Global Information Assurance Certification Paper

Chief Security Officer Challenges: USB Drives, Portable Storage Devices and Physical Security

Paul-Michael Ferguson
GIAC Security Essentials Certification (GSEC)
Practical Assignment, Version 1.4b, Option 1
Submitted 24 August 2004

Abstract

The Chief Security Officer (CSO) faces the challenge of constantly changing and adapting the security posture and readiness of the enterprise as new technology becomes available. Miniaturization and functional integration of electronic devices continue to pose new concerns in protecting the digital environment. Although recent focus has emphasized the risks posed by USB drives, administrators should also be aware that many other products exist on the market that easily serve clandestine purposes. This paper suggests a holistic approach to combating risks associated with the introduction of these new technologies in the workplace. It also provides a characterization of the threat, recommendations for minimizing risks and an update on products currently available which have security implications.

> *Security managers and CIOs are well aware of the threat posed by insiders, but often find it easier technically and politically to take action against external threats instead. Businesses must take steps to secure themselves against criminally intent insiders or resign themselves to suffering significant losses from insider crimes.* – Victor Wheatman, managing vice president for Gartner.[1]

Senior executives are pressing the CSO[2] to develop and publish policies that address the hottest product in every office worker's hands: the Universal Serial Bus (USB) drive, flash drive or "thumb drive" as is the current vernacular. These executives have become self-professed

[1] "Gartner Says 60 Percent of Security Breach Incident Costs Incurred by Businesses Will Be Financially or Politically Motivated." 29 May 2003. URL: http://www3.gartner.com/5_about/press_releases/pr29may2003a.jsp# (6 June 2004).

[2] *The Chief Security Officer (CSO) the newest C-level executive making their way into the executive suite. CSO's form an organization's security policy, implement it and enforce it. But whether they are called CSO's, CISO's (Chief Information Security Officers) or another top-level title, these are the executives who are charged with protecting their organization's tangible and intangible assets, and are faced with the growing challenge of balancing the correct levels of risk versus business opportunity.* URL: http://www.csoonline.com.au/index.php/aid;4 (6 June 2004).

experts on the subject after having seen headlines like "USB Flash Drives: Useful Device or Security Threat?"[3] and "USB Pen Drive + Real Pen = Real Threat (Do the Math)."[4]

When requested to put into words the actual threat posed by USB drives, the executives' typical response is that these devices are small, easy to use, and can download and store tremendous amounts of data[5] in just a few seconds with the latest 2GB device. The CSO usually provides a supportive smile and a nod while thinking its better not to point out to the boss that he just described exactly what the device was designed to do. However the CSO also knows that, like any other good tool, there exists the capacity for misuse and smartly replies to the boss with a short answer to that effect.

Taking a conservative and politically "safe" posture, some CSO's are banning these "flash drives" from their organization until their peers in other organizations create standard policies for their use – the same approach many took with the adoption of wireless technologies. However, banning the use of USB drives is difficult since many CSO's personally depend on them for their own daily needs. They are happy to find that it is no longer necessary to carry bulky CD-R's, floppy disks or ZIP disks for downloading and transporting large documents or presentations. Nor is it necessary to install software or drivers to allow these technologies to work. The USB drive has much higher capacity than other removable media[6] and is "plug and play" in Microsoft Windows 98 and above operating systems. On the other hand, this flexibility of use and strength in capabilities must be weighed against some of the risks involved with using these devices. Many people use USB drives to carry most of their important files that may be company proprietary and very sensitive information. Although worker productivity increases by having critical files handy at all time, it is also very easy to leave the drives attached to a computer, for them to fall out of pockets, or for them to be outright stolen. They may also be used clandestinely to quickly[7] copy and aggregate information not normally provided to users. These myriad capabilities and the risks associated with them are now also embedded in a variety of shapes and sizes beyond the typical USB drive.[8]

Rather than taking the time addressing the use of every new device by promulgating directives prohibiting them, there is a more efficient and effective approach. Following these few principles can make the adoption of new technologies much easier and change the role of the CSO from Cyber-Nazi to Cyber-Hero: 1) Keep a database of new technology devices, 2) Have a thorough understanding of the risk introduced by these devices and 3) Take actions to mitigate risk posed by identified threats.

