

Laptop Data....

As portable computing devices such as laptops and PDAs (Personal Digital Assistants) get smaller and more powerful, they are becoming more popular, particularly in the corporate world.

There is a need among many busy executives to have access to communication systems such as email via "Push" technologies like Blackberry and the Nokia Business Centre and Communicators. These people, the "Road Warriors", also need to have offline information available to them when they are not able to get network connections, particularly when in aircraft.

This increased need for access to corporate data has dramatically ramped up the Information Security risk that these devices pose to the organisation.

In many cases, the personnel that are supplied with these portable-computing devices are more senior and would typically have a requirement for access to more highly classified information.

This area of portable computing devices is a risk area that is often overlooked by many organisations. They have developed policies with regard to the use of these devices, but these policies and controls have often not been reviewed with the change in use of the devices and technology.

There are a number of risk areas associated with the loss of these devices and the main ones are as follows:

- Loss of the physical asset and direct financial impact – replacement costs and user productivity loss
- Potential Information Security breach due to information stored on laptop
- Potential Information Security breach due to corporate remote access services installed on device that may have poor authentication requirements
- Compliance issues with regard to industry sector regulatory requirements or legislative instruments for the protection of data
- Technical support staff with network diagrams, security configurations and passwords etc.

A number of high profile laptop losses over the last 12 months have highlighted the impacts that the loss of information stored on these devices can have. Some of the worst examples relate to one of the "big-four" audit firms in the world. An auditor from this firm breached their own policy by having sensitive customer information on their laptop, which was not encrypted. The customer in this case was Sun Microsystems and the information on the laptop was personal information of a large group of employees, including Scott McNealy, the CEO. This information contained items such as Social Security Number, address, date of birth etc. This, and other laptops lost or stolen are alleged to have contained information not just on Sun employees, but also on those from Cisco, BP, IBM and Nokia (US). This information is like gold dust to the Identity Theft criminals. As a result of these breaches, free credit and identity management services have been offered to the affected employees to ensure that they do not suffer as a result of this loss.

A 2nd of the big four also revealed in the last months that an employee had left a Compact Disc containing the personal information of thousands of McAfee staff on an airplane. Once again, this data was unencrypted and free credit management services were provided to the staff in a pre-emptive move by the auditing firm.

We have also heard of hard disks being purchased on Internet based auction sites that are second user items. When the purchaser gets the hard disk and performs a data recovery on the disk, and sometimes this isn't even necessary, it is amazing what can be revealed. Some newsworthy discoveries have included the alarm system layout for celebrity footballer mansions, account details for international music stars and so on.

Having a simple policy in place can easily prevent all of these breaches, and that is that all portable-computing devices must be encrypted (completely). Depending on the classification of data stored on the device, it may be necessary to implement strong, multi-factor authentication to access the device.

When setting a policy such as this, it is vital to select an appropriate technical solution. There are many options to be considered ranging from encryption algorithms and credential management through to installation and central management options. It is also vital to consider the resources available to a party that may be interested in attempting to subvert the security controls that have been implemented.

In the future, Microsoft are promising that the Vista Operating System will incorporate strong file system encryption using a technology called BitLocker. This will integrate with a hardware security module, the TPM (Trusted Platform Microprocessor) that Intel and others are integrating on certain current and most planned motherboards. This is a secure chip implemented in hardware on the PC where the keys for encryption utilities such as BitLocker and other security information can be stored securely. It will not be accessible by MalWare running on a PC and can thus offer a secure storage area. Microsoft is claiming that BitLocker will be a stronger solution than the EFS (Encrypting File System) available today. Many PC manufacturers are integrating the TPM today, particularly on laptops and some of the 3rd party full-disk encryption utilities make use of it.

Similar solutions are available today for other platforms than the PC and laptop running a version of Windows. For instance, you can now purchase a solution from a disk encryption vendor that can install on the Windows XP platform, the Windows Mobile platform for PDAs and phones, and the Symbian mobile phone operating system. This makes it much easier for Information Security teams to implement and manage a consistent set of controls across an organisation.

As these devices get smaller and more powerful, they are also becoming easier to steal and more attractive to the thieves. There is a ready market available, unfortunately, for these stolen devices and that will fuel the thefts. We have heard of how people are now starting to use earphones other than Apple's trademark white iPod earphones as they are being assaulted to steal the iPod. iPods are increasingly being used to transfer data in and out of organisations due to their simplicity and capacity. When editing the Lord of the Rings, Director Stephen Jackson used a briefcase full of iPods to transfer digital images between New Zealand and the United Kingdom.

We have talked before about the risks of using the very convenient USB flash memory disks for the storage of confidential information. This is due to the fact that their owners on such a frequent basis lose them. They are also an extremely easy way for malicious employees to remove data from an organisation. It has been reported in the recent past the in the bazaars in the Middle East near American military bases, USB disks are for sale that contain classified military intelligence. This has resulted in American soldiers going into the bazaars to buy back the disks and prevent the information on them getting into the wrong hands. Again, these removable media should be covered in the selection process of a solution to encrypt PCs, PDAs etc.

A solution should also be investigated that can prevent any USB disks being introduced that are not approved for business purposes. These solutions can help prevent against the unauthorised removal of information from the organisation.

In summary, any portable computing device that is supplied to staff of an organisation must have appropriate data protection controls applied. The selection process of an appropriate solution must also include a Risk Analysis to determine the impact to the organisation, or others, of unauthorised access to the data. This Risk Analysis must also take into account what external, remote access this device can provide to an organisations internal networking infrastructure.

Contact Information

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com