



---

## The Threat from Mobile Devices

*How to Protect Business Critical Information*

---



---

**emereo**

*Protecting Your Organisation  
Without Inhibiting Your People*

## The Threats from Mobile Devices How to Protect Sensitive Information

The popularity of mobile devices, including USB flash drives, poses serious risks to corporate data. Recent development advances have made threats from mobile devices more urgent. At the same time companies have seen an increase in their financial exposure as legislation requires expensive mitigation steps when data leakage happens. This whitepaper highlights some of these developments and explains how organisations can protect themselves.

### Threats and Costs

New threat trends include viruses that target USB storage and the way Windows automatically runs programs from certain devices. The real cost of data breaches is becoming more apparent as more organisations are forced to disclose security incidents .

### Viruses Targeting USB Storage

There's nothing silly about the "W32/SillyFD" worm that was recently discovered. This worm is specifically designed to spread itself via removable devices, such as USB flash drives. This particular worm is not very sophisticated and most virus experts view it only as a moderate danger. However, it is likely a sign of things to come. Virus writers design their products to spread using any popular medium. In the 1980s the main medium for virus propagation was floppy disks.

The 1990s saw a shift to e-mail. Today's popularity and preponderance of mobile storage devices makes them an attractive target for virus writers and you are sure to see more viruses targeting mobile storage. Most likely future viruses will be more sophisticated and destructive than W32/SillyFD. Anti-virus software may catch these viruses, but it's dangerous to rely on this as your only protection. Like anything else, antivirus software can fail. Security experts advocate the concept of "Defense in Depth", which relies on multiple layers of protection, ensuring that security is maintained even if one layer fails. Control of what data can be transferred to and from a mobile storage device can be an important part of a comprehensive security policy.

### 'Just Plugging It In' Becomes Dangerous

Imagine that on your way to work you found a USB stick lying on the ground. What would you do? If you're like most people, you would pick it up, take it to your office and plug it into your computer. Whether out of curiosity or a desire to locate the rightful owner of the device, most people in this situation want to see what data is on the device — even if there's a corporate policy against the use of entrusted media. The biggest danger of accessing the USB drive is that you might run a malicious program from it. Hopefully you won't do this, but you're still at risk. Hackers have found an ingenious method to *automatically and silently run malicious software* when a USB device is plugged into a computer.



Here are the details on how this is possible:

In Windows you can create an autorun.inf file in the root of any drive to tell Windows to automatically start any program specified in this file. You probably have seen behavior like this when an installation program starts upon inserting a software CD into your computer's CD-ROM drive. In an effort to strike a balance between a smooth user experience and making computing secure, the Windows default settings allow programs to start automatically from a CD-ROM.



When you insert removable USB storage, Windows requires your confirmation before the program can run. Based on these defaults, you would at least be warned if a program attempted to run automatically from a USB stick, but hackers have found a method to automatically run a program from a USB stick without any warning: if a USB stick looks to Windows like a CD-ROM drive, the Autorun feature works without the user notification and the result can be that malicious software gets launched on your computer without requiring your approval.

Making a USB drive appear as a CD-ROM drive is not as difficult as it seems, as long as the device conforms to the relatively new U3 standard, which was developed by a consortium of leading flash drive manufacturers. According to this group, U3 drives "let you carry software programs on a USB flash drive with your personal preferences so you can launch software and access all of your own data on any Windows XP or Windows 2000 PC." U3 devices look like regular USB sticks, but when you insert it into a computer, Windows sees not only a USB storage device but also a CD-ROM drive. By design, only a manufacturer-supplied installation program can write to the partition that appears as a CD-ROM drive, and these programs are designed to only copy U3-certified applications. Unfortunately, hackers have found ways to circumvent this restriction. Anyone can find instructions on the Internet for how to copy other data to a U3 device, including malicious software and a corresponding autorun.inf.

### What About CDs

*The same USB-based attack described in this whitepaper can also be performed by getting an unsuspecting user to insert a CD containing malicious software into a CD-ROM drive. Accomplishing this can be very simple. Using the concept of "social engineering", or tricking someone into doing something, can be very effective.*

*For example, a criminal may mail the victim a professional and legitimate looking CD that appears to come from a business partner or a trade association. In all likelihood the recipient will not hesitate to use this CD without first confirming whether it's safe to do so.*

What's the worst that can happen when you use such a modified U3 USB drive? After you insert it into your computer, and after Windows has recognised the hardware, the program specified in the autorun.inf automatically runs without requiring any confirmation. This may be one of the programs that have been created by criminals specifically to steal data off computers. *This is not just a theoretical threat.* Programs such as *Switchblade* and *Hacksaw* are designed to copy confidential data, record keystrokes and find password hashes. Some versions of these tools store the results on the USB stick, but others send the data to an attacker as an e-mail message.

Combine this threat with another development in Internet security and the problem gets even worse: Over the last two years there has been a *sharp increase in computer crime that's profit-oriented and targeted at specific companies.* A USB stick or CD containing malicious software most likely doesn't originate from a teenage hacker but was planted by a hardened criminal who knows exactly which data he wants to steal from your company. Or, imagine that the malicious program on the USB stick encrypts important files on your workstation or a server, rendering the data inaccessible to you. This is then followed by a blackmail notice demanding money in return for the key needed for decrypting.

