

Survey shows IT profession see risk of removable media but turn a blind eye!

Submitted by: Eskenzi PR Limited

Monday, 13 June 2005

Newmarket - 13th June 2005 According to a survey on "Removable Media in the Workplace" companies' information security expenditure could all be for nothing as they turn a blind eye to the threat of removable media. The research, conducted by mobile security specialists Pointsec, shows that removable media devices such as media players and USB flash drives are now routinely used by a huge number of employees in the vast majority of UK businesses, but with little regard to the security threat they pose.

A staggering two-thirds of IT professionals who use USB flash drives themselves at work admitted that they did not protect them with encryption even though they are aware of the associated dangers.

The survey highlights that a large number of organisations are yet to address the problem of removable media. With removable media plummeting in price, memory capacity soaring and more people using them at work, companies need to be aware of how easy it is for staff to use them, lose them or take competitive information away on them, all in the palm of their hands. If lost or stolen, vast amounts of valuable company information could seriously expose a company to extortion, digital identity fraud, or damage to their reputation, integrity and brand.

Some of the headline statistics from the survey, conducted amongst 300 UK IT professionals (many of whom are IT security managers), reveals that:

- Removable media devices are being used in 84% of companies.
- On average 31% of employees within a company are utilising them in the office.
- 90% percent of those surveyed were aware of the potential danger that removable media presents.
- A third of organisations state that removable media is being used within their company without authorization.
- 41% of IT professionals are not aware how easy it is to protect the data on a removable media device.

Martin Allen, Managing Director of Pointsec UK said "There seems little point in companies spending vast sums of money on information security if at the same time they're letting their staff use these devices at work which allow them unhindered access to download vast quantities of sensitive company information."

"Storing information on devices is not a new problem – not so long ago it would have been information stored onto a 1.5mb floppy disk, however, now the problem is a much greater storage problem and therefore, needs to be dealt with in the security policy. Organisations need to introduce strict guidelines on the use of removable media devices in the workplace, as well as investing in encryption software which will allow administrators to force the encryption of all data put onto a mobile device. Using this type of software is just as vital and inexpensive as using anti-virus software, yet only a fraction of organisations have woken up to the problem."

The proliferation of high capacity media players and USB flash drives on the market makes it possible to save anything up to 100GB's of information on one. This means an employee could download 4 million

documents of valuable data on what appears at first sight to be just an entertainment tool. USB pen drives and USB memory sticks can now store 4GB's of memory which equates to around 160,000 documents.

In addition, employees could unintentionally expose their organisation to infection from viruses, worms or other types of malware when these devices are used to transfer data from non-company controlled computers to the user's computer at work.

To secure your company from the security implications associated with removable media and mobile devices Pointsec recommend that you:

1. Deploy user mobile guidelines or ensure that your corporate IT security policy includes corporate directives that states the importance of proper handling of mobile devices such as removable media.
2. Ensure that all members of staff are aware of that their employment does not allow non-company devices to be used within the company network.
3. Use encryption software such as Pointsec Media Encryption which enables centralised policy enforcement of strong encryption of all data stored at mobile devices and removable media.
4. Use policies to control the amount of login attempts that people may use to try and get at information they shouldn't.
5. Have methods in place which enables encrypted data to be decrypted in a controlled way outside the corporate network.
6. The encryption process should be transparent and quick to the user, so that it does not interfere with their work or put any extra requirements on the user.
7. Have methods (independent of the end user) which enable decryption of all encrypted data within the company network

Preventing people bringing removable media devices into the office is an extremely difficult problem. However, although they are fun and convenient they are very easy to lose or abuse and therefore a real security threat. If companies are to prevent breaking new legislation such as Sarbanes Oxley, Basel 2, The Data Protection Act, as well as not falling victim to the havoc these tiny portable devices can cause, companies need to rapidly get to grips with the risks associated with removable media and protect themselves against these risks.

Ends

About Pointsec

Pointsec is the worldwide de facto standard for mobile device security – with the most customers deployed, highest level of certification, and more complete device coverage than any other company. Pointsec delivers a trusted solution for automatic data encryption that guarantees proven protection at the most vulnerable point where sensitive enterprise data is stored – on mobile devices. By securing sensitive information stored on laptops, PDAs, smartphones, and removable media, enterprises and government organizations can protect and enhance their image, minimize risk, shield confidential data, guard information assets, and strengthen public and shareholder confidence. Pointsec's customers include blue chip companies and government organizations around the world. Founded in 1988, Pointsec AB is a wholly owned subsidiary of Protect Data AB, publicly traded (PROT) on the Stockholm stock exchange. The company has four U.S. offices and 11 EMEA offices. Visit our web site at:
www.pointsec.com.

Pointsec and Pointsec for PC are registered trademarks of Pointsec Mobile Technologies. All other product or service names mentioned herein are the trademarks of their respective owners.

If you would like a copy of the survey questions or more information on this survey please contact:

Yvonne Eskenzi

Tel. 020 8449 8292

Email Yvonne@eskenzipr.com