New Technologies

- ***What is a USB drive?***

[3] "USB Flash Drives: Useful Device or Security Threat?" 10 December 2003. URL: http://labmice.techtarget.com/articles/usbflashdrives.htm (6 June 2004).
[4] Black, Jeff. "USB Pen Drive + Real Pen = Real Threat (Do the Math)." 21 March 2004. URL: http://www.empiresecurity.com/displayarticle215.html (6 June 2004).
[5] 76923 pages in MS Word based on the average of size of one page being 26k. Pure text files can be as small as 3.9k a page which translates to approximately 512820 pages. Additionally, 40000, 5714, and 2000 image files at medium (50k), high (350k), and very high (1MB) resolutions respectively.
[6] Floppy disks have a maximum capacity of 1.44MB, ZIP disks 750MB, and CD-R's 800MB. DVD-R's support up to 4.7GB, but is not standard yet on all new systems and they are still larger and slower than USB drives.
[7] Most new computers support USB 2.0 which has data transfer speeds of 480 Mbits/sec.
[8] For example wristwatch USB devices and fountain pen USB devices. See 'Hot Products' section for more details.

Almost all computers have had Universal Serial Bus (USB) connection capabilities since 1998. Both Macintosh and Windows operating systems can use USB and now most Linux and Unix versions also provide native support. USB technology was designed to allow "plug and play" capabilities making it easy for employees to attach devices to a computer and begin using them right away without complicated installation procedures or privileged access to the computer. In 2001, the USB 2.0 specification was finalized which increased the data transfer speed from 12Mbps to 480 Mbps. USB drives today employ USB 2.0 technology and are small, handheld electronic storage devices that allow users to attach them to a computer to use it like a hard disk drive. At the core of the USB drive is a non-volatile flash memory chip that works similar to RAM chips in computers, but data stays resident on the chip without any power feeding it. An employee can read, write, delete, and rewrite files to the device and then conveniently take it with them. Most implement a hardware switch for write-protect capabilities. Many vendors are responding to demands to better secure the data on USB drives by implementing encryption and password protection capabilities on the device. Some even include biometric identification requirements to access data on the chip.[9]

It's important to note that flash memory chips available on the market do not only use USB interfaces; they can also operate on standard computer interfaces like IEEE 1394 (Firewire), PCMCIA and others.[10] These standards have similar plug and play capabilities and have even greater data transfer capabilities:

- FireWire 1394a – 400 Mbps
- FireWire 1394b – 800 Mbps (copper)
- FireWire 1394b – 1600 Mbps (fiber)
- PCMCIA CardBus – 1000 Mbps

Flash memory chips can be adapted to use almost any input/output port on a computer existing today and new proprietary methods are being developed all the time. Although the most popular form today is in the recognizable USB drive, flash memory chips are being embedded in many more non-descript ways. For example, manufacturers are adapting their use in cellular phones, cameras, camcorders, Personal Digital Assistants, two-way email devices, watches, and even ballpoint pens! Some of these implementations include CompactFlash®, CF+, Sony Memory Sticks, and Panasonic SD Memory Cards. Data on storage media of this type is usually downloaded or synchronized onto a computer by directly connecting the camera or music player. However, data transfer can also move from the computer to the device, making it possible to transfer company files to a portable music player, which might not be an authorized transaction. Even if this type of transaction is authorized, these devices do not provide data security functionality like many USB drives do.

- ***Relative importance of USB drives***

Taking into consideration flash memory can come in many different sizes and shapes, be embedded in items not normally thought to be used for computer data storage, as well as have any one of a wide selection of computer interfaces, the USB drive form factor may not seem to be as much of a risk as dealing with the multitude of other flash memory implementations. The CSO may be accustomed to seeing the typical USB drive in the workplace and authorize them for use, but he or she may not be checking pens and watches to see if they have data storage capabilities also. It's not easy keeping up with every mitigation technique against new consumer

[9] See Thumbdrive Touch at http://www.thumbdrive.com/prd_info.htm.
[10] For an extensive list of computer interfaces and specifications, see http://www.techfest.com/hardware/bus.htm.

technologies that are being introduced everyday. The CSO is kept busy dealing with traditional network and system security issues such as viruses, intrusion attempts and other hacking activities. As an executive in the company, these mitigation activities must be quantified and investments in protection technologies must be analyzed and evaluated for return on investment. With all these high priority activities going on, there just isn't enough time to research every new product as it gets released and provide a thorough analysis of its impact to the organization.

