

The threat posed by portable storage devices

Strategies and solutions to combat corporate data theft

In a society where the use of portable storage devices is commonplace, the threat that these devices pose to corporations and organizations is often ignored. This white paper examines the nature of the threat that these devices present and the counter-measures that organizations can adopt to eliminate them.

Introduction

In an on-demand society where individuals can easily access portable music players, PDAs, mobile phones and digital cameras, technological innovation has responded to personal needs with the development of electronic devices that include data storage capabilities. There is, however, a downside to this modern-day scenario – the misuse of these devices in a corporate environment can spell disaster to a corporation! The statistics are not encouraging; for instance, the 2005 CSI/FBI survey reports that “theft of proprietary information is up from [US] \$168,529 in 2004 to [US] \$355,552 in 2005” (Gordon et al., 2005).

■ **2005 CSI/FBI computer crime and security survey**

“Theft of proprietary information up from \$168,529 in 2004 to \$355,552 in 2005.”

Today, corporations who recognize the extent of the data theft problem are enacting security policies that regulate the use of portable storage devices in the corporate environment. But is a security policy alone the best solution to mitigate the risks posed by portable storage devices? And what are the real risks associated with the uncontrolled use of portable storage devices?

Introduction.....	2
The rise of portable storage devices	2
Why do corporations require protection?	3
Commonly used countermeasures.....	6
Conclusion.....	6
References	7
About GFI	9

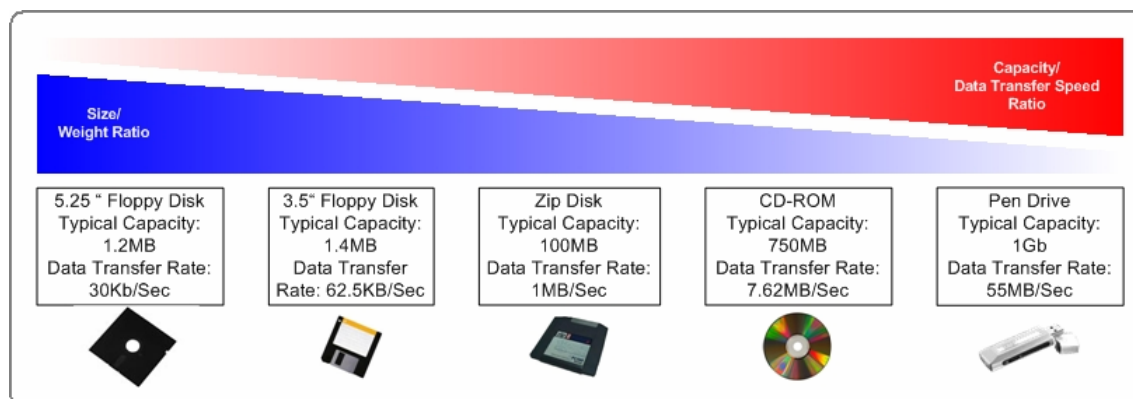
The rise of portable storage devices

In the last ten years data storage technology has broken all the barriers that used to bind it to large devices that stored limited amounts of data. These technological breakthroughs have:

- Increased data storage and data transfer speeds exponentially
- Increased device portability through a substantial reduction in physical device size
- Increased device availability by the development of mass-appeal low-cost products
- Simplified the connectivity method to computer systems.

A typical example is the Apple iPod released in October 2005. This device can store up to 60 GB of data – as much as the typical corporate workstation’s hard drive. In practice, this translates to millions of proprietary, financial, consumer and otherwise sensitive corporate records!

Transferring data from one computer system to another is nowadays a non-technical, highly efficient, inconspicuous task. This effectively puts corporations in harm's way, since the misuse of portable storage devices can expose corporate networks to a number of dangerous issues which might have an impact on corporations in a variety of ways.



The evolution of portable storage media

Why do corporations require protection?

Statistics demonstrate that 98% of all crimes committed against companies in the U.K. had an insider connection (Computer Crime Research Center, 2005). Data theft, legal liabilities, productivity losses and corporate network security breaches are all dangers that corporations have to face if malicious insiders or careless employees misuse portable storage devices at their workplace.

■ Scotland Yard

"98% of all crimes against companies in the U.K. had an insider connection."

Data theft

The actual act of stealing corporate data by insiders is quite simple in itself and today software that is easily available for download automates the whole process. Insiders only need to plug in the portable storage device on a corporate workstation and all data, including sensitive data is automatically copied, without any additional user intervention. This automated process, commonly known as 'pod slurping', is able to copy whole databases and other confidential records to a portable storage device in a matter of a few minutes.

■ Serious Organized Crime Agency (SOCA) – U.K.

"...one of the big threats still comes from trusted insiders. That is, people inside the company who are attacking the systems."

