



Preventing Data Leakage

A defence-in-depth approach to mitigate against the loss of sensitive data.

July 2009

Loop Technology, 2009
ABN 76 114 448 225
© All rights reserved.

No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior permission in writing from the owners.

First published and distributed in January 2008.

Table of Contents

1. Executive Summary	3
2. Introduction	4
2.1 Background	4
2.2 Purpose	4
2.3 Document Structure	4
2.4 Definitions	4
2.5 References	4
3. Threats	5
3.1 Lost/Stolen Device	5
3.1.1 Likelihood	5
3.1.2 Impact	5
3.1.3 Mitigation	5
3.2 Insider Attack	6
3.2.1 Likelihood	6
3.2.2 Impact	6
3.2.3 Mitigation	6
3.3 Network Intrusion	7
3.3.1 Likelihood	7
3.3.2 Impact	7
3.3.3 Mitigation	7
3.4 Accidental Loss Of Data	8
3.4.1 Likelihood	8
3.4.2 Impact	8
3.4.3 Mitigation	8
4. Potential Controls	9
4.1 Information Security Policy	9
4.2 Access Control Policy	9
4.3 Data Classification Scheme	10
4.4 Acceptable Use Policy	10
4.5 Security Awareness Campaigns	10
4.6 Human Resource Security	11
4.7 Technical Access Controls	11
4.8 End Point Encryption	11
4.9 Penetration Testing	11
4.10 Logging And Auditing	12
4.11 Incident Handling Strategy.....	12
5. Loop Technology	13
Appendix A: Mapping Risks To Controls	14

1. EXECUTIVE SUMMARY

“The massive computer data breach at TJX may be worse than expected: At least 94 million Visa and MasterCard accounts — nearly double the previous estimate by the retailer — could have been exposed, new court files say... The depositions say fraud-related losses of Visa cards range from \$68 million to \$83 million and will rise as thieves continue to use data from compromised cards.”

Data leakage is the loss of sensitive information through the edges of an organisation via emails, Web or portable media. It is a complex issue that requires organisations to take a defence-in-depth approach to its prevention. The four major threats related to data leakage, that are applicable to all organisations are:

- Lost/Stolen Devices;
- Insider Attack;
- Network Intrusion; and
- Accidental Loss of Data.

These threats are discussed further in [Section 3](#).

Once an organisation understands the nature of the threat against them, they need to establish effective mitigation strategies.

To establish which controls are appropriate, an organisation should consider all possible controls. Some controls that may assist in the prevention and detection of data leakage are:

- **Information Security Policy.** A Policy that demonstrates management commitment to information security and sets out clear security objectives.
- **Access Control Policy.** A Policy that defines who has access to information and how the access is controlled.
- **Data Classification Scheme.** A scheme that categories data in terms of its value, legal requirements, sensitivity and criticality to the organisation and which can be used to define levels of protection.
- **Acceptable Use Policy.** A Policy document that establishes what is and is not acceptable use of an organisation’s assets.
- **Security Awareness Campaigns.** A campaign that provides education on an organisation’s Security Policy and helps employees understand how the Policy protects vital assets.
- **Human Resource Security.** Procedures that define employee, contractor and third-party user security responsibilities prior to, during and post employment. These include definition of security roles and responsibilities, background checks performed on new employees, awareness training, and exit procedures.

- **Technical Access Controls.** Controls that can prevent sensitive information from easily being emailed or copied onto an unauthorised device.

- **End Point Encryption.** Tools that will encrypt sensitive information when it is moved from your network or system to a portable media device such as a USB drive or portable hard drive.

- **Penetration Testing.** Testing that will highlight any existing network vulnerabilities which can be exploited to cause damage to the organisation. These vulnerabilities can vary from eavesdropping of communications to obtaining account numbers, passwords etc to modification of information and denial of service attacks.

- **Logging and Auditing.** Mechanisms that record access to sensitive material and systems which can be reviewed in a timely manner.

- **Incident Handling Strategy.** A strategy that defines how incidents are processed when detected and dealt with in a timely manner.

These potential controls are discussed further in [Section 4](#).