With a full plate just maintaining perimeter defense and fighting the latest worm or distributed denial of service (DDOS), it's hard to see the importance of taking time to address USB drives. According to TheInfoPro/Secure Computing Corp., only 10% of security managers surveyed views USB flash memory cards as a "major problem" and a potential security risk.[11] However, being busy and ignorance of the risk factors are not excuses for ignoring how usage of these devices increases risk to the organization. For example, viruses normally enter the organization through attachments in e-mail. However, USB drives can be used to hand carry viruses past all the normal electronic defenses and inject them into the network without any virus check. Additionally, a marketing executive developing the latest advertising campaign could drop the device while attending an industry conference with many competitors present. How much could the loss of this data and/or theft of this data by a competitor be to the organization? CSO's must take a proactive stance in integrating these new technologies into the corporate environment.

- ***Keeping track of the latest gadgets***

A prudent CSO never lets any new technologies get past him and finds ways to stay ahead of the game. A CSO should start by developing an information security knowledge repository (typically a database of products and lessons learned that is accessible and searchable through a web interface) and creating a special area for documenting new products and their specifications.

Development of this knowledge repository must recover the costs of implementation, so starting small is a good idea. The basic formula for ROI is **RETURN = BENEFIT ÷ COST OF IMPLEMENTATION**. To enhance the defining of benefits, focus first on the technical access and privileges that employees have for company proprietary information and the costs associated with destruction or theft. Second, focus on how implementing certain devices through an acceptable use policy can enhance worker satisfaction and productivity.

There are a few good places on the Internet to start collecting data on new data storage technologies. These sites seek out new devices and upgrades to existing ones at tech exchanges, conventions and foreign release venues in Japan and around the world. Below are a few sites that can help provide a baseline of devices to document:

- Future Technology News (http://www.i4u.com/)
- Think Geek (http://www.thinkgeek.com)
- I Want One of Those (http://www.iwantoneofthose.com)
- Gadget Universe (http://www.gadgetuniverse.com)
- Computer Geeks (http://www.compgeeks.com)
- Tiger Direct (http://www.tigerdirect.com/)

System administrators and network technicians also are die-hard techies at heart and love to have the latest and greatest toys. Have them add value to your knowledge repository by validating the baseline entries, adding comments based on their personal experiences with

[11] TheInfoPro/Secure Computing Corp. "Flash Risk." Information Security. April 2004.

devices in the database, and updating the store with any new devices they know about that may not already be in there. Additionally, the capability to update entries might be opened up to those in the general workforce that register and demonstrate a requisite level of technical knowledge.

As the database grows, common specifications among all of the devices will allow for quick searching to produce different classes of devices. For example, a search for flash memory and USB could produce a list that contains the USB drive, a watch with retractable mini-USB interface, and a pen that doubles as a USB drive. Finding any vulnerabilities associated with any one of those devices may indicate a need to check the others for the same type of vulnerability.

Defining "Threat" to Better Understand Risk

- ***Risk = Threat x Vulnerability***

Up to this point, the words threat, vulnerability and risk have been used liberally and somewhat interchangeably. But as a professional whose assessment of risk versus capability can have significant impact on the bottom line of the enterprise, distinctions should be clearly made here. Bad product choices can waste large sums of money, but failures in risk assessment can also manifest itself in less tangible ways such as a loss of confidence, customer trust, branding credibility and/or stock fluctuation, which usually end up having even greater effects on the bottom line.

According to Princeton's lexical database of the English language, the word "threat" means something that is a capable source of danger. It is also a declaration of an intention or a determination to inflict harm.[12] One thing to remember is that a "source of danger" and "intent to inflict harm" must be directed against something that is deemed valuable or the threat is of negligible consequences.

Given this definition of the word threat, USB drives do not fall neatly within this characterization. The device itself does not present a source of danger in and of itself, or it would not be allowed to make it to market. The USB drive's contribution to overall risk is not that it is a specific threat, rather it may be used as a threat vector. Viruses or malicious software might be brought into the enterprise via a USB drive, but there is no intention within the device itself to actually cause any harm. Regarding the loss of valuable company data such as customer data or R&D information in clinical trials, the device again does not try to lose itself or promote itself as a device to steal, but there is a human factor here that must be evaluated since safety protocols are not usually implemented when using a USB drive.

Malaria is definitely a source of danger to human health and when introduced in the bloodstream, it operates with the intent to inflict harm. However, the mosquito is merely a carrier of the threat. Not until a threat is combined with a threat vector, or vulnerability, can we truly assess risk against valuable assets. Common among security professionals is a theoretical formula for assessing risk expectations to the organization: **RISK = THREAT x VULNERABILITY**.

