Information Security Updates

Portable Storage Media

Issue 8

I. Background

Industry Story

University of Arizona Losses Drive Containing Personal Information on Thousands

The University of Arizona recently announced the loss of a hard drive containing the personal information on former students. The drive, holding information on individuals enrolled at the university between 1997 and 2008, contained names and Social Security numbers of over 8,000 former students. The drive was moved during the summer of 2010 to a new building and was discovered missing in October 2010.

According to the University of Arizona's Dean of Students Dr. Carol Thompson, the files and drive were always under supervision, even during the move. Thompson called the incident troubling. In a notice to the affected individuals, the university asks that the former students watch for signs of possible identity theft.

See this article:
http://www.adamdodge.com/esi/university_arizona_losses_drive_containing_personal_information_thousands

Key Benefit of Portable Storage Media

The emergence of external hard drives, USB sticks or even smart phones makes our work and life much easier. Portable storage media with large storage sizes and convenient connectivity interface allow students or staff to take their study and work wherever they go.

Key Risks of Portable Storage Media

Nevertheless, portable storage media poses a number of security threats to the university. Without adequate protection mechanism like authentication or encryption, portable storage media may bring significant risk of data theft or data loss. On the other side, improper use of protection mechanism (e.g. loss of decryption key) or device failure could deny the university from accessing important data timely.

Another common threat is the introduction of malware from portable storage media to the university's IT systems. Hackers may use social engineering techniques to manipulate users into connecting infected portable data storage devices to their desktop, laptop or even university's IT systems.

Related Article

Portable devices pose biggest risk to data security in 2011

The Digital Systems Knowledge Transfer Network has made this announcement that devices capable of storing data in a portable form factor, will allow cybercriminals the opportunity to exploit new security weaknesses in 2011. It is not just the data storage abilities of these devices but also the fact that they can connect to wireless networks that makes them vulnerable, according to Mr Dyhouse. He expects hackers to find new ways of hijacking the data being sent and received over Wi-Fi and Bluetooth, allowing criminals to act in a clandestine manner which is difficult to detect, while harvesting significant amounts of information. (http://www.backup-technology.com/5671/portable-devices-pose-biggest-risk-to-data-security-in-2011/)

Statistical Report

The threats posed by portable storage devices

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. (http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf)

Reference:
http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(C7C220BBE2D77410637AB17935C2BD2E)~PDSDSecurity-CIOPaper.pdf/$file/PDSDSecurity-CIOPaper.pdf

II. Management

In order to manage the risks associated with the use of portable data storage media by staff and students, while enjoying the benefits of greater mobility and flexibility, the Management should consider the following dimensions of security practice:

Policies and procedures

Policies and procedures should be developed to clearly outline the roles and responsibilities with respect to the use and management of portable data storage media for university's data.

1. Establish a portable data storage system security policy, which encompasses both university-issued and privately owned portable data storage media. This security policy should also be integrated into university's overall IT security framework and rigorously enforced.

2. Review and consequently revise or update the university's portable data storage system security policy, particularly in light of the availability of new data storage technologies, and in the wake of security incidents involving portable data storage systems.

3. Develop a set of handling procedures to cover the entire life-cycle of portable data storage devices, including acquisition, deployment, use, to disposal.

4. Limit or prohibit the connection of privately owned portable data storage devices to university's IT systems. For university's sensitive data, rigorous access control procedures should be implemented to prevent unauthorised data access, modification and leakage.

5. Consider establishing a centralised encryption key and password repository system to achieve efficient management of authentication information and avoid accidental loss of encryption keys or passwords

People

Applying security controls to counter the security risks caused by human mistakes and negligence is critical for securing the portable storage media used by university. Sufficient staff and student awareness and training programs should be offered by university to achieve the following objectives:

1. Identify and communicate roles and responsibilities of staff and students in securing their portable storage media.

2. Inform staff and students of the risks associated with the use of portable storage media and consequence when those threats are exploited by malicious parties.

Related Article

University Policy - Encrypting Mobile and Storage Devices

If you transport restricted University data, or data that is classed as "sensitive" under the Data Protection Act, on any mobile or storage device, be that a laptop, notebook, USB stick, or CD/DVD or similar, then that device must be encrypted. It is further recommended that any mobile or storage device containing restricted data that is only used within the University is also encrypted and/or locked away when the office is left empty in case of theft. (http://www.bris.ac.uk/infosec/uobdata/encrypt/device/)

Recent Incident

University Medical Centre Loses Flash Drive Containing Patient Information

The University of Rochester Medical Centre is working to notify patients after a doctor lost a flash drive containing patient information. The flash drive, contained the names, birth dates and diagnosis of some patients. Jeffery Powell, the URMC CIO, said they medical centre will being looking into encryption for all computers and flash drives. (http://www.adamdodge.com/esi/university_rochester_medical_center_doctor_loses_flash_drive_containing_patient_inforamtion)

Reference:
http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(C7C220BBE2D77410637AB17935C2BD2E)~PDSDSecurity-CIOPaper.pdf/$file/PDSDSecurity-CIOPaper.pdf

II. Management (cont'd)

3. Emphasise the importance of timely reporting on suspicious data leakage, data loss or data denial incidents to university's IT security team.