[Appendix A](#) contains an easy to reference table mapping the data leakage threats to the potential controls.

Loop Technology provides a range of security services that can address the threat of Data Leakage by implementing various controls designed to minimise the risk. Through the combination of Information Security Policy, procedures and tools, Loop can help an organisation identify the risk associated with data leakage and minimise both the likelihood and the impact of this risk by implementing appropriate controls.

2. INTRODUCTION

2.1 BACKGROUND

Data leakage is the loss of sensitive information through the edges of an organisation via emails, Web or portable media. It is a complex issue that requires organisations to take a defence-in-depth approach to its prevention.

In a recent Deloitte's Global Security Survey of those organisations that experienced a security breach, 49% indicated they had experienced an internal attack. Of these 18% related to the leakage of customer data. The use of mobile and wireless technology has exacerbated this problem which has put pressure on organisations to try and protect company and client data.

2.4 DEFINITIONS

Control	Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be administrative, technical, management, or legal in nature.
Data Leakage	The loss of sensitive information through the edges of an organisation, such as emails, internet or portable media.
Information Security	Preservation of confidentiality, integrity and availability of information.
Sensitive Data	Any data within an organisation that is vital to the organisation's core business.
Threat	A potential cause of an unwanted incident, which may result in harm to an organisation.
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats.

2.5 REFERENCES

Ref	Details	Date
1.	AusCERT, Australian High Tech Crime Centre, Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australian Police, Tasmania Police, Victoria Police and Western Australian Police, 2006 Australian Computer Crime and Security Survey.	2006
2.	Computer Security Institute, 2007 CSI/FBI Computer Crime and Security Survey.	2007
3.	U.S. Secret Service and CERT Coordination Center, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors.	May 2005
4.	Carnegie Mellon University (CyLab), Preventing Insider Attacks: Lessons Learned from Actual Attacks.	Nov 2006
5.	Carnegie Mellon University (CyLab), Common Sense Guide to Prevention and Detection of Insider Threats (2nd Edition) V2.1.	July 2006
6.	Proofpoint and Forrester Consulting, Outbound Email and Content Security in Today's Enterprise.	July 2007
7.	Defence Signals Directorate (DSD), ACSI 33 - Australian Government Information and Communications Technology Security Manual.	2006
8.	Deloitte 2006 Global Security Survey	Oct 2007

2.2 PURPOSE

This paper discusses the major threats associated with data leakage and presents a selection of practical controls for organisations to consider when attempting to prevent and detect data leakage. It looks at how organisations can establish what threats are relevant to their business, and includes guidance on how to implement controls appropriate to their environment.

2.3 DOCUMENT STRUCTURE

This document contains the following sections:

- **Threats.** This section presents the major threats that can result in data leakage. It also discusses the likelihood, impact and mitigation strategies associated with the threats.
- **Potential Controls.** This section discusses the potential controls organisations can implement to mitigate data leakage threats.
- **Appendix A:** Mapping of Threats to Controls. This appendix contains an easy to reference table mapping the data leakage threats to the potential controls.

3. THREATS

When assessing an organisation's risks, it is important to establish the likelihood of a threat eventuating, as well as its potential impact. A threat's likelihood and impact will vary between organisations; however the factors to consider when assessing risks and selecting controls to mitigate risks, are the same. The following section looks at the four threats related to data leakage that are applicable to all organisations:

- Lost/Stolen Devices;
- Insider Attack;
- Network Intrusion; and
- Accidental Loss of Data.

3.1 LOST/STOLEN DEVICE

Increased usage and functionality of portable electronic devices such as USB keys, PDAs and Blackberries, coupled with a growing mobile workforce has resulted in many employees storing and processing large amounts of sensitive data in devices that can be easily lost or stolen. As a result, organisations need to be aware of the threats associated with the use of portable electronic devices.

3.1.1 LIKELIHOOD

The 2007 CSI/FBI Security Survey found 50% of the organisations surveyed experienced laptop and mobile device theft. These results are reflected in Australia. The 2006 Australian Computer Crime & Security Survey reported 58% of organisations surveyed experienced laptop theft in the last 12 months. These statistics suggest that organisations utilising portable electronic devices have a significant likelihood of this threat eventuating.

