GFI White Paper

The threats posed by portable storage devices

Uncontrolled use of iPods, USB sticks, PDAs and other devices on your network can lead to data theft, introduction of viruses, legal liability issues and more.

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 devices such as iPods, USB sticks, flash drives and smartphones present and the counter-measures that organizations can adopt to eliminate them.

GFI®

Contents

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 2008 CSI survey reports that dealing with the cost of theft of proprietary information or loss of customer and employee confidential data averaged at approximately $241,000 and $268,000 respectively.

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?

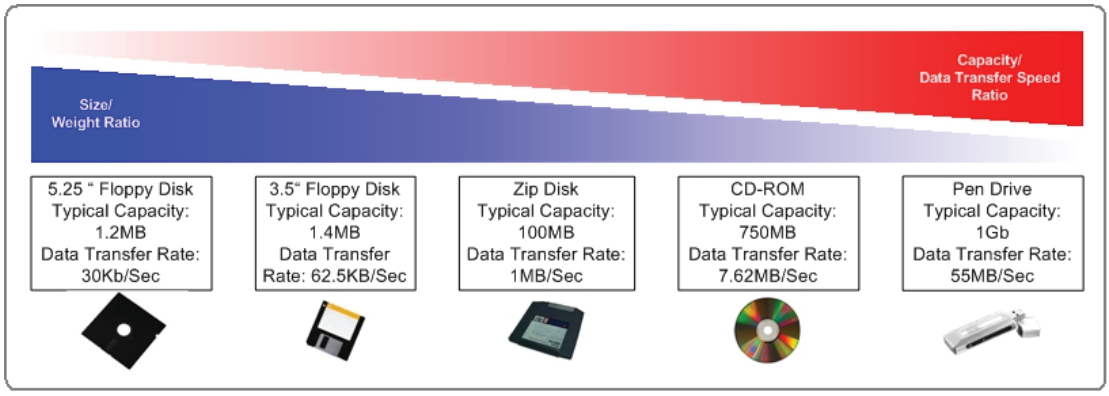
The rise of portable storage devices

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?

According to the CSI survey, 44% of incidents reported were insider abuse while another 9% reported theft/ loss of proprietary information from mobile devices and other sources. 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.

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) – UK

"…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 defence, 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.

US Secret Service and 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 US 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 survey which indicates that 44% of respondents claimed losses due to security breaches originating from insiders.

2008 CSI Computer Crime and Security Survey

"44% 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.

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.

Country	Laws
USA	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
EU	Data Protection Directive, Privacy and Electronic Communication Regulations; EU Annex 11, Computerized Systems
UK	Turnbull Guidance Act [1999], Companies Act, Data Protection Act, Freedom of Information Act, Money Laundering Regulations 2003
UK	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)

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).

US 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 solution which helps you protect your corporation against portable storage device threats. This is GFI EndPointSecurity™ – an effective counter measure against the enemy within! GFI EndPointSecurity gives you direct control over what devices are in use on your network. You not only gain control over what is in use but you also know what has been used by who, and most importantly you gain knowledge of what data has been copied. GFI EndPointSecurity allows you to actively manage user access and the log activity of dozens of portable storage devices such as media players, USB drives, PDAs, BlackBerry handhelds, smartphones and so on. 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 helps combat such 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.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

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).

Richardson R. (2008) 2008 CSI 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 Strenghtening 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 Accoutability Act of 1996 available from: http://aspe.hhs.gov/admnsimp/pl104191.htm (last cited 28 July 2006).

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI 1030 may11

GFI®