4. Educate users and administrators regarding the physical access control, acceptable use, permissible data storage devices, and security incident handling and escalation procedures in relation to portable storage media.

Technology

Whilst technical solutions cannot substitute for an integrated and comprehensive portable data storage security framework, a range of technologies or products can effectively reduce the level of risk exposure arising from the portable data storage devices, and mitigate the impact of security incidents when they occur.

1. Encrypt sensitive data residing on portable data storage devices using strong passwords or algorithm. For example, 8-character alpha-numeric password, RSA key encryption.

2. Alter the default settings of the university's IT system to prohibit automatic execution of applications residing on a portable data storage device upon connection.

3. Deploy and enable audit logging function that record connection of portable storage devices and data transferred between university IT systems and portable data storage media.

4. Block the ability to connect portable data storage media for university's IT systems holding sensitive data by disabling connection sockets on related desktops, laptops or servers.

5. Where possible, implement tiered connection states (i.e. no connection, read only data from the portable data storage media, read/write data to and from the portable data storage media) within university's IT systems based on the institutional imposed risk criteria.

6. Employ secured physical or logical destruction mechanism to enforce safe disposal of portable storage media.

Related Article

Security Trends in Mobile Devices

Recent mobile devices are based on standard operating systems, and have a huge range of functionality. However the altering of the PC-oriented operating systems for mobile use, being a new concept for manufacturers, associated security measures around data sitting or being transported on these devices are not fully mature or proofed.
A good example of a not fully matured security measure is the device encryption of the iPhone which implies that the data is stored encrypted. That is true however decrypting is as easy as powering on the device.
(http://www.datalossbarometer.com/14718.htm)

Statistical Report

Data Loss Barometer report – November 2010

Key Findings include: An overall downward trend (25%) in reported data loss incidents; The 'Malicious Insider' is a continuing threat; Portable media are still largely unencrypted; More people affected by Hacking than any other cause of data loss; Incidents involving a third party is more commonplace in the Government sector; and more records are lost or stolen within Financial Services than any other sector.
(http://www.datalossbarometer.com/docs/KPMG_Data_Loss_Barometer_-_Issue_3_-_November_2010.pdf)

Reference:
http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(C7C220BBE2D77410637AB17935C2BD2E)~PDSDSecurity-CIOPaper.pdf/$file/PDSDSecurity-CIOPaper.pdf

III. General Users

Care and Storage

Users should keep portable storage media with information related to university out of sight from other people to minimise the risk of theft. In addition, such media should not be left unattended at any time.

Where possible, users should utilise the security features of the portable storage media (e.g. USB stick with finger print recognition function) or security tools recommended by the university (e.g. data encryption software) to protect the information from unauthorised access or modification.

Important data stored on portable storage devices should be regularly backed up to designated file servers of the university.

Cleansing and Sanitisation

Portable storage media containing the university related information must be appropriately cleansed and sanitised after use and before disposal. If un-rewritable portable storage devices/media are used, such as CD and DVD, they must be destroyed either by a disintegrator, or by grinding, smashing or burning.

Lost or Stolen Portable Storage Media

Users must report to the IT Help Desk as soon as possible if a portable storage device containing information related to the university is lost or stolen. The IT security staff must be notified immediately and record the identification (e.g. serial number, type, asset register code) of the device, the physical appearance of the device and the details of the information stored.

Restriction

Unless specifically approved, users should not keep the university related information on privately owned portable storage media. On the other hand, data related to personal matters should not be kept on the portable storage provided by the university.

Conclusion

The convenience and flexibility of portable storage media increase the efficiency of university’s staff and students during their work and study. However, the security threats of data loss or denial cannot be ignored. To build a safe environment for using portable storage media, both the Management and general users should pay great attention to the establishment, enforcement and maintenance of necessary security measures.

Recent Incident

University of Nevada School of Medicine Computer Equipment Stolen

The University of Nevada, Reno is alerting current and former students over the loss of a USB drive containing student information. The drive contained the names and Social Security numbers on 16,000 students enrolled as freshman during the fall semesters between 2001 and 2007. In a letter to affected students, the University offers one year of free identity theft protection. While the university has no evidence that the information is being misused, the university asks anyone that notices fraudulent activity contact the university's police department. (http://www.adamdodge.com/esi/institutions/university_nevada)

Related Article

University of Missouri - Information Security Policy

University Departments should ensure compliance with appropriate University policies; ensure all electronic storage devices are processed by a professional IT staff person (or delegate approved by the ISO) before being transferred; and seek assistance from the central IT department if necessary.
University Employees must ensure that University data is removed from their personally owned electronic storage devices prior to leaving the University. Employees should seek assistance from professional IT staff to ensure adequate removal of electronic data. (http://infosec.missouri.edu/assets/device-disposal.html)

Reference:
http://security.tennessee.edu/pdfs/SMDBP.pdf
http://www.sandisk.com/media/226722/enterprise_whitepaper_endpointsecurity.pdf