisations to regulate, manage and audit the use of USB flash drives as ensuring the ability to secure information on the network and the opportunity to manage data which enter and leave the company environment is key for any organisation regardless of its size and maturity.

With the increased number of portable devices used in business, with employees travelling and taking work home, a secure use of USB flash drives and awareness of the related risks should be an integral part of the organisation's overall security strategy.

ENISA hopes this paper will provide enterprises with a valuable tool to overcome obstacles within their organisations.

References and sources for further reading

A users' guide: how to raise information security awareness, *ENISA, June 2006*.

'Afghan market sells US military flash drives', Paul Watson, Los Angeles Times*, 18 April 2006, available at http://www.veteransforcommonsense.org/ArticleID/7120 (last visited on 28 May 2008).*

'Analysis of USB flash drives in a virtual environment', Derek Bem and Ewa Huebner, Small Scale Digital Device Forensics Journal*, Vol. 1, No 1, June 2007.*

'Another laptop stolen from Pfizer, employee information compromised', Lee Howard, 12 May 2008, available at http://attrition.org/dataloss/2008/05/pfizer01.html (last visited on 30 May 2008).

'Closed doors policy', Daniel Tynan, FedTech Magazine*, August 2007, available at http://fedtechmagazine.com/article.asp?item_id=352 (last visited on 30 May 2008).*

'*Data breaches are "everyday incidents"', Matt Chapman, vnunet.com, 15 Nov 2007, available at http://www.vnunet.com/vnunet/news/2203540/security-breaches-everyday (last visited on 30 May 2008).*

'*Data-leak security proves to be too hard to use', Infoworld.com, available at http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (last visited on 2 June 2008).*

Dataquest insight: USB flash drive market trends, worldwide, 2001–2010*, Joseph Unsworth, Gartner, 20 November 2006.*

DataTraveler for Enterprise*, Kingston, 2008, available at http://www.kingston.com/flash/DataTravelers_enterprise.asp (last visited on 30 May 2008).*

DataTraveler Secure *and* DataTraveler Secure — Privacy Edition White Paper*, Kingston Technology, Rev. 2.0, June 2007.*

Determine the appropriate level of ITAM controls for mobile assets*, Jack Heine, Gartner, 15 November 2005.*

'Disc listing foreign criminals lost for year', The Times*, 20 February 2008*.

Educational security incidents (ESI) — Sometimes the free flow of information is unintentional*, available at http://www.adamdodge.com/esi/month/2008/01*

Forecast: USB flash drives, worldwide, 2001–2011, Joseph Unsworth, *Gartner, 24 September 2007.*

Getting started with McAfee host data loss prevention*, McAfee, 2008.*

Magic quadrant for mobile data protection, 2007*, John Girard, Ray Wagner, Gartner.*

McAfee Encrypted USB — data sheet*, McAfee.*

McAfee® VirusScan® USB — proven security that protects your USB drive against viruses*, McAfee, 2006, available at http://download.mcafee.com/products/manuals/en-us/vsusb_datasheet_2007.pdf (last visited on 30 May 2008).*

New attacks: device vulnerabilities stand out, *Avivah Litan, Don Dixon, Greg Young, Gartner, 21 June 2005.*

'New report chronicles the cost of data leaks', Physorg.com, 2007, available at http://www.physorg.com/news96708147.html (last visited on 2 June 2008).

Plugging the leaks: best practices in endpoint security, *SanDisk, 2008.*

Prepare for DRAM threat to encrypted data storage, *John Girard, Ray Wagner, Eric Ouellet, Gartner, 25 February 2008.*

'Prince of Wales Hospital announced an incident of loss of USB flash drive containing hospital files', press releases, 6 May 2008, available at http://www.info.gov.hk/gia/general/200805/06/P200805060232.htm (last visited on 30 May 2008).

Privacy and identity theft', Dave Jevans, IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008).

Plugging the leaks: best practices in endpoint security, *SanDisk, 2008.*

SanDisk Endpoint Security Survey, *SanDisk, April 2008.*

Seven steps to secure USB drives, *SanDisk, July 2007.*

'Small drives cause big problems', Jon Swartz , USA Today, *16 August 2006, available at http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm (last visited on 27 May 2008).*

'Spring students' info at risk after laptop theft', KHOU.com staff report, 16 May 2008, available at http://attrition.org/dataloss/2008/05/spring01.html (last visited on 30 May 2008).

Survey of US IT practitioners reveals data security policies not enforced, *Ponemon Institute and RedCannon Security, December 2007, available at http://www.ponemon.org/press/RC_PonemonSurvey_FINAL.pdf (last visited 2 June 2008).*

'TAMU Corpus Christi prof loses flash drive with 8 000 student records', Paul McCloskey, Campus Technology, *18 August 2007, available at http://campustechnology.com/articles/48635 (last visited on 30 May 2008).*

The portable risk of high capacity USB drives, *Allan Leinwand, GigaOM, 5 December 2007, available at http://gigaom.com/2007/12/05/the-portable-risk-of-high-capacity-usb-drives/ (last visited on 30 May 2008).*

'Thumb drives are too often the victims of convenience', John Zyskowski, GCN, *14 December 2006, available at http://www.gcn.com/online/vol1_no1/44136-1.html (last visited on 30 May 2008).*

Timetable of missing data blunders', The Times, *20 February 2008.*

Toolkit sample template: a sample employee agreement for the use of personal digital devices, *Jay Heiser, Gartner, 1 February 2008.*

Top 10 Cyber menaces for 2008, *SANS Institute, available at http://www.sans.org/2008menaces/ (last visited on 2 June 2008).*

Understanding data leakage, Jay Heiser, *Gartner, 21 August 2007.*

'US military secrets for sale at Afghanistan bazaar', Watson, Los Angeles Times*, 10 April 2006.*

USB flash drive market trends, Worldwide, 2001–2010*, Joseph Unsworth, Gartner, November 2006.*

USB flash drive protection*, Ron LaPedis, SanDisk, Disk Encryption Forum, 13 February 2007.*

Use the three laws of encryption to properly protect data, Rich Mogull, *Gartner, 24 August 2005.*

http://www.enisa.europa.eu/rmra/rm_ra_methods.html

http://www.enisa.europa.eu/rmra/rm_ra_tools.html

Assessing the security of hardware-based vs. software-based encryption on USB flash drive*, SanDisk, May 2008.*

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu