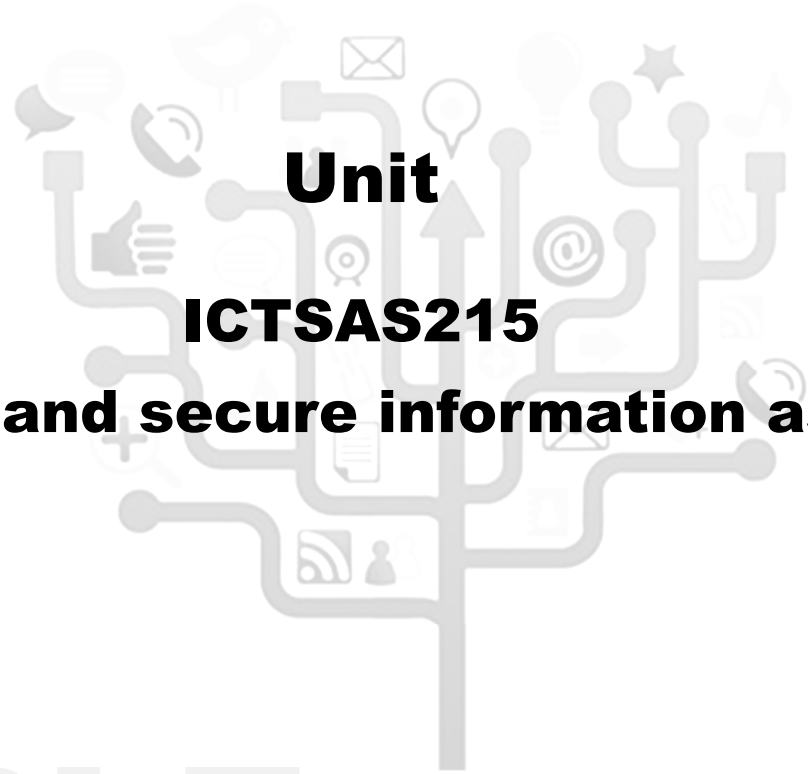
PASSING LANE

ICT - Information and Communications Technology

ICT20120
Certificate II in Applied Digital Technologies



Unit

ICTSAS215

Protect and secure information assets

Student/Trainee Manual

Passing Lane Pty Ltd
PO Box 975
COWES VICTORIA 3922

MATERIALS PUBLISHED IN AUSTRALIA

STUDENT/TRAINEE DETAILS

Student/Trainee Name

Student/Trainee Email

Teacher / Trainer Name

School / Institution / Training Organisation / Employer

PASSING LANE

TABLE OF CONTENTS

INTRODUCTION

This manual was developed to provide training content that addresses the specific 'Unit of Competency' as outlined in the following pages.

We encourage you the student / trainee to take your time when reviewing this content and seek any assistance from your teacher/trainer should you have difficulty in understanding the information.

LEARNING ACTIVITIES

Also included in this Student / Trainee manual are a series of Learning Activities.

The learning activities in the student and/or trainee manuals are 'Form Enabled' so that if the resources are delivered online, the activities can be entered in using the computer keyboard.

Each learning activity is identified with the following icon.

Learning activities come in the following forms.

- ☆ Questions
- ☆ Research
- ☆ Tasks
- ☆ Interviews

INTRODUCTION—CONT'D

Questions

Questions generally relate to the information presented on previous pages. Questions will also include multiple choice questions, 'Yes' and 'No' questions and/or 'True' and 'False' questions.

Research

This type of learning activity requires you to locate information by using research methods. The research methods could include:

- ☆ Internet searches
- ☆ Reading textbooks and other reference sources
- ☆ Location visits

Tasks

This learning activity type requires you to actually do something and some examples of tasks may include:

- ☆ Creating reports
- ☆ Visiting locations such as workplaces
- ☆ Performing an activity in a workplace

Interviews

This learning activity type would require you to interview person(s) in an actual workplace environment or a person(s) who are experienced in the industry sector which you currently are undergoing training.

You will be made aware of the type of learning activity by noting the learning activity type displayed under the learning activity icon.

INTRODUCTION—CONT'D

USING THE FORM ENABLED FEATURE

If you are using this manual online, you can fill in some of the answers using your computer keyboard.

Your teacher or trainer will provide you with the information and instructions on how to use the 'Form Enabled' feature in this manual.

SELF ASSESSMENT

At the end of each manual is a series of questions that you should review and answer either Yes or No.

The term 'Self Assessment' means you will ask yourself these questions and therefore is no need to provide the answers to the self assessment questions to your teacher or trainer, unless they require you to do so.

This self assessment is to ensure you have reviewed and understood the information that was presented in this manual.

If you answered 'No' to any of these questions or are unsure of your understanding in any of the topics reviewed, you are encouraged to go back and review the information again and/or seek the assistance of your teacher or trainer.

