Trusted Information Sharing Network
for Critical Infrastructure Protection

PORTABLE DATA STORAGE SECURITY INFORMATION FOR CIOs/CSOs

Best Before – November 2011[1]

Executive Summary

In today's business environment, managing and controlling access to data is critical to business viability and survivability, and to ensure corporate compliance with legal and regulatory requirements. Storing organisational data outside of the IT system in which it is being used has always been a source of risk, with the level of risk increasing significantly for valuable or sensitive information.[2]

Historically, a relatively small portion of an organisation's information holdings could be easily stored and removed on an individual item of media or portable device. However advances in data storage technology have meant that a larger portion of an organisation's information may reside in media or devices that can readily move in and out of an organisation's controlled security environment. Media and portable storage devices can also provide a vector by which malware or other undesirable content are introduced into enterprise IT systems.

This paper – developed by the IT Security Expert Advisory Group (ITSEAG), part of the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection[3] - provides information on the risks associated with portable data storage security systems, and a basic set of actions that your organisation can undertake to manage and respond to these risks. This paper does not cover mobile devices such as laptops. These issues are already addressed in another paper issued by the ITSEAG.[4]

---

[1] The IT security environment is highly dynamic, with threats and risks changing continuously. In this light, the 'Best Before' date represents a judgement on the useful lifespan of the good practice guidance and references contained in this paper.

[2] Portable media is also used for most off-site backup

[3] The TISN is the Trusted Information Sharing Network for Critical Infrastructure Protection where the owners and operators of critical infrastructure work together, sharing information on security issues that affect them. It provides a safe environment where industry and government can share vital information on critical infrastructure protection and organisational resilience. The TISN is made up of nine different business sector groups, called 'Infrastructure Assurance Advisory Groups', and two Expert Advisory Groups, which are overseen by the Critical Infrastructure Advisory Council (CIAC). For more information on the TISN, please see www.tisn.gov.au. The ITSEAG provides advice on IT Security problems identified by the nine Infrastructure Assurance Advisory Groups, as well as projecting emerging trends that have the potential to impact on all critical infrastructure sectors.

[4] The ITSEAG's Mobile Device paper can be accessed from: www.tisn.gov.au

November 2009

An Overview of Portable Data Storage Systems

Portable data storage systems include:

- **Data Storage Media**. These include media such as various types of media cards, optical disks and magnetic tape - used for the storage of data in digital form. These interface with an IT system via a reader device, which is generally specific to a particular type and format of media.

- **Devices with an ancillary storage function**. These encompass a variety of hand-held mobile devices[5], including 'smart' phones, personal digital assistants, digital cameras and media players which – in addition to their principal function[6] – have the capability to store significant quantities of data in a digital form. Often these devices also incorporate readers which can accept data storage media, as described above. These devices can be connected to enterprise IT systems via either cable or wireless means.[7] Whilst not generally considered portable devices, multifunction printers can also present a risk to organisations, as the information transmitted to the device will remain in the memory, and could be accessed by another party.

- **Data Storage Devices**. These are dedicated devices that are specifically used for the storage of data in digital form. This includes devices such as 'thumb' drives, desktop travel drives and external disk drives (using both magnetic and optical data storage technologies). In contrast to storage media – which require a reader mechanism – data storage devices can generally be connected to an IT system directly via cable with the appropriate connector, or in some cases via wireless connection.

Technological advances have dramatically increased the capacity, data transfer rate and ease of use of portable data storage systems – particularly with regards to connecting them to enterprise IT systems. These advances have also greatly reduced the cost and physical size of portable data storage systems. Indicative data storage volume and data transfer rates of typically commercially available portable data storage systems are outlined in **Table 1** below.

DEVICE TYPE	DATA STORAGE VOLUME	POTENTIAL MAXIMUM DATA TRANSFER RATE
Optical Disk	30 GB	54 MB/s
Media Card	32 GB	45 MB/s
Magnetic Tape Cartridge	1 TB	80 MB/s
Media Player	250 GB	60 MB/s
'Thumb' Drive	Up to 128 GB	30 MB/s
Desktop Travel Drives	Up to 500 GB	60 MB/s
External Hard Disk Drive	2 TB	3 Gb/s

Table 1 – Specifications of Indicative Portable Data Storage Systems[8]

These attributes make portable data storage devices an important business tool – in particular, for supporting an enterprise workforce that is mobile or working remotely. But these attributes can be a source of risk to enterprise IT systems.

---

[5] For a more general treatment of the risks associated with mobile devices, see the ITSEAG paper *Mobile Device Security: Information for CIOs/CSOs* (dated May 2009), available from: www.tisn.gov.au.