3.1.2 IMPACT

Considering the diversity of portable electronic devices available, the possible impacts on an organisation can vary significantly. Some factors that should be considered when assessing the impact of a lost or stolen device are:

- Cost to replace the device;
- Quantity and type of information stored on the device; and
- Access the device has to the organisation's network/s.

3.1.3 MITIGATION

In most organisations, attempting to reduce the likelihood of this threat occurring through discouraging or preventing employees from utilising these devices is not only unrealistic, but can negatively impact productivity. However, it is realistic to reduce the likelihood through a practical **Acceptable Use Policy**, coupled with a comprehensive **Security Awareness Campaign**. Running security awareness sessions that highlight the threats and impacts of mobile devices and discouraging unsafe practices (such as leaving a device unattended) are likely to decrease the chance of a device being lost or stolen.

It is also possible to reduce the impact of a device being lost or stolen through technical controls. Some recommended technical controls include:

- **End Point Encryption**. Encrypt sensitive information on the device using a hard disk encryption product.
- **Technical Access Control**. Implement controls that prevent sensitive information from easily being copied onto unauthorised portable devices and media.

Where possible, organisations should remove additional or unnecessary functionality from the device.

In conjunction with the technical controls, it is essential that organisations have an **Incident Handling Strategy** in place to ensure these incidents are detected and dealt with in a timely manner.

These controls are discussed further in **Section 4**.

3.2 INSIDER ATTACK

An Insider Attack encompasses any malicious activity inside an organisation's network that has or had any level of authorised access to the network. Malicious insider activity can be categorised into three types :

- **Insider Sabotage.** A current or former employee or contractor intentionally misuses authorised access in an attempt to harm the organisations, employees, data, systems, reputation or operations.
- **Fraud.** A current or former employee or contractor obtaining information or services from the organisation unjustly through deception.
- **Theft of Information.** A current or former employee or contractor stealing sensitive information from the organisation.

The motivations for insider attack include:

- Disgruntled former employee;
- Seeking revenge for a negative event; and
- Expecting financial gain.

It should also be noted that some perpetrators of successful insider attacks are unaware that their behaviour is illegal.

3.2.1 LIKELIHOOD

There seems to be varying opinion about the prevalence of successful Insider Attacks. The CSI/FBI Security Survey found a slight decrease in the percentage of perceived losses due to insider attack; however it could be argued that Insider Attacks are difficult to detect. Regardless of its prevalence, the likelihood of an insider attack eventuating varies based on several factors. When attempting to establish the likelihood of an insider attack, organisations should consider:

- Value of information outside the organisation;
- Staff turn over and satisfaction levels; and
- Number of technical staff.

Information from previous insider attacks gives some indication of trends that can help organisations establish the likelihood of an attack. The US Secret Service and CERT Study found the majority of Insider Attack cases were executed by former employees, with a significant majority (86%) found to be employees in technical positions.

3.2.2 IMPACT

Given the potential knowledge of an insider, the impact of a successful attack could be devastating to an organisation. The most significant consequences include major financial impact due to loss of Intellectual Property and damage to public/corporate reputation through disclosure of sensitive information to the public.

3.2.3 MITIGATION

The diversity, nature and motivation of Insider Attacks makes establishing mitigation strategies a daunting task. Some controls that will assist in reducing the likelihood of an Insider Attack are:

- **Acceptable Use Policy.** Establish and communicate what is and is not acceptable use of electronic equipment and corporate assets.
- **Access Control Policy.** Document and implement a need-to-know access strategy and ensure separation of duties to reduce the chances of an individual employee modifying critical system configurations.
- **Logging and Auditing.** Log all access to sensitive material and systems. Ensure these logs are reviewed in a timely manner.
- **Human Resource Security.** Perform stringent background checks on employees and ensure exit procedures include termination of an employee's access quickly after they have left the organisation.
- **Technical Access Controls.** Implement controls that prevent sensitive information from easily being copied onto unauthorised devices.

