Methods of accessing, transmitting, storing and disposing of confidential information in a secure way

Introduction

Information is a vital asset to the Council, which needs to be suitably protected from unauthorised access. The recent loss of information by high profile Government departments such as Her Majesty's Revenue and Customs (HMRC) has drawn significant attention to the suitability of information security measures applied to protecting information.

Purpose

The purpose of this document is to clearly define the information security measures appropriate for accessing, transmitting, storing and disposing of confidential information. To ensure the recommended security measures are appropriate the following will be taken into consideration:-

* Threats to the information

* Vulnerabilities

* Regulator requirements and

* Heightened media attention.

So what are the threats?

Information loss is typically associated with the actions of internal staff and threats are most commonly associated with the behaviour of those internal staff. The common types of threats are:-

* Loss or theft of storage devices

* Human error – actions of internal employees to third parties

* System malfunction or unforeseen effect of change – creation of a back door

* Malicious third parties – social engineering

Loss or theft of storage devices

As data storage has become highly portable (USB sticks, media players) and remote working has become the norm (using laptops) the loss or theft of these devices can result in huge amounts of information being lost.

Human error – actions of internal employees to third parties

Unintentional actions resulting in information loss can be related to:

* A lack of awareness training around the protection of confidential information

* Inadequate information classification schemes

* Poorly implemented or confusing controls (for example not providing any warning when sending an external e-mail)

* Pressure of work

* The increased use of open plan and shared office resources, such as printers and photocopiers, where confidential information may be left unattended.

System malfunction or unforeseen effect of change – creation of a back door

The unintentional creation of 'secret means of access' to a system can cause information to be leaked. This can also be associated with software problems or inappropriate systems controls.

Malicious third parties – social engineering

Third parties can be associated with an unintentional leak – for example where lost information is acquired by a malicious party to commit identity threat or commit fraud. Social engineering can also be deployed to encourage internal staff to leak information.

So what are the vulnerabilities?

The degree of vulnerability of information to threats varies according to a numbers of factors. These factors are largely associated with what is termed the 'information state', i.e. whether the information is being processed or changed; transmitted through some medium; or held within a storage mechanism.

Some of the vulnerabilities associated with these information states are listed below:

Examples Degree of vulnerability Typical strength of controls Notes

Processed

Contained within

Corporate System Low High Corporate systems are typically designed to protect information

Processed on an end

user device (e.g. PC) High Low End user environment tend to have weaker controls permitting information to be copied and subsequently leaked.

Processed by a third

party / outsourcer Medium Generic Outsourcers or third parties typically serve several clients and may have standard levels of controls irrespective of the value of the information.

Processed on a home

PC High Low Often shared by family and friends.

Transmitted

Through a private

network Low Medium Well designed private networks are unlikely to leak information.

By wireless High Variable Wireless can be poorly secured, particularly when outside of organisational control.

Across the Internet High Unknown Controls are unknown and information may be cached on public servers, where leakage can occur.

By the spoken word High Low Particularly when in public place, spoken information has few controls and can easily be overheard by third parties.

By courier or postal

service Variable Variable Outside of organisational control

Stored

In a corporate database Low High Typically well secured, but key staff (such as database administrators) may be susceptible to social engineering techniques to get them to leak

information.

Within a file system

(e.g. LAN) Variable Generic Often with a single level of control irrespective of the value of the information.

On paper High Low Easily copied (e.g. photocopied), removed or lost.

On a laptop High Medium Can be subject to ‘shoulder surfing’ when used in public places.

On a portable storage

device (e.g. USB stick

or media player) High Low Information is easy to copy. Additionally there is often a high likelihood of loss or theft.

On a home PC High Low Information stored on a home PC can be assessed by friends and family.

As waste waiting

disposal High Variable Equipment containing storage is often poorly controlled when being decommissioned or recycled. Paper waste awaiting shredding can be susceptible to theft (dumpster diving).

So what should we do in order to reduce the likelihood and the impact of any loss of information?

Educate staff and third parties about information leakage

Information often leaks from people who were authorised to access the information and hence we need to focus on better understanding of information leaks and educating staff to help reduce the incidents.

Delivering the right message on information leakage to employees is often difficult. All too often the message delivered is perceived as “We don’t trust you – therefore we’re going to lock everything up”.

There should be reluctance to create a corporate culture of secrecy and a balance needs to be established between protecting information and sharing it for business benefit.

Education should also extend to third parties where they are handling high value information – and they should be under a contractual obligation to maintain confidentiality of information.