Data theft does not limit itself to corporate insiders. Outsiders can use social engineering techniques to manipulate unsuspecting employees into using media or portable storage devices on the corporate network workstation. Seeded with malware, these devices open backdoors in the corporate perimeter defense, allowing hackers easy access to corporate data. A well publicized example was an experiment conducted in 2006 by the Training Camp, a UK-based training institution (Sturgeon, 2006). This involved the distribution of promotional CDs to office workers. However, apart from the advertised material, these CDs contained a script that tracked and advised The Training Camp when the CD was used. Notwithstanding the fact that the CD contained an advisory note to check their company's security policy before running it, 75 out of the 100 CDs distributed were used on the corporate network. This experiment underscores the fact that employees, acting in good faith, can bypass the best perimeter security, exposing corporations to serious repercussions.

Corporations typically accumulate a wide array of data that can be stolen. This includes:

- Blueprints and engineering plans
- Tenders, budgets, client lists, emails and pricelists
- Credit card and other financial information
- Software source code and database schemas
- Medical or other confidential personally identifiable records
- Classified, restricted or personal information
- Scripts, storyboards, print material, photographic, video or animated film
- Score sheets, lyrics, sound files and other forms of phonographic material.

■ **U.S. Secret Service & CERT Coordination Centre**

"Respondents identified current or former employees and contractors as the second greatest cyber security threat, preceded only by hackers."

The data stolen can be sold to competitors or used by the insiders, their criminal associates or hackers to commit a wide range of crimes ranging from identity theft to extortion and blackmail. Employees leaving the company to work with a competitor may also use the data acquired to gain an edge over their previous employer or directly discredit the image of that company. Surveys conducted by the U.S. Secret Service and CERT Co-ordination centre concluded that: "Respondents identified current or former employees and contractors as the second greatest cyber security threat, preceded only by hackers" (Keeney et al., 2005). This is further corroborated in the CSI/FBI survey which indicates that 68% of respondents claimed losses due to security breaches originating from insiders (Gordon et al., 2006).

■ **2006 CSI/FBI Computer crime and security survey**

"68% of respondents claimed losses due to security breaches originating from insiders."

Legal liabilities

When confidential information is 'lost' or illicit/objectionable data is introduced on the corporate network through portable storage devices, corporations might become legally liable for any information that is stolen or illicitly introduced. Liabilities can impact the corporation's assets significantly under different laws in different countries; under HIPAA (USA) the wrongful disclosure of individually identifiable health information, can be penalized with a maximum fine of \$250,000 and 10 years imprisonment. The table below outlines a list of laws and the country in which they are applicable.

Country	Laws
U.S.A.	Sarbanes Oxley Act , Gramm-Leach-Bliley Act , USA PATRIOT Act , Title 21 of the Federal Regulations Part 11 (21 CFR Part 11) , Federal Information Security Management Act , HIPAA
E. U.	Data Protection Directive , Privacy and Electronic Communication Regulations ; EU Annex 11, Computerized Systems ;
U.K.	Turnbull Guidance Act [1999] , Companies Act , Data Protection Act , Freedom of Information Act , Money Laundering Regulations 2003
Japan	Personal Information Protection Act 2003
Canada	Personal Information Protection and Electronic Document Act (PIPEDA)
Australia	The Federal Privacy Act (Privacy Act 1988)

Productivity loss

The corporate network can be misused by untrustworthy employees who use portable storage devices to bypass perimeter security personal files. These could include part-time work or hobby related material to be carried out during working hours. The problem grows to an exponential level when video games are transferred to the workplace. Video games are addictive, require constant user input and through multiplayer capabilities these can be a means of enticing and distracting more than one employee.

Corporate network security breaches

The usage of portable devices at work can also impact corporate network security through the intentional or unintentional introduction of viruses, malware or crimeware that can bring down the corporate network and disrupt business activity. Law enforcement agencies today acknowledge that "...one of the big threats still comes from trusted insiders. That is, people inside the company who are attacking the systems" (Ilett, 2006).

■ U.S. Federal Trade Commission

"Disgruntled employees gaining access to customer lists and other information is proving a growing danger."

Commonly used countermeasures

There are only a few countermeasures that corporations can adopt to prevent unauthorized portable device use. Banning portable storage devices on the corporate premises and the physical blocking of computer access ports are common practices. The deployment of Windows Group Policies is also utilized. These countermeasures however have a number of shortcomings:

- Most portable storage devices are small and easily concealable, therefore it is difficult to ensure that no-one has brought in a banned device.
- The inability to discriminate between legitimate devices and devices that should be denied access to resources.
- The overhead in manpower required to enforce these countermeasures.

The only really effective solution to counter portable device threats is by deploying a software solution that protects the corporate network perimeter against unauthorized device usage – a solution that allows you to discriminate between legitimate and illegitimate use of devices, in compliance with the custom security policies set up by the corporation.