The controls discussed above can assist an organisation to reduce the likelihood of the threat occurring; however it is also important to take steps to reduce the impact if the threat eventuates. Unlike losing a piece of physical equipment, data loss/theft can be difficult to detect. Stringent **Logging and Auditing** procedures will not only assist in the prevention of attacks, they will also decrease the chance of an attack going undetected. Furthermore, implementing **Technical Access Controls** that prevent sensitive information from easily being emailed or copied will reduce the amount of data that can be removed from the organisation and thus reduce the impact of a successful attack.

It is also suggested that regular backup procedures and a documented business continuity plan will also help reduce the impact if this threat eventuated.

These controls are discussed further in [Section 4](#).

3.3 NETWORK INTRUSION

The threat of network compromise encompasses any intrusion on the network by an attacker. There are two major kinds of attacks that organisations need to be aware of:

- **Unsophisticated Hacker Attack.** These attacks are orchestrated by inexperienced, malicious hackers who use programs and scripts developed by others to attack systems. Known colloquially as “Script Kiddies” their objective is usually to try to impress their friends or gain credit in underground hacker communities. They generally select targets at random by scanning the internet for a specific weakness.
- **Targeted Attack.** These attacks are usually orchestrated by experienced, malicious hackers and crackers with a defined objective. They usually involve malware and are aimed exclusively at a specific organisation or small subset of organisations. Increasingly the attacks are perpetrated by organised crime to achieve financial gain.

Regardless of the type of attack, there are a variety of ways to penetrate and exploit a network. Some common exploits utilised by attackers include:

- Null or default passwords on network hardware;
- Default shared keys;
- IP Spoofing;
- Eavesdropping;
- Application vulnerabilities; and
- Denial of Service (DoS) attacks.

3.3.1 LIKELIHOOD

Network Intrusion attacks pose a threat to all networks connected to the internet, regardless of its location and value. The 2006 Australian Computer Crime & Security Survey reported 63% of respondents viewed exploitation of unpatched or unprotected software vulnerabilities as contributing to electronic attacks which harmed the confidentiality, integrity or availability of their network data or systems in the last 12 months.

The CSI/FBI Security Survey found almost one-fifth of survey respondents who suffered one or more kinds of security incidents further said they had suffered a ‘targeted attack’. Unfortunately the survey did not provide details regarding the industries of the organisations attacked; however it is unlikely that these attacks were distributed evenly across different industries. The likelihood of a targeted attack on an organisation’s network is dependant on several environmental factors. When establishing the likelihood of an attack, organisations should consider:

- Connections to untrusted networks;
- Type and motivation of attackers likely to target the organisation;
- System patch levels; and
- Value of sensitive information to a potential attacker.

3.3.2 IMPACT

The impact of a successful Network Intrusion can include:

- Financial loss;
- Damage to reputation;
- Negative media publicity;
- Disruption to networks and services; and
- Permanent loss or corruption of sensitive information.

3.3.3 MITIGATION

When mitigating Network Intrusion it’s important to remember that the majority of intruders are looking for an easy target, therefore keeping system patches up-to-date and ensuring default passwords are changed will reduce the likelihood of a successful attack. Regular **Penetration Testing** will highlight any existing network vulnerabilities which when remediated will help prevent the organisation from being an easy target.

A comprehensive approach to **Logging and Auditing** coupled with a clearly defined **Incident Handling Strategy** will help lessen the impact of any successful Network Intrusion.

These controls are discussed further in **Section 4**.

3.4 ACCIDENTAL LOSS OF DATA

One of the most difficult threats for an organisation to measure is accidental data loss through human error. Technical mistakes and accidents in the workplace can happen in a variety of ways, for a variety of reasons. They range from a minor error, such as a mislabelled email, to a potentially major error, such as a failure to initialise a backup script. The 2007 Outbound Email and Content Security in Today's Enterprise survey found that nearly 1 in 5 outgoing emails contains content that poses a legal, financial or regulatory risk (the most common form of non-compliant content is email that contains confidential or proprietary information) and more than half of the organisations surveyed say that it is 'important' or 'very important' to reduce the legal and financial risks associated with outbound email in the next twelve months.

