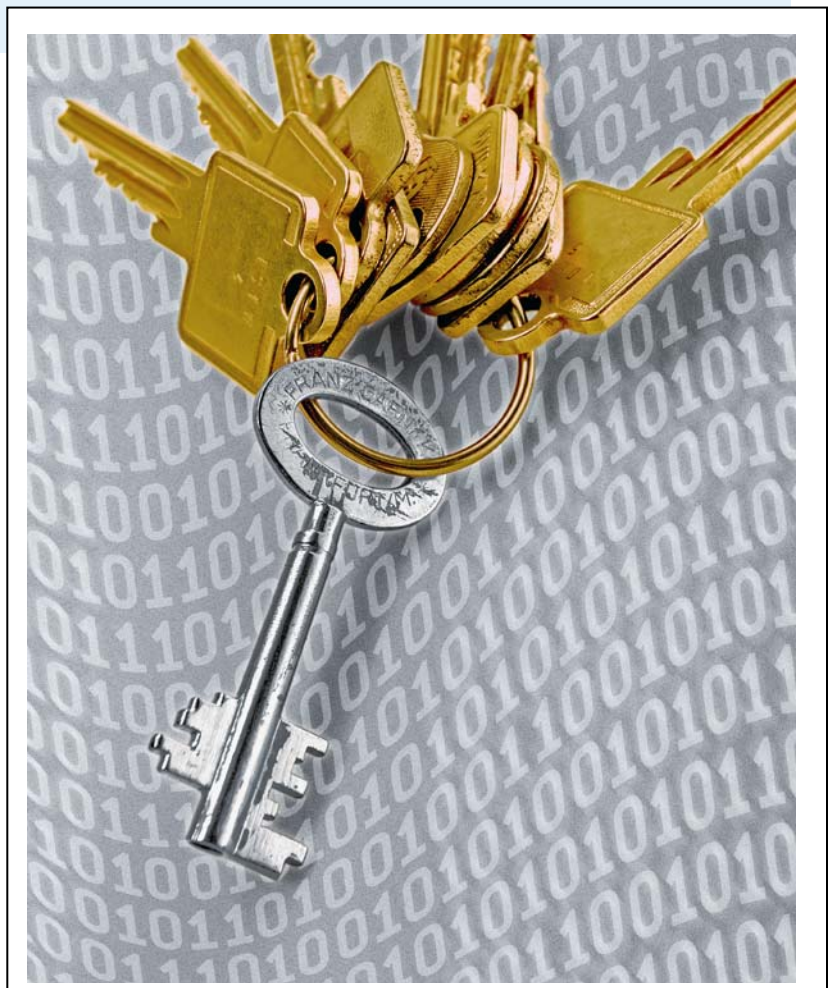




Threats from Mobile Devices

How to protect your sensitive information



|

Threats from Mobile Devices

How to protect your sensitive information

The popularity of mobile devices, especially storage devices poses new risks to corporate data. This whitepaper presents an overview of these risks and assesses the available protection mechanisms.

Mobile devices are a constant presence in today's computing. The USB standard has made it possible to easily attach a wide range of devices, from external network adapters to coffee warmers, to any computer. Especially popular are mobile storage devices, from the ubiquitous memory stick to music players that can also hold any type of data. In the twelve months ending in October 2006, Apple alone had sold 39 million iPods, each of them capable of holding up to 80 GB of music—or of corporate documents.

At the same time, companies are increasingly concerned about protecting their data. Recent high-profile cases of data disclosure, and there is an increase in legislation and regulatory requirements that can result have a severe financial impact when data gets stolen or compromised. No wonder, that data protection and compliance are among the most critical issues for today's companies, according to the 2006 Computer Crime and Security Survey, jointly conducted by the Computer Security Institute and the FBI.