- ***Will the real threat please stand up?***

If USB drives and the multitude of devices and gadgets like it are merely vectors of threats, then what is the actual threat? In this case, the sources of the threat are the users of these

[12] WordNet 2.0 Search: Threat. URL: http://www.cogsci.princeton.edu/cgi-bin/webwn?stage=1&word=threat (12 June 2004).

devices. They are regular full-time employees of the enterprise and contractors who are temporarily allowed in the office spaces to provide professional outsourcing or even nighttime cleaning crews.

Misuse of these devices can be unintentional, such as loss of valuable data from loss of the device itself. The worst situation is when this data gets into the wrong hands and is used in a manner that is detrimental to the organization both financially and reputationally. Protection of data must be commensurate with the value that the data represents. Another unintentional misuse is bringing in a virus to the office from home. USB devices connect to computers and create a drive for files to be transferred to and from, but this connection does not trigger an automatic scan for viruses on the drive. A user can pass a virus-laden file from the USB drive to the corporate server without incident and multiple people could access the file from the server to activate and spread the virus.

Misuse of these devices can also be intentional, such as with corporate espionage and theft of proprietary data by the authorized visitor. Being small and quick in data transfer capabilities is not the fault of the device, but those features can be used to conceal the device and make the theft that much easier. Also, a disgruntled worker could be the instigator and do more damage with his or her intimate knowledge of the operations by placing malicious files in specific shared areas of high use.

Try to get a picture of what the measure of insider threat may actually be in a typical organization. The nature of most people is to be trusting of coworkers, therefore initial assumptions may be that the measure of threat is relatively low. However, over the past eleven years there has been a national study on insider crime in the United States. Every year a report is published analyzing the threat and its components. In this study, calculating inventory shrinkage due to employee theft produced the measure of insider threat. According to the 2002 National Retail Security Survey, loss due to employee theft was measured at 48.5%. This is actually an increasing metric, because the previous two years reported 45.9% and 44.5% respectively.[13]

Mitigating the Risk

- ***Risk reduction through vulnerability reduction***

According to a RAND-led study of insider misuse,[14] threats incorporate elements of motivation, opportunity, vulnerability, and skill to exploit. In this case, the device presents the vulnerability. The measure of vulnerability can vary based on protection measure employed such as password protection, file encryption, or biometric access requirements. The other threat elements can be matched with value of the data to determine a high, medium, or low threat. The below table is a model that adapts these threat elements to specific exploits:

[13] Hollinger Ph.D., Richard C. National Retail Security Survey. November 2002. URL: http://retailindustry.about.com/library/weekly/02/aa021126a.htm and http://web.soc.ufl.edu/SRP/NRSS_2001.pdf

[14] "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems." 19 October 1999. URL: http://www.csl.sri.com/users/neumann/insider-misuse/ins.pdf.

	Destruction / Interruption of Corporate Network Services	Theft of Corporate Data on Company Premises	Loss or Theft of USB Device	
Motivation				
Opportunity				
Vulnerability				
Skill				**Overall Risk**
Total Risk				

Assuming that banning all new technologies is out of the question, especially since the malicious individual will just ignore the directive, it will be prudent to address the issue head on and start with applying general usage policies. As technologies mature, and where necessary, specific procedures can be implemented to further reduce risk. The Defense Information Systems Agency (DISA) published a white paper last year discussing how to secure data on USB drives using Microsoft Windows operating systems.[15] Specific recommendations included changing the file system on the USB drive to NTFS to enable ACL permissions; physically protecting the USB devices as they are easily stolen; and disabling unused USB ports on computers since unauthorized personnel could connect, copy sensitive files, and disconnect very quickly. However, since the recommendation to disable USB ports fell under the physical security section of the report, two key items may be noted. First, that any vulnerability related to usage of USB drives is predicated on physical access to a machine. However, there is a common security mantra stating "if someone has physical access to the box, they own the box." Therefore the second item is that when physical access is involved, the threat is really the user, not the technology that is being used.

Since our discussion in the previous section showed the greatest sources of threat were insiders, specific recommendations can be made to address this issue and thereby have the greatest impact on risk reduction.

- ***Risk reduction through threat reduction***

There are three stages during the lifecycle of employment that the risk from insider threat can be mitigated. 1) During the hiring process, 2) Throughout their employment, and 3) Actions taken upon separation.