GFI Software offers a permanent solution which helps you protect your corporation against portable storage device threats. This is GFI EndPointSecurity – the effective counter measure against the enemy within! GFI EndPointSecurity allows you control entry and exit of data via portable storage devices, allowing you to prevent users from taking confidential data or introducing viruses and trojans to your network. GFI EndPointSecurity allows you to actively manage user access to media players (including iPod and Creative Zen), USB sticks, CompactFlash, memory cards, PDAs, Blackberries, mobile phones, CDs, floppies and more. To read more and to download a trial version, visit <http://www.gfi.com/endpointsecurity/>.

Conclusion

The uncontrolled use of portable storage devices by corporate insiders is a definite threat to the security and stability of every business. Malicious insiders and gullible employees who fall for social engineering practices are the weakest link in the corporate security chain. Relying on user voluntary compliance to the corporate device usage policy is not a solution – you must deploy software countermeasures that thwart this risk. GFI EndPointSecurity is a real alternative to corporate turmoil. It ensures business continuity by allowing portable device access to legitimate users whilst keeping corporate business sheltered from unauthorized data transfers to and from portable devices. With GFI EndPointSecurity, corporations are permanently protected!

References

Canadian Parliament (2000) *Personal Information Protection and Electronic Documents Act* available from: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp (last cited 28 July 2006).

Commission of the European Communities (2000) *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* available from: http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com2000-385en.pdf (last cited 28 July 2006).

Computer Crime Research Center (2005) *Security issues: find the enemy within* available from: <http://www.crime-research.org/analytics/security-insider/> (last cited 28 July 2006).

European Parliament and the Council of the European Union (2002) *Directive on privacy and electronic communications* available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML> (last cited 28 July 2006).

European Parliament and the Council of the European Union (2003) *Annex 11 Computerised systems*, Labcompliance available from: <http://www.labcompliance.com/documents/europe/h-213-eu-gmp-annex11.pdf> (last cited 28 July 2006).

Federal Trade Commission (1999) *Gramm-Leach Bliley Act* available from: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> (last cited 28 July 2006).

Financial Reporting Council (2005) *Internal Control: Guidance for Directors on the Combined Code* available from: <http://www.frc.org.uk/documents/pagemanager/frc/Revised%20Turnbull%20Guidance%20October%202005.pdf> (last cited 28 July 2006).

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2005) *2005 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Ilett D. (2006) "Trusted insiders" a threat to corporate security, silicon.com available from: <http://www.silicon.com/research/specialreports/idmanagement/0,3800011361,39158361,00.htm> (last cited 28 July 2006).

Japanese Government (2003) *Personal Information Protection Act 2003* available from: <http://www.privacyexchange.org/japan/PIPA-offtrans.pdf> (last cited 28 July 2006).

Keeney M., Kowalski E., Cappelli D., Moore A., Shimeall T. and Rogers S. (2005) *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S Secret Service and CERT Coordination Center/SEI.

Leahy P. (2001) *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, H.R. 3162 Section-by-section Analysis* available from: <http://leahy.senate.gov/press/200110/102401a.html> (last cited 28 July 2006).

NIST Computer Security Division (2002) *Federal Information Security Management Act of 2002* available from: <http://csrc.nist.gov/policies/FISMA-final.pdf> (last cited 28 July 2006).

Office of Legislative Drafting and Publishing (2006) *Privacy Act 1988* available from: http://www.privacy.gov.au/publications/privacy88_030706.pdf (last cited 28 July 2006).

Sarbanes-Oxley (2002) *Sarbanes-Oxley Act of 2002* available from: http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley (last cited 28 July 2006).

Sturgeon W. (2006) *Proof: Employees don't care about security, silicon.com* available from: <http://software.silicon.com/security/0,39024655,39156503,00.htm> (last cited 28 July 2006).

United Kingdom Parliament (1989) *Companies Act 1989* available from: http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm (last cited 28 July 2006).

United Kingdom Parliament (1998) *Data Protection Act 1998* available from: <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm> (last cited 28 July 2006).

United Kingdom Parliament (2000) *Freedom of Information Act 2000* available from: <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm> (last cited 28 July 2006).

United Kingdom Parliament (2003) *The Money Laundering Regulations 2003* available from: <http://www.opsi.gov.uk/si/si2003/20033075.htm> (last cited 28 July 2006).

U.S. Food and Drug Administration (2000) *Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic Records; Electronic Signatures* available from: http://www.fda.gov/ora/compliance_ref/part11/ (last cited 28 July 2006).

U.S. Department of Health & Human Services (1996) *Health Insurance Portability and Accountability Act of 1996* available from: <http://aspe.hhs.gov/admsimp/pl104191.htm> (last cited 28 July 2006).

About GFI

GFI is a leading developer of network security, content security and messaging solutions, providing a single source for network administrators to address their network security and messaging needs. GFI is a market leader in network software and has a customer base in excess of 160,000 customers to date. A product within GFI's range of solutions is GFI EndPointSecurity. GFI EndPointSecurity provides full network-wide control of portable devices such as iPods, USB sticks, mp3 players and more. More information is available at www.gfi.com.

© 2006 GFI Software Ltd. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANGuard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