Threat Assessment

» Threat: Data Theft

Most businesses and organizations don't realize how real the dangers from data theft are. However, there's reason to worry. Even smaller organizations may store information that's valuable enough to others to make it

U3: A NEW STANDARD FOR USB

U3 is a recent standard for USB memory sticks that creates the ability to run programs, such as Web browsers, entirely from the U3-compliant device. This can be useful to ensure privacy when surfing the Internet from a public terminal. However, such a USB stick can be easily modified to automatically run any program. One possible application would be a USB stick that upon insertion into a computer could copy data to the device within seconds, even without touching a keyboard or mouse. Using such a device, data thieves can accomplish their goal with even less risk of detection.

worthwhile to mount an effort to steal this data. Confidential research data may come to mind, but something as innocuous as a price lists may be extremely interesting to a competitor, and customer from your network could be used by a criminal gang in a massive identify theft scheme. Considering how easy it is to store large amounts of data on mobile storage devices, current security measure are insufficient for ensuring that your data remains confidential. In addition, if an employee copies data to a mobile device, it's unlikely that anyone ever finds out because such actions are rarely audited.

Corporate losses as a result of the theft of confidential information were \$30 million US in 2005 alone. But the risk is underestimated by most organizations, and attacks from the inside are as likely as attacks from the outside. Computer crime doesn't occur only in large organizations. Many incidents affect small companies and new products or

technologies, which may be of interest to the competition. Almost any device attached to a computer, such as USB sticks, flash drives, PDAs or iPods can lead to major security breaches and become a vehicle for the theft of confidential and private information.

» Threat: Data Disclosure

Data theft is a serious issue, but disclosure of confidential information due to carelessness is even more prevalent. Employees frequently copy data to laptop computers and mobile storage devices to work on them while away from the workplace. Because of some high-profile cases of lost laptops, many organizations have started to look at how to encrypt information on these computers. Data disclosure due to lost USB sticks and other mobile storage devices is probably much more common, but no reliable data exist because employees

rarely report the loss of a USB stick, even if it contains confidential information. However, there are studies that show that tens of thousands of mobile devices are left behind in taxi cabs every month in the United States alone.

THE COST OF DATA BREACHES

According to a 2006 study by the Ponemon Institute, data breaches cost companies an average of \$182 per record. This includes direct costs, (legal, notification) indirect costs (loss of employee productivity) and opportunity cost (loss of customers). Government fines, legal action, shareholder value loss and diminished goodwill may increase the total cost.

In addition to disclosure of information to competitors, such disclosure can also have a severe impact on an organization's reputation and result in significant costs when legislation requires that affected customers are informed that information about them is lost. In some cases, companies and public agencies have even had to purchase identity theft protection for all affected clients to contain the damage to their reputation.

» Threat: Intrusion

Uncontrolled mobile devices can create an uncontrolled entry point into a corporate network that completely bypasses any protection that's created by a corporate firewall. There have been reported cases of criminals entering corporate networks by attaching unauthorized devices, such as wireless network adapters, on corporate networks. However, sometimes careless or uninformed employees can pose a larger risk. To prove the point, a security company in London handed out compact discs to commuters in London's financial district. These discs were designed to start a program that contacted a central server. The data that was collected showed that employees of many major banks had inserted the discs into their work computers and thus run the program. If the CDs had contained a malicious program instead, the results could have resulted in the installation of spyware or other malicious software. A similar study also showed that many people would insert a USB memory stick that they found lying around in public, again creating the risk of the introduction of malicious software into a corporate network.

By using a small USB flash drive, anyone can take control of a computer in seconds. This includes installing Trojan Horse programs that may e-mail or transfer data to a remote location. Running undetected in the background, such programs may also enable remote access to the computer, install backdoors, including admin accounts, as well as infect any other removable media device that is plugged into that system. Software for this purpose can be downloaded from the internet and it is relatively easy to use.

» Threat: System Instability

When employees can attach any device to a computer, helpdesk calls increase when these devices cause computers to become unreliable and unforeseen interactions between corporate software and these devices emerges. Troubleshooting problems caused by the uncontrolled use of peripheral devices can become time-consuming and expensive.