Identify environments that may be susceptible to information leakage

We need to identify the environments that are most likely to suffer information leakage so that resources can be prioritised accordingly.

Techniques for identifying susceptible environments include business impact analysis, independent auditing of controls and root cause analysis of incidents involving information leakage.

Classify information in accordance with its level of confidentiality

In order to protect the information correctly we need to understand the value of it so that resources can be targeted at those that have the highest likelihood of causing harm if leaked.

There are four techniques to help us in the implementation of an agreed information classification scheme

* Label information

* Train staff

* Maintain an inventory and

* Establish contracts

Ensure general controls include information leakage considerations

Information leakage is not a new incident type, but there are new threats (e.g. loss of USB devices, remote working and the use of open plan offices) that can contribute to this type of incident. General security controls should be reviewed in the context of these new threats to ensure that they operate effectively.

Consider the deployment of technology solutions for high value or sensitive information

There are many products on the market that can help the Council to prevent information leakage, ranging from infrastructural level products that integrate into the whole organisation, to niche point solutions, such as laptop or USB encryption. The cost effectiveness of these solutions needs to be aligned with the value and sensitivity of the information.

Be prepared to respond to information leakage incidents

Unintentional (or indeed deliberate) leakage of information that is sensitive or has a high value is likely to result in some sort of incident. Business continuity and incident response procedures should include information leakage as a possible scenario and a response should be planned and rehearsed.

Methods of transmitting confidential information to third parties

Transmission Method Degree of Vulnerability Recommended security control

By the spoken word High Information must only be disclosed to a third party where the possibly of someone overhearing is not possible, i.e. a secure meeting room.

By courier or postal

service High Information exchanged on paper must be:- * sent in a sealed envelope using a Council approved courier service or the postal services secure delivery method (recorded delivery) and * the third party must be required to sign for the envelope. Sending a file created using any of the Microsoft Office 2002 products or later must be:- * Encrypted before it is transferred to a removable media device such as a CD, or memory stick etc. * The encryption types (available on Microsoft Office products 2002 or later) acceptable for encrypting the file with a key length of 128 bits is as follows:- o RC4, Microsoft Enhanced Cryptographic Provider o RC4, Microsoft Enhanced DSS and Diffie Hellmann Cryptographic Provider o RC4, Microsoft RSA and AES Cryptographic Provider

o RC4, Microsoft Strong Cryptographic Provider * The encrypted removable media device must be sent in a sealed envelope using a Council approved courier service or postal services secure delivery method where the third party must sign for the envelope. * A file created using an earlier version of Microsoft Office 2002 will not have this security encryption function and should not be sent unless the file can be sent securely. The recommendation for anyone using an earlier version is to upgrade to the Microsoft Office 2002 or greater.

Across the Internet High * Electronic information should not be included in e-mail text or attachments unless done in an encrypted environment. * E-mail attachments which are created using any of the Microsoft Office 2002 products or later must comply with the same rules as for sending information via courier or the postal service. * E-mail attachments not

created using any of the Microsoft Office 2002 products or later should not be sent without consulting the IT security team.

Fax to Fax High * Fax transmissions over phone lines (fax to fax) are secure if appropriate safeguards exist when faxing information. Safeguards such as making sure the recipient's fax number is correct and the recipient does not

leave the fax in an unsecured area. * Fax transmissions involving computer networks (fax to computer, computer to fax, computer to computer) are not secure and should be discussed with the IT security team first.

Storage of Confidential Information

Departments must actively work to remove information from electronic files, databases, images, and paper documents. Historical files, databases, documents, and images containing information may be maintained provided access to them is limited and secure.

* Information should not be stored on a local workstation, laptop, floppy disk, CD/DVD, personal digital assistant (PDA), USB flash drive, or any other portable storage device. If storing information on such a device is necessary, the information must be properly protected and the device must be physically secured.

* Computer applications requiring the information must store the information on a secure network server. Encryption adds another layer of security.

* Servers, tapes, disks, back-ups, and other electronic storage devices containing the information must reside in secure physical locations.

* Documents and forms containing the information must be stored in secure drawers/ cabinets with appropriate security.

* Anyone working with paper that contains the information must take steps to secure that information.

Disposal of Confidential Information

As confidential information is eliminated from the normal course of business, departments must follow these standards for secure disposal.

* Prior to disposal, steps must be taken to destroy portable electronic storage devices, floppy disks, and CD/DVDs containing the information.

* Prior to recycling or disposal, desktop, laptop, and server disks containing data must be erased (scrubbed) using current industry standards.

* Paper documents containing the information should be shredded locally or disposed of in accordance with agreed confidential document destruction policies.