Many hiring managers do not take it upon themselves to follow due diligence when hiring new personnel, especially in the IT sector where critical skills are in high demand. Initial integrity screening tools should include many of the following: verification of past employment history, personal reference checks, staged or multiple interviews, criminal conviction checks, credit checks, drug screening, driving history checks, education verification, and personality

[15] "Security for Hard State USB Mobile Disk Devices on Windows 2000/2003/XP." DISA Field Security Operations. 12 June 2003.

questionnaires. Once hired, they should undergo a trial period of possibly 90 days and sign acknowledgement statements having agreed to existing policies of the enterprise.

Throughout the period of regular employment, user awareness and education is required. As technologies develop and new vulnerabilities arise, make the user population aware of their existence, the policy of the enterprise towards use of the new technologies, and what they are obligated to do if they witness misuse of a new or any technology. The emphasis should not be on what cannot be done, rather it should be on how it can be done and delivery of clear procedures for doing it according to policy.

Lastly, when there is a violation of policy, especially if it was malicious and intentional, swift and strict measures must be taken. All instances must be copiously documented and counseling must occur right away. If there is enough evidence and due cause, then firing of the employee is recommended. Do not make the employee someone else's problem with a lateral move or allowing them a quiet resignation. This accomplishes two good things for continued success of the company. First, it shows the public that the company is committed to the highest ideals of integrity and transparency continues to be upheld. Second, among the internal population, nothing motivates policy compliance like the threat of a pink slip.

Hot Products

High Capacity USB Drives: Limits to the size of flash memory drives grow larger everyday. Currently, a 2 Gigabyte (GB) USB drive can be purchased for $599.99. (see picture)[16] Smaller sizes in the range of 128-512 Megabytes (MB) retail between $20-170. These devices require no external power, need no special drivers, and can be installed by any user (default settings) on the current operating systems. Some are beginning to incorporate data access security mechanisms such as requiring a password to use the drive or integrating biometrics and allowing for multiple people to register their thumbprint on the device. Although these devices are meant to be small, they usually are large enough to display a company logo or security sticker as mandated by security policy. However, the Pretec IDisk Tiny, at under 5 centimeters in length is a device that challenges proper labeling protocol and begs the necessity and purposefulness of its small size.[17] If a USB device was to be used for clandestine purposes, this would probably be the drive of choice.

Meritline's SpyPen™ has similar features as a normal USB drive, but also hides its primary function that is incorporated into the form of a pen. See pictures at right.[18]

[16] "High Capacity USB Flash Drive." IT Ave. URL: http://www.itave.com/prod_usd/highcap.html (19 June 2004).
[17] "IDisk Tiny – The Smallest USB Flash Drive in the World." 18 March 2004. URL: http://www.pretec.com/PR/PR_iDisk_CeBIT2004.pdf (6 April 2004).
[18] http://lib1.store.vip.sc5.yahoo.com/lib/meritline/spypen1.jpg and http://store1.yimg.com/I/meritline_1807_386837923 (20 August 2004).

Another device that is not apparent as a data device is the **USB Memory Watch** that can be found on the Think Geek web site.[19] It stores up to half a gigabyte of data. The USB cable tucks into the band of the watch and is not easily noticed. See picture at left.[20]

The **C-Pen** is a small handheld scanner. The C-Pen 800C is used like a highlighter to capture text directly to a computer or it can store over up to 2000 pages of text.[21] The device also has infrared capabilities to beam information to a notebook computer or a handheld. See images at right.[22]

The **Casio Color Wrist Camera Watch** is a device you would only expect James Bond to have, but anyone can have it for under $330.[23] Not only does it take color photos, but it has a 2x zoom for when the individual needs to get a better shot from further away. Its built-in memory can take up to 100 pictures and transmit them over infrared beams. The databank function can also be used for inputting up to 24 characters of text for each photo. See image at left.[24]

The **iRiver H300** series digital audio and photo player is a very powerful device that can transfer and store up to 40 gigabytes of data without the aid of a computer. For example, USB drives and digital cameras can connect to the iRiver device directly and transfer its contents while on the go and display them later. The device can also connect directly to a computer via USB exactly the same way a USB drive does, but can transfer up to 80 times the amount of data that can fit on a 512 MB USB drive. The iRiver also comes with a built-in microphone for recording voice conversations. See image at right.[25]