Human error is a fact of life; however being aware of the likelihood and impact of potential errors and implementing appropriate controls will enable an organisation to protect itself from embarrassing situations that can damage its reputation.

3.4.1 LIKELIHOOD

Email has emerged as the most important tool for communication in the modern business environment, therefore evaluating email security is a logical place to start when looking to establish the likelihood of an accidental loss of data within a company. The 2007 Outbound Email and Content Security in Today's Enterprise survey found more than a third of the companies surveyed investigated a suspected email leak of confidential or proprietary information in the past 12 months.

3.4.2 IMPACT

Similar to the impact of a deliberate Insider Attack, accidental loss of data can result in significant financial losses through the disclosure of Intellectual Property (IP) and damage to corporate reputation. An accidental disclosure of financial information can lead to regulatory penalties and/or legal action.

3.4.3 MITIGATION

The statistics suggest that controlling and monitoring an organisation's email server can go a long way to reducing the likelihood and impact of accidental data loss eventuating. Some suggested controls for reducing data leakage through accidental loss of data are:

- **Acceptable Use Policy.** Establish and communicate what is and is not acceptable use of electronic equipment.
- **Logging and Auditing.** Log all access to sensitive material and systems. Ensure these logs are reviewed in a timely manner.
- **Data Classification Scheme.** Ensure that sensitive data is recognised and appropriately protected. Sensitive emails should be identified and possibly encrypted.
- **Technical Access Controls.** Implement controls that prevent sensitive information from easily being emailed or copied onto an unauthorised device. Content filtering and encryption are examples of such controls.
- **Security Awareness Campaigns.** Communicating employee responsibilities and what is considered acceptable use will greatly reduce the chances of employees accidentally sending or losing sensitive data outside the organisation.

These controls are discussed further in [Section 4](#).

4. POTENTIAL CONTROLS

A control is a method to treat or mitigate the effect of a threat to security through policies, procedures, guidelines, technical practices or organisational structures. Once an organisation has an understanding of the risk applicable to their business, they can select appropriate controls to help mitigate the risk. This section details a list of potential controls that organisations can implement to minimise the likelihood and impact of the threats associated with data leakage.

Accurately assessing the risk of a business decision is an intrinsic part of a proactive approach to IT security. It allows organisations to make informed decisions regarding the security within their organisation. To ensure that risk assessments are comparable and repeatable, organisations should have a documented risk assessment methodology. At a minimum this methodology should define the criteria for accepting risk and the acceptable risk level for an organisation.

Once a risk assessment methodology is in place, an organisation can begin a risk assessment. The AS/NZS 4360:2004 Risk Management standard states that the risk assessment methodology should:

1. Establish the Context;
2. Identify Risks;
3. Analyse and Evaluate Risks;
4. Examine Risk Treatment Options;
5. Select Controls for the Treatment; and
6. Gain Management Approval for Residual Risk.

This process involves a monitoring and review of risks on a regular basis i.e. quarterly, yearly. The results of risk assessment need to be communicated to management.

For more advice on how to perform an organisation wide risk assessment, please refer to ISO27001.

4.1 INFORMATION SECURITY POLICY

The main purpose of a documented and maintained Security Policy is to demonstrate management commitment to information security and set out clear security objectives to ensure the confidentiality, integrity and availability of information. It is an important cornerstone for an organisation that guides security decisions. Without a documented Security Policy, making consistent and smart security decisions is extremely challenging.

A good Security Policy includes:

- A defined scope;
- A clear definition of user responsibilities (including Administrators);
- A realistic approach to implementing and maintaining security;
- A balance between security and productivity;
- Can be enforced through audit; and
- Is supported by management.

When developing and implementing any security controls it is important to always apply the defence-in-depth approach, as no single policy, procedure or technical control will secure an organisations information.

ISO 27002 provides guidelines on what should be contained in a Security Policy, and is a good starting point for any organisation looking to develop a Security Policy for the first time.