» Real-World Examples

Security breaches due to uncontrolled mobile devices are an everyday occurrence. While most of them go unreported, many of them appear in the news:

January, 2007: *The head of the U.S. nuclear security agency was forced to resign due to serious security breaches. One of the issues was the discovery of USB flash drives containing classified documents when police raided a drug house in Los Alamos, NM.*

December, 2006: *A portable drive containing personal information about more than 2,500 students and faculty at California State University, including Social Security Numbers, was stolen from the trunk of a car.*

December 2006: *Bank of America announced that a former contractor may have stolen Social Security numbers and other personal information about an undisclosed number of the bank's customers.*

October, 2006: *Department of Homeland Security officials announced that a storage device containing sensitive personal information about employees at Portland International Airport may have been lost.*

September, 2006: *The Michigan Department of Community Health purchases identity theft protection for*

over 4,000 participants in a scientific study after losing a flash drive containing personal information about them.

June, 2006: *Funds were stolen from the accounts of customers of the international bank HSBC after a call center employee in Bangalore, India passed confidential information on to criminal associates.*

October, 2006: *McDonald's Japan launches a recall of 10,000 MP3 players that it gave away as part of a contest after discovering that they were infected with dangerous spyware.*

February, 2006: *A British security firm hands out CDs to commuters in London's financial district, claiming they contained a Valentine's Day promotion. Monitoring software on the CDs reported back to the firm that many of the recipients, including some working at large financial institutions, had placed the CD into computers at work. Had the CDs contained malicious software, the result could have been a large-scale installation of spyware on computers containing sensitive information.*

» Current Protection Mechanisms

Current protection mechanisms don't adequately protect against these threats. The following table highlights the shortcomings of the most common methods in use today.

File Permissions	Corporate Policy	Full-Drive Encryption	Windows Policies
Permissions on servers and workstations only control initial access to data. Once the data resides on a mobile device, permissions no longer apply and anyone can access the data.	Corporate policy may specify how mobile devices can be used and what can be copied to these devices. However, without enforcement, such policies are ineffective.	Software that encrypts entire hard drives can effectively protect against data leakage due to lost laptops. However, such a solution does not address mobile devices.	Windows offers multiple methods to disable mobile devices, but all of these methods are very inflexible. Windows Vista's controls are better but in many cases impractical to configure.

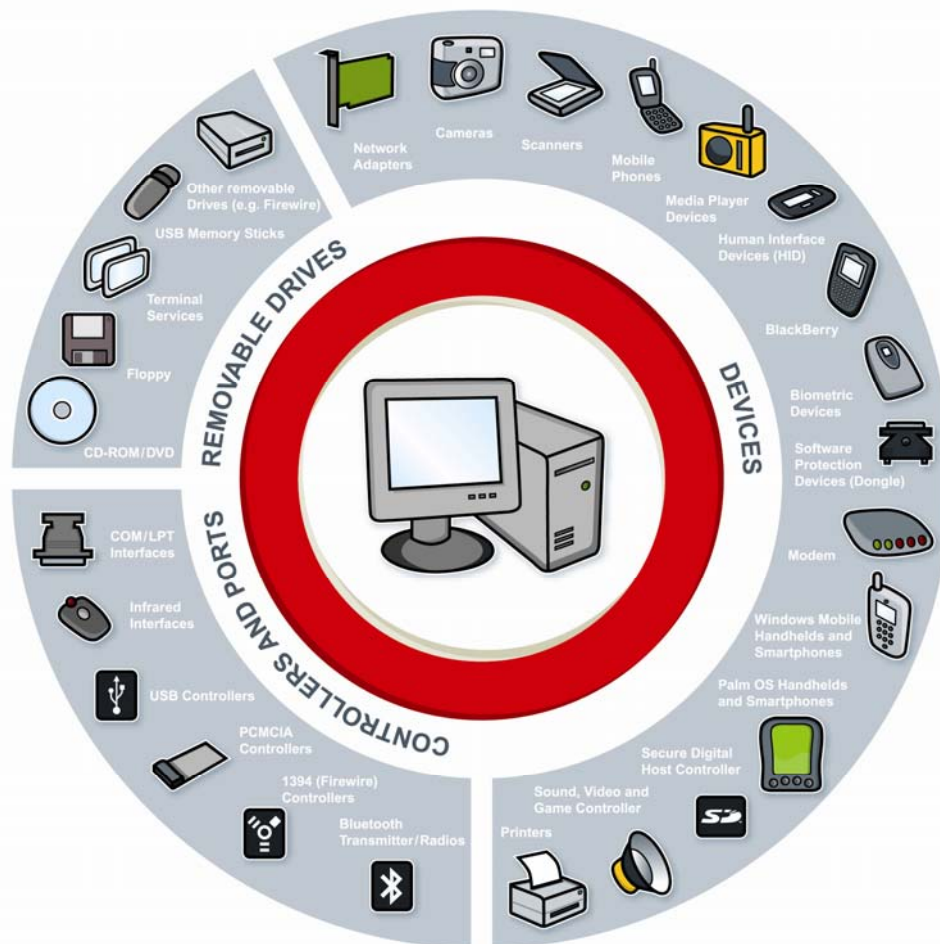
The Challenge: Productive and Safe Use of Devices