The threats from attacks using mobile devices and removable media are real and you can't afford to ignore them. As the examples above illustrate, even honest and well-meaning employees can jeopardize the security of your entire network simply by plugging a device or inserting a CD into a computer.

### Ignoring Device Security Can Be Expensive

Data theft is not the only threat associated with mobile storage devices. Accidental disclosure of confidential data can be just as damaging. Data leakage happens frequently, often through mobile storage.

» According to the latest Symantec Internet Security Threat Report, theft or loss of a computer or data storage medium, such as a USB memory key, made up *54 percent of all identity theft-related data Breaches.*

» The same study shows that threats to confidential information made up 66 percent of the top 50 malicious code reported to Symantec, and representing a 48% increase on the previous period.

You don't have to look for long to find specific examples. Data breaches are reported almost daily. Here are just a few recent examples:

» 25 million lost child benefit records.

» 26,000 retail staff warned that their personal data is at risk following the theft of a laptop containing pension information

» FSA hits Building Society with a £1m fine following the theft of a laptop

» 3 million UK learner driver records go missing

The overall costs of data leakage by companies, government agencies and others are staggering. But what's the risk to your organisation? The financial exposure and risk depend on the value of your data and the costs involved in recovering from a data breach. But even the simple disclosure of customer information can be costly, and no matter what the result how you calculate the risk, there's no question that any data loss would be expensive.

*According to Forrester Research, the cost of a security breach is \$90 To \$305 Per Lost Record. Other studies show even higher numbers.*

Lost or stolen flash drives, hard drives, CDs and laptops are a frequent source of data leakage. Controlling what data is kept on such devices and encrypting data that is legitimately stored on them must be a crucial component of any IT security strategy.

### What You Can Do

To protect your network against the threats described in this whitepaper, you need to take a combination of measures, ranging from eliminating software vulnerabilities to educating employees. One critical step is to take control of who in your organisation is allowed to use mobile storage devices and how these devices are used. When there is a real business need to store data on mobile storage device, encryption is necessary to ensure that no unauthorised access to the data is possible if the device is lost or stolen. However, encrypting is only effective when it doesn't make it more difficult for people to do their jobs. This means that encryption must be automatic and transparent to users. Finally, effective protection must be traceable. In case a flash drive or CD is lost, it is necessary to know what data was on the device and whether it was encrypted.

Emereo|EPS, powered by DriveLock™ from CenterTools, is an effective device control solution with a proven track record for controlling and securing devices. DriveLock™ can help you:

» Take complete control of who is allowed to use any device on your organisation's computers.

» Keep malicious software out of your network and stop the theft and accidental disclosure of data.

» Automatically and transparently encrypt all data copied to mobile devices.

» Implement comprehensive auditing so you know where your data is going.

More than 80% of all attacks originate inside the company

Computing – November 2008

DriveLock™ 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 with dynamic, configurable access control for mobile drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.). DriveLock™ also lets you control 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 and when. 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.

Ease of administration and implementation are important elements of DriveLock. Installation of the client software (the DriveLock™ Agent) and policy deployment are 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).

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 (SRC) 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.

DriveLock's extensive 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 no longer connected to the computer. The DriveLock™ Agent doesn't need to be installed on the target computers to use the Device Scanner.





## About Emereo Solutions

Emereo Solutions (UK) Limited (formerly AdRem Software UK) was founded in 2004 as a privately held company. Its installed base serves a diverse range of customer types base from Central and Local Government, the NHS, Education, Finance Services, Law firms and many more organisations where the goal is making IT effective and available. Emereo's solutions have been deployed on over 15,000 servers across the UK and Ireland.

Emereo provides rapidly-deployed software solutions for infrastructure management covering network management and monitoring, network behaviour analysis, end-point security and IT service management. Our solutions help organisations secure greater resilience of their enterprise networks so IT can provide better services to the business and operations it supports.

Best-of-Breed products adhere to ITIL and COBIT best practices and ensure compliance with initiatives such as Sarbanes Oxley, FSA, GSI, e-Health and e-Government (Co-Co). The Company's products deliver efficient and effective solutions without prohibitive costs and extended consulting times traditionally associated with enterprise solutions.



*Protecting Your Organisation  
Without Inhibiting Your People*

**Emereo Solutions (UK) Limited**  
6 Rickett Street  
London SW6 1RU

Telephone: 0871 717 7294  
Facsimile: 020 7385 7183

**[www.emereo.eu](http://www.emereo.eu)**

©2008 Emereo Solutions (UK) Limited  
This document is written by Emereo Solutions and represents the views and opinions of the Company regarding its content, as of the date the document was issued.  
The information contained in this document is subject to change without notice.

Emereo Solutions encourages the reader to evaluate all products personally.  
Emereo and Emereo|EPS are trademarks or registered trademarks of Emereo Solutions (UK) Limited.  
DriveLock is a registered trademarks of CenterTools GmbH  
All other product and brand names are trademarks or registered trademarks of their respective owners.

First Published February 2008. Revised February 2009