4.2 ACCESS CONTROL POLICY

The main purpose of an Access Control Policy is to define how information dissemination should be controlled. Like all policies it should consider the applicable standards, industry regulations and/or contractual obligations. A comprehensive Access Control Policy should address:

- General User Access. This should define user ID and password requirements, the authorisation process, how the need to know principle is enforced and any conditions of access.
- Administrator Access. This should cover all the areas listed in General User Access, any additional authorisation requirements as well as address separation of duties.
- Removal/Modification of Access. This should detail the process for removing and modifying employee access.
- Auditing of Access Privileges. This should address how regularly general and administrator access should be reviewed.

This policy should also take into consideration the organisations Data Classification Scheme.

4.3 DATA CLASSIFICATION SCHEME

A Data Classification Scheme allows organisations to apply protective security measures to information based on value and risk acceptance. An effective scheme provides information confidentiality, integrity and availability. Organisations that are looking to implement a Data Classification Scheme should:

1. Identify information sources that need to be protected;
2. Define Classification levels such as Secret, Confidential, Internal, Public;
3. Separate the information into groups that require similar protection (classification levels);
4. Establish protective measures (these are usually technical and should address authentication, encryption and administrative controls);
5. Map protective measures to classification levels.

Some examples of high-risk data might include:

- Customer or employee information with names, addresses, tax file numbers and other identity-related information;
- Customer lists that could be used by a competitor for poaching clients;
- Trade secrets and intellectual property;
- Financial information not yet released to public;
- Pricing data;
- Credit card data such as the Primary Account Number (PAN).

The above steps should not be viewed as a once-off solution to establishing a Data Classification Scheme. They should be used iteratively and an independent evaluation process should be implemented.

NOTE: The classification levels established for data classification can be included in an organisation's Security Policy; however it is recommended that any protection mechanisms be documented separately, in a System Security Plan or Data Classification Scheme.

4.4 ACCEPTABLE USE POLICY

An organisation's Acceptable Use Policy should provide guidance to employees to ensure that they are aware of the boundaries surrounding use of the organisation's systems. Specifically, it should define what the organisation views as Intellectual Property (IP) and provide guidance on:

- Reasonable personal use of the systems;
- Opening unknown emails and attachments;
- Creating secure passwords;
- Installing new programs;
- Using portable electronic devices; and
- Posting of employees email addresses to newsgroups.

It should also detail what is considered unacceptable use, as well as authorisation for monitoring and enforcement of the policy.

NOTE: For an Acceptable Use Policy to be effective, it is imperative that it is communicated to all employees through a Security Awareness Campaign.

4.5 SECURITY AWARENESS CAMPAIGNS

The 2006 Australian Computer Crime & Security Survey highlighted that a need to change users' attitudes and behaviour regarding computer security practices was again the most common challenge cited by organisations in 2006 (60% in 2006 compared to 61% in 2005 and 65% in 2004). A successful Security Awareness Campaign should not only provide education on an organisation's Security Policy but should help employees understand how the policy protects vital business assets, including themselves.

To protect against data leakage, a Security Awareness Campaign should cover:

- Acceptable use (portable devices, desktops, email, etc);
- How to classify and protect data;
- How to identify social engineering;
- Employee responsibilities; and
- Incident reporting procedures.

A comprehensive employee training regime should include an initial security awareness session with new employees and compulsory refresher sessions. Organisations should also consider online resources and training for off-site employees.

4.6 HUMAN RESOURCE SECURITY

Implementing security controls around Human Resource processes will ensure employees understand their responsibilities – while reducing the risk of theft, fraud or misuse of facilities. Human Resource Security can also assist the Human Resource department in determining suitability of candidates for specific roles within an organisation through the definition of roles and detailed screening processes. Chapter 8 of ISO 27001 provides a comprehensive list of controls for organisations looking to implement secure human resource security practices. Possible controls include:

- Defined roles and responsibilities;
- Screening potential employees;
- Terms and conditions of employment;
- Awareness training; and
- Exit procedures.

4.7 TECHNICAL ACCESS CONTROLS

Several companies have released products that place technical controls on sensitive data to prevent it from leaving the organisation. There is a diverse range of products that can provide multi-layer protection of information in a broad range of environments. Depending on an organisations business requirements and budget, technical access controls can be implemented to:

- Lock down access to information on a file sever, database or system;
- Restrict usage of sensitive data, for example prevent the ability to print, rename or copy sensitive data onto removable media;
- Block the sending or forwarding of sensitive emails and memos outside the organisation;
- Track the movement of sensitive information through the network; and
- Log the access and modification of information.