[6] These functions include interfacing with telecommunications services, personal information management, and playing games, music and/or audiovisual files.

[7] For an overview of the risks associated with wireless communications, see the ITSEAG papers on *Wireless Security* (dated October 2008), available from www.tisn.gov.au.

[8] The specifications in **Table 1** reflect generally available portable data storage systems as at July 2009.

Risks Arising from Portable Data Storage Systems

Key risks posed to the enterprise from portable data storage systems are as follows:

- **Loss and theft**. The generally small size of portable data storage systems makes them highly susceptible to loss or theft. If data stored on a portable data storage device is not encrypted then the data can be easily accessed. In the case of devices with an ancillary storage function, authentication controls for the device often do not – of themselves – provide protection for access to the data on the device. These devices can easily be disassembled to gain access to the data storage components, thereby providing ready access to the data.
- **Disposal**. When portable data storage devices are disposed of the risk of data being accessed by an unauthorised person remains, as data may still exist on the device. Data which has been manually erased from the device may still physically reside on the device until it is overwritten by new data. Software and hardware products that can recover erased data from a portable data storage device are readily available.
- **Data theft from IT systems**. Portable data storage systems provide a ready means by which valuable and/or sensitive data can be stolen from enterprise IT systems. The small size of portable data storage systems – particularly of data storage media – means that they can be moved in and out of an enterprise's controlled environment without attracting attention. Also, the ubiquity of consumer electronic devices with ancillary storage functions – such as media players – means that the theft of data can occur in plain sight, the apparent innocent use of such devices being used to conceal information theft. Also, as portable data storage systems often connect to enterprise IT systems via file systems – rather than via network connections – the use of these devices may not be detectable to IT security measures that are focused on protecting enterprise IT systems from external threats.
- **Data Denial.** The storage of corporate data on portable data storage systems – where not otherwise stored on enterprise IT systems – creates the risk that important data can be lost to the enterprise by accident or malicious act. Where data is held in encrypted form on a portable data storage system, there is the risk that users may lose or forget the key for decrypting the data, thereby denying it to the enterprise (even though it has not been destroyed). Similarly, disgruntled employees – whilst physically returning a portable data storage system to the enterprise – can deny the enterprise access to encrypted data by refusing to disclose their cryptographic keys.
- **Introduction of Malware**. Portable data storage systems can readily act as a vector for the introduction of malware – both deliberately and by accident – onto enterprise IT systems. The writers and exploiters of malware may use a variety of social engineering techniques to manipulate users into connecting infected portable data storage systems to enterprise IT systems, and to transfer the malware from the portable data storage system onto the enterprise IT system. Legitimate users may accidently introduce malware onto enterprise IT systems by connecting portable data storage systems that have been infected elsewhere (home, internet café, or other location outside of a controlled security environment) to enterprise IT systems.
- **Introduction of Unwanted Software or Data**. As distinct to malware, portable data storage systems may also act as a conduit for the introduction of unwanted software or data onto enterprise IT systems. This could include game or entertainment software that – whilst not actually damaging or illicit – misuses enterprise IT system resources and undermines corporate productivity. This could also include illicit or illegal content (such as pornography or illegally acquired copyrighted media content), with the consequent risk of reputation damage and/or the threat of prosecution for the enterprise from the authorities or the legal owners of the media content.

Protecting the Organisation

In order to manage the risks associated with the use of portable data storage systems within your organisation, you should consider the following dimensions of security practice:

- **People**. Applying security controls to counter people-related risks, such as the accidental installation of malware, is critical for protecting an enterprise's information and systems from threats arising from portable data storage systems. The awareness and training of staff is a critical factor in ensuring that technology and policy/procedural security controls are implemented.

- **Technology**. Whilst technical solutions cannot substitute for an integrated portable data storage system security policy, a range of technical actions can reduce the level of risk exposure arising from their use, and mitigate the effects of security incidents when they do occur.

- **Policies and procedures**. Policies and procedures need to be developed that outline clear roles and responsibilities with respect to the use and management of portable data storage systems within the enterprise across their entire life-cycle (acquisition, deployment, use and disposal).