---

[19] http://www.thinkgeek.com/gadgets/watches/5eec/ (12 Aug 2004).
[20] http://www.thinkgeek.com/images/products/front/memory-watch-new.jpg (12 Aug 2004).
[21] http://www.cpen.com/Products/Portable/technical_specification?model=p3 (12 Aug 2004).
[22] Images are displayed from the C-Pen homepage at http://www.cpen.com/ and http://193.109.209.201/cpen/images/products/pens/cpen800C.gif (12 Aug 2004).
[23] http://www.casio.com/index.cfm?fuseaction=products.detail&Product=WQV10D-2# (12 Aug 2004).
[24] http://www.casio.com/images/a/wqv10d-2_a_300x362.jpg

Cellular phones and digital cameras are converging as is evident in **Samsung's SPH-S2300**. Phones have had camera capabilities for some time now, but this is the first to have the same quality, about 3.2 megapixels, as other consumer digital cameras. In addition, it has video recording of up to 2 hours, audio recording, MP3 playback, direct connect to TV for viewing pictures and video, direct connection to computers to use as data transfer device, and memory can be expanded with MiniSD flash memory cards.[26] Of course, it also comes with the full array of PDA-like features that most modern hand phones have. See images at right.[27]

Conclusion

There is a natural tendency to rely on technology to fix our business problems or to blame technology as the cause of many business challenges. However, technology is only a business tool that must be looked at carefully for inherent vulnerabilities or can be utilized to assist in mitigating other vulnerabilities. They do not pose a threat to the organization in and of themselves. Ultimately the banter of the promises of USB drives versus their "threats" will go away with the next hot technology. What needs a deeper look is how the measure of human borne threat stacks up in your organization compared to others in your industry. This paper provided specific steps and guidance on how to identify and mitigate the insider threat.

The previously listed products are only some of the technology devices that are causing concern for CSO's today. Awareness of their existence and their capabilities will assist in knowing what employees are using these days and in developing policy to mitigate vulnerabilities posed by introduction of these devices in the workplace.

[25] Image and specifications found at http://www.dpreview.com/news/0405/04052803iriverh300.asp and http://www.iriver.co.jp/product/h300/ (12 Aug 2004).
[26] http://www.anycall.com/i_world/i_view/view_detail.jsp?PFID=SPH-S2300&real=feature
[27] http://www.anycall.com:8082/upload/i_world/product_/SPH-S2300.zip

References

1. A good listing of computer interfaces and specifications. URL: http://www.techfest.com/hardware/bus.htm (8 Aug 2004).

2. Black, Jeff. "USB Pen Drive + Real Pen = Real Threat (Do the Math)." 21 March 2004. URL: http://www.empiresecurity.com/displayarticle215.html (6 June 2004).

3. Definition of CSO. URL: http://www.csoonline.com.au/index.php/aid;4 (6 June 2004).

4. Example of USB devices that incorporate biometrics. URL: http://www.thumbdrive.com/prd_info.htm (8 Aug 2004).

5. "Gartner Says 60 Percent of Security Breach Incident Costs Incurred by Businesses Will Be Financially or Politically Motivated." 29 May 2003. URL: http://www3.gartner.com/5_about/press_releases/pr29may2003a.jsp# (6 June 2004).

6. "High Capacity USB Flash Drive." IT Ave. URL: http://www.itave.com/prod_usd/highcap.html (19 June 2004).

7. Hollinger Ph.D., Richard C. National Retail Security Survey. November 2002. URL: http://retailindustry.about.com/library/weekly/02/aa021126a.htm and http://web.soc.ufl.edu/SRP/NRSS_2001.pdf (8 Aug 2004).

8. "IDisk Tiny – The Smallest USB Flash Drive in the World." 18 March 2004. URL: http://www.pretec.com/PR/PR_iDisk_CeBIT2004.pdf (6 April 2004).

9. "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems." 19 October 1999. URL: http://www.csl.sri.com/users/neumann/insider-misuse/ins.pdf (8 Aug 2004).

10. "Security for Hard State USB Mobile Disk Devices on Windows 2000/2003/XP." DISA Field Security Operations. 12 June 2003.

11. TheInfoPro/Secure Computing Corp. "Flash Risk." Information Security. April 2004.

12. "USB Flash Drives: Useful Device or Security Threat?" 10 December 2003. URL: http://labmice.techtarget.com/articles/usbflashdrives.htm (6 June 2004).

13. WordNet 2.0 Search: Threat. URL: http://www.cogsci.princeton.edu/cgi-bin/webwn?stage=1&word=threat (12 June 2004).