Prior to implementing any technical access controls, organisations should have an understanding of their requirements surrounding protection of sensitive information. They need to understand the volume and nature of the data, as well as the business requirements to access and communicate the information.

4.8 END POINT ENCRYPTION

End point encryption products which encrypt a device's hard disk are available for portable electronic devices and laptops. When establishing the requirements for an end point encryption product, organisations should consider:

- Full or partial disk or flash memory encryption;
- Type of encryption used; and
- Active memory encryption.

Implementation of end point encryption needs to be supported by a data encryption policy and security awareness training.

NOTE: For Australian Federal Government Agencies, ACSI 33 has clear cryptographic standards that must be adhered to.

4.9 PENETRATION TESTING

Penetration tests are a specialised method of evaluating the security of a specific network or system by simulating an attack by a malicious user. They enable organisations to understand the technical vulnerabilities that may exist and can be used in conjunction with a risk assessment to establish the organisation's security posture. A standard penetration test will usually consist of an information gathering phase, an automated vulnerability scan and the manual verification of suspected vulnerabilities. Prior to conducting the test, an organisation should ensure the following is documented:

- Testing scope and objective,
- Rules of engagement;
- Agreed time windows for scans (preferably outside of core business hours); and
- Non-disclosure agreement.

4.10 LOGGING AND AUDITING

The main purpose of logging and auditing on a network is to detect unauthorised information processing activities; however effectively striking a balance between limited amounts of log management resources and the growing supply of log data is challenging. There are several Security Information and Event Management (SIEM) tools available that can assist organisations with the management of their log data, however before an organisation can select the SIEM tool that is appropriate to their business requirements they need to have a Logging Standard in place.

A Logging Standard should be based on risk analysis and applicable legislation or standards. It should provide a baseline that covers the following areas:

- Log Generation (including mandatory attributes and events).
- Log Monitoring (including filtering, integrity checking, automated alerts and reporting).
- Log Storage (including rotation, archiving, protection and disposal).

NOTE: Organisations with Data Classification Schemes should follow the Scheme's guidance on how to appropriately protect and dispose of log information. Once an organisation has established their Logging Standard, they should evaluate the potential SIEM tools available. This evaluation process needs to consider the tools functionality in conjunction with the network architecture and any resource limitations.

4.11 INCIDENT HANDLING STRATEGY

Establishing an effective strategy for identifying and responding to incidents in a timely manner ensures that corrective action can be taken to lessen the impact on an organisation.

A comprehensive strategy for handling incidents should include the following procedures:

1. Identifying the incident. The identification process should include monitoring vulnerability advisories, reviewing logs and ensuring staff have the ability to report an incident.
2. Investigating and classifying the incident. An important aspect of identifying an incident is to classify its severity to ensure it receives the appropriate level of attention.
3. Responding to the incident. The response process could include isolating the affected computer or network, scanning any connected system for malicious content, blocking the attacking IP address, updating anti-virus software and/or advising users of the compromise.
4. Recovering from the incident. Recovery procedures should reflect any relevant Business Continuity Plans and aim to meet applicable Service Level Agreements (SLAs).
5. Learning from the incident. To prevent an organisation from continually dealing with the same type of incident because of an unrecognised vulnerability, organisations should endeavour to quantify and monitor the types, volume and cost of incidents. This information should feed into the organisations risk management process.

For an Incident Handling Strategy to work, it's imperative that it is communicated to all the stakeholders. This should ideally be apart of a comprehensive Security Awareness Campaign.

5. LOOP TECHNOLOGY



Loop Technology is a focused information security specialist that partners with organisations to deliver a holistic approach to IT security.

We have been a trusted security advisor to many leading organisations in Australia for more than a decade through our commitment to staying on top of emerging security issues and industry developments.