UNIT OF COMPETENCY OVERVIEW

The following pages are extracts from Training.gov.au website and outlines this specific 'Unit of Competency' including the 'Elements' and the 'Performance Criteria'. The content within this manual has been developed to address this unit.

ICTSAS215 PROTECT AND SECURE INFORMATION ASSETS

ELEMENT	PERFORMANCE CRITERIA
1. Identify assets and threats	1.1 Identify information assets in the organisation 1.2 Identify and record mechanisms by which information assets are accessed, transmitted and stored 1.3 Identify nature of threats to information assets and determine threat impact according to organisational processes
2. Protect assets	2.1 Identify and confirm actions, mechanisms and strategies to protect information assets with required personnel 2.2 Secure assets according to organisational procedures 2.3 Report outcomes and escalate issues to required personnel
3. Mitigate or prevent damage to assets	3.1 Identify signs and evidence that information assets are threatened or undergoing loss or damage 3.2 Provide first level response to reduce effects, mitigate damage and protect evidence 3.3 Report incident, resulting effects and actions taken to required personnel
4. Document final condition of information assets	4.1 Finalise documentation outlining current state of information assets according to organisational procedures 4.2 Save, store and back up reports according to organisational procedures 4.3 Maintain records and reports of information assets according to organisational procedures

You as the student or trainee should be aware that in order to successful complete this unit of training, you will be required to protect and secure at least two different information assets types.

Generally, it is expected that you will be observed doing the above mentioned tasks as an employee in a workplace environment.

If this is not the case then your teacher or trainer would create a simulated workplace environment where you would be observed performing those protection and the securing of two information assets.

In any case, this training manual assumes that you are an employee.

Section One

Identify Assets and Threats

PROTECT AND SECURE INFORMATION ASSETS

SECTION ONE—IDENTIFY ASSETS AND THREATS

Introduction

All organisations will have a level of information or data being stored on a computer system of some type.

It is likely that a significant amount of this information would be considered confidential and sensitive therefore would need to be protected from unauthorised access and improper use.

This training unit describes the skills and knowledge required to ensure information assets are protected from improper access and to secure assets in the event that they are threatened.

It applies to those who, while working under a level of supervision in a frontline technical support capacity, have the responsibility to exercise security measures on information assets in a small or large office environment.

Section Learning Objectives

At the completion of this section you will learn information relating to:

- ☆ Identifying information assets in the organisation
- ☆ Identifying and recording mechanisms by which information assets are accessed, transmitted and stored
- ☆ Identifying nature of threats to information assets and determining threat impact according to organisational processes

Identify information assets in the organisation

The definition of an information asset is deliberately wide as it is important for organisations to recognise the various different kinds and types of assets it has.

However, Information assets can be described as a body of information, managed as a single unit, so that it can be understood, shared, protected and exploited efficiently.

To understand whether something is classified as an information asset, that information needs to be assessed by some of the following criteria:

- ***Value*** **-** Does the information have value to the organisation?
- ***Risk*** **-** Is there a risk associated with the information? (What would happen if it was accessed)
- ***Content*** **-** Does the information have a specific content?
- ***Lifecycle*** **-** Does the information have a manageable lifecycle? (How long would the information be of value to the organisation)

However, to assess every single individual file an organisation holds is not a feasible operation.

As such, information assets need to be grouped into more manageable portions.

If an information asset is defined at a level that allows all of its constituent parts to be managed usefully as a single part they become easier to control, define and record.

This highlights that managing and grouping information assets is not as straightforward as it may seem.

If you classify them too broadly you will not have enough level of detail and you will have too many assets, which become hard to manage.

Examples of Types of Information Assets

Information assets can come in many guises, information of value that organisations hold can span many different categories related to all aspects of business.

Here are some examples:

- ***Strategy*** **-** Any plan, goal, or objective that has been developed to improve the organisations future
- ***Intellectual property*** **-** Copyrights, trademarks, patents
- ***Trade secrets*** **-** Methods, processes, formulas and designs that give the organisation a competitive advantage
- ***Products and services*** **-** Information that is sold to customers, such as books or learning material
- ***Training material*** **-** Content used to train employees
- ***Marketing*** **-** Advertising material used to generate demand and brand awareness
- ***Customer information*** **-** Databases about customers and their details
- ***Operations*** **-** Data used to complete process and procedures
- ***Financials*** **-** Accounting data and financial reports
- ***Employees*** - Personal details on all employees
- ***Research and development*** **-** Information on market research and product designs

Learning Activity

Question

LEARNING ACTIVITY ONE

1) In this Section we learned that to understand whether something is classified as an information asset, that information needs to assessed by some criteria. What were the four 'criteria points' we learned about?

2) What were the eleven examples of an organisation's information assets as outlined in this Section?

Learning Activity

Task

LEARNING ACTIVITY TWO

To successfully complete this 'Unit of Competency' you will be required to demonstrate your ability to 'protect and