Most of the threats from unapproved device usage can be eliminated by simply disabling the ports that these devices can be attached to. However, this is not a realistic solution for organizations that depend on selected external devices for approved business functions or that need to move data between computers using mobile storage. To make this possible, it is necessary to have granular control over can use which device on corporate

computers. Windows does not give administrators this type of granular control, creating the need for specialized software solutions. Such a solution must meet a number of important requirements:

» Comprehensive Device Support

To be effective, any device control solution has to be comprehensive. While USB devices are most common today, other connectivity methods, such as FireWire, pose similar challenges. And device control must be able to differentiate between different types of devices so administrators can, for example, allow the use of USB keyboards while preventing the use of music players.



» Granular Control

Not everyone in an organization has the same requirements for legitimate device usage. For example, a mortgage company may determine prohibit call center employees from using mobile storage devices to prevent the theft of customer data, but help desk personnel may need to copy driver files from a flash drive to the help desk computers. A small company may perform a daily backup of local data to a portable hard drive every evening but does not want to allow the use of other portable storage. An effective device control solution can differentiate between devices by type, model, or even serial number, and it allows administrators to allow or deny device usage based on device, user, time of day, or a number of other factors.

» Data Protection

Many employees have a legitimate need to copy data to a mobile device. One employee may use a USB stick to give a file to a business partner. Another employee may use a portable hard drive to take files with her to work on them at home. An effective device control solution must not only make this possible, it must also provide a mechanism to ensure that the loss of a storage device does not result in data disclosure. This means that it has to include a mechanism to encrypt the data so that someone who finds a lost device cannot access the data. Ideally such an encryption solution is transparent to the user but allows easy authenticated access to the data even on computers that are not managed by the organization.

REGULATORY REQUIREMENTS

Protection of confidential data has led to an increase in federal and state laws that require private companies and public entities to safeguard data they maintain about customers. Some of these laws are:

- **Sarbanes-Oxley Act**
The Sarbanes-Oxley Act requires publicly traded companies to implement controls and procedures to prevent fraud, unauthorized activity or the loss of vital data.
- **HIPAA**
The Health Information Privacy and Accountability Act requires medical service providers to safeguard health information and provides penalties for non-compliance that can range up to \$250,000 and 10 years in jail.
- **Gramm-Leach-Bliley Act**
The Gramm-Leach-Bliley Act requires financial institutions to safeguard consumers' personally identifiable information
- **California SB 1386**
California SB 1386 requires organization to notify individuals if private information has been compromised. Many other states have enacted similar legislation.
- **PIPED (Canada)**
The Personal Information Protection and Electronic Data Documents Act is similar in intent and impact as the Gramm-Leach-Bliley Act in the US

Some legislation requires companies to take action if they suspect that data has been lost or misplaced, even when there's no concrete evidence that someone has obtained this information.