Loop Technology’s approach to security is to understand every layer of your organisation’s security strategy and drivers, continually assess the risks that affect your business, recommend practical security controls and provide high-quality education, maintenance and support for all of your information security requirements. We provide a full range of security services and solutions which are designed to deliver your business a secure environment.

Through the combination of Information Security Policy, Procedures and tools, Loop can help you to identify the risk associated with data leakage and minimise both the likelihood and the impact of this risk by implementing appropriate controls.

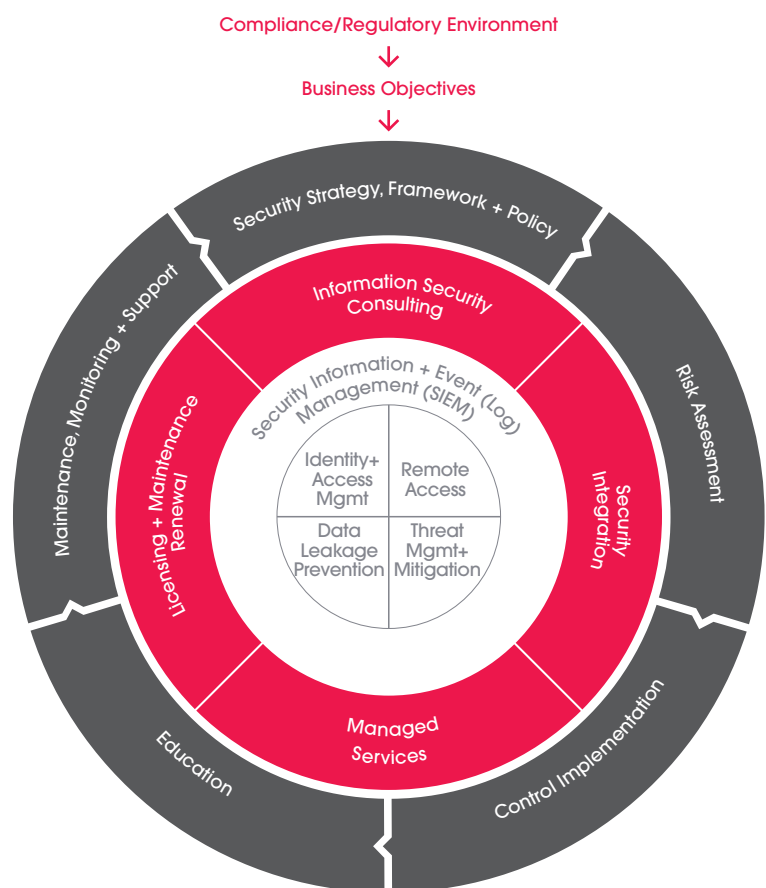
To speak with a Loop Technology expert on preventing data leakage or to discuss any of your organisations information security requirements please contact 03 9643-3600 or info@looptech.com.au.

Loop Technology Pty Ltd
www.looptech.com.au
 ABN 76 114 448 225

Sydney
 Level 6, 75 Miller St, North Sydney NSW 2060
 T: +61 2 9464 0100

Melbourne
 Level 8, 474 Flinders St, Melbourne VIC 3000
 T: +61 3 9643 3600

Brisbane
 Unit 3, 7 Camford St, Milton QLD 4064
 T: +61 7 3367 2666



APPENDIX A: MAPPING THREATS TO POTENTIAL CONTROLS



		POTENTIAL CONTROLS										
		Information Security Policy	Access Control Policy	Data Classification Scheme	Acceptable Use Policy	Security Awareness Campaigns	Human Resources Security	Technical Access Controls	End Point Encryption	Penetration Testing	Logging and Auditing	Incident Handling Strategy
THREATS	Lost/ Stolen Device	Π	Π		Π	Π		Π	Π			Π
	Insider Attack	Π	Π		Π	Π	Π	Π	Π		Π	Π
	Network Intrusion	Π	Π		Π	Π		Π	Π	Π	Π	Π
	Accidental Loss of Data	Π	Π	Π	Π	Π		Π	Π		Π	

Sydney 02 9464 0100
LOOPTECH.COM.AU

Melbourne 03 9643 3608

Brisbane 07 3367 2666