Examples of specific controls across each of these areas are detailed in Table 2:

People
• Identify key roles and responsibilities with respect to portable data storage system security across their entire life cycle (acquisition, deployment, use and disposal). • Identify portable data storage system user groups, and the scope of each group's usage, to enable the evaluation and mitigation of risks arising from portable data storage systems. • Educate users and administrators of portable data storage systems regarding risks, physical control and accounting, acceptable use, permissible data storage, and response and reporting actions in the event of security incidents or loss of the portable data storage system.
Technology
• Encrypt sensitive data residing on portable data storage devices. • Enable authentication processes for connecting portable data storage systems to enterprise IT systems, so that only authorised users can connect approved portable data storage systems to the enterprise IT system, consistent with their respective user privileges. • Disable enterprise IT system default settings that allow applications residing on a portable data storage device system to execute automatically, upon their connection to an enterprise IT system. • Deploy and enable enterprise IT system logging tools that record connections, and data transfer between enterprise IT systems and portable data storage systems. • For enterprise IT systems holding particularly sensitive corporate data, physically block the ability to connect portable data storage systems by securing or disabling connection sockets on the enterprise IT system. • Where possible, enabled tiered connection states (no connection, read only data from the portable data storage system, read/write data to and from the portable data storage system) between enterprise IT systems and portable data storage systems, subject to enterprise IT system imposed risk criteria. • For portable data storage systems that have held particularly sensitive enterprise data, consider the secure physical destruction of the portable data storage system as the only authorised means for the

disposal of portable data storage systems deemed surplus to enterprise requirements.
Policies and Procedures
• Develop a plan covering the entire life-cycle of portable data storage systems (acquisition, deployment, use, and disposal). Risk assessments and security controls are easier to undertake and implement when the organisation approaches portable data storage system security in a holistic and systematic fashion. • Limit or prohibit the connection of privately owned portable data storage systems to enterprise IT systems. For particularly sensitive enterprise data – and where it is possible to implement rigorous access control procedures – consider an outright prohibition on the movement of privately owned portable data storage systems in and out of the enterprise's controlled security environment. • Establish a portable data storage system security policy, which encompasses both enterprise-issued and privately owned portable data storage systems. • Integrate portable data storage system security issues into the enterprise's overall IT security and physical security policies, and rigorously monitor and enforce them. • Review – and if necessary – consequently revise or update the enterprise'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. • Consider developing a centralised encryption key and password management register to gain the benefit of encryption and control its risks.

Table 2 – Potential Organisational Controls

Conclusion

It is vital that enterprises have appropriate protective measures in place to mitigate and respond to the security issues arising from portable data storage systems. This paper provides essential good practice guidance for identifying, managing and mitigating the risks associated with the use of portable data storage systems within the enterprise.

Portable data storage system security policies should ensure that portable data storage systems cannot be connected to enterprise IT systems without the knowledge and authorisation of IT management. In addition, security controls should remove the ability of users to unilaterally alter settings associated with portable data storage systems – and the means by which they are connected to enterprise IT systems – which have the capability to impact adversely on the enterprise's risk profile.

The security of portable data storage systems should be an integral, routine and continuous element of an enterprise's approach to securing its IT systems.

References

- Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual – Unclassified Version*, dated Sep09_rev1 http://www.dsd.gov.au/_lib/pdf_doc/ism/ISM_Sep09_rev1.pdf (Information Technology Security – Media Security section).

- US National Institute of Standards and Technology, *Guide to Storage Encryption Technologies for End User Devices, NIST Special Publication 800-111*, dated November 2007: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

- US National Security Agency, *Disabling Storage Devices*, dated March 2008: http://www.nsa.gov/ia/_files/factsheets/I731-002R-2007.pdf

- AS/NZS ISO/IEC 27001:2006 *Information technology - Security Techniques* http://www.standards.org.au/

Feedback Form

The ITSEAG is keen to ensure that its work meets the IT security information needs and expectations of the owners and operators of Australia's critical infrastructure. By completing and returning this feedback form on this publication: *Portable Data Storage System Security*, you can assist the ITSEAG to achieve this objective.

Question 1 – How relevant is the topic of this publication for you? (Tick one)

Not At All Relevant	Not Very Relevant	Somewhat Relevant	Relevant	Very Relevant

Question 2 – How useful was the content of this publication for you? (Tick one)

Not At All Useful	Not Very Useful	Somewhat Useful	Useful	Very Useful

Question 3 – Do you think that this publication could be improved? (Tick one)

Yes		If yes, please indicate here how this publication might be improved:
No		

Question 4 – To what industry sector does your organisation belong? (Answer in the box below)

Question 5 – What is your role within your organisation? (Answer in the box below)

When completed, please return this form by:

- **Email:** Scan this form and email to: ITSEAG@dbcde.gov.au
- **Fax:** Fax this form to (02) 6271 1827 (Attention: ITSEAG Secretariat)
- **Mail:** Mail this form to: ITSEAG Secretariat, Department of Broadband, Communications and the Digital Economy, GPO Box 2154, Canberra ACT 2601