» Monitoring

Being able to monitor how devices are used and what data is copied to and from devices is a crucial requirement for all but the smallest organization. More and more organizations face regulatory requirements that require them to notify customers and clients when personal data may have been compromised, even when this involves no confirmed misuse. Being able to show that the lost data is encrypted can eliminate the notification requirement with the associated cost and loss of reputation. An effective monitoring solution must be comprehensive, flexible, and include detailed information about device usage and the copying of files.

» TCO

When assessing the total cost of any IT solution, it is necessary to look both at the purchase cost and at the cost of ongoing administration. Both of them add up to create the total cost of ownership (TCO). As with any IT component, the ongoing costs of a device control solution are influenced by the required infrastructure and the time spent on administration. Many IT solutions require a dedicated central infrastructure to accomplish their tasks. This can be costly, and smart managers look for solutions that take advantage of already existing infrastructure components instead of requiring more dedicated servers. Also, solutions that provide a low TCO typically take advantage of existing skills in IT departments instead of requiring administrators to learn how to use new tools.

CenterTools DriveLock™—The Leader in Device Control

DriveLock™ from CenterTools provides effective protection from mobile device threats, while addressing the requirements of organizations of any size. DriveLock™ is a lightweight software solution that helps you secure your computers. DriveLock™ offers dynamic, configurable access control for mobile drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.) and also controls the use of most other device types, such as Bluetooth, Palm, Windows Mobile, BlackBerry, virtual devices, Smartphones, media devices and many more. By configuring whitelist rules based on device type and hardware ID you can define exactly who can access which device at which time. Removable drives can be controlled according to vendor, product ID and even according to serial number, allowing you to define and enforce very granular access control policies. Additional features let you unlock specific authorized media and to define time limits and computers for whitelist rules. You can even unlock DriveLock's device control on a computer temporarily if required, and you can do this even when this computer is offline and not connected to a network. DriveLock's support for different device types and granular control make it easy to enforce virtually any corporate policies on device usage.

Installation of the client software (the DriveLock™ Agent) and policy deployment can be easily accomplished by using existing software deployment mechanisms or by using the Group Policy feature of Active Directory. Alternatively, you can distribute policies using configuration files for standalone computers or in environments without Active Directory (for example Novell).

DriveLock's auditing capabilities, coupled with its shadowing functionality give you the control and information you need to enforce policy compliance. By using the DriveLock™ Device Scanner you can detect any drive or device used in your network, even if it is not longer connected to the computer. The DriveLock™ Agent doesn't need to be installed on the target computers to use the Device Scanner.

Automatic and transparent encryption of mobile data makes it easy for users to take data with them without administrators and management having to worry about unauthorized disclosure. DriveLock™ can enforce the use of encryption when data is copied to removable drives to secure sensitive information. The Security Reporting Center is DriveLock's central database and reporting console. The SRC consolidates all DriveLock™ events, information about whitelist rules, client configuration and Device Scanner results in a central SQL Server database. Administrators can then use this data to create dynamic reports for auditing and management reports. All of this adds up to a device control solution that is easy to implement, easy to administer and easy to use.

To read more about DriveLock™ or to download a fully functional trial, visit

<http://www.pcprofile.com/USBScanner.htm>

CenterTools DriveLock™ is available from;



PCProfile
Adelaide South Australia
Timezone GMT +0930
Contact via Cell/Mobile +61 (0) 448 650 227
Fax +61 (0) 8 8265 1961
email : pcprofile@pcprofile.com
<http://www.pcprofile.com/USBScanner.htm>

DriveLock
Intelligent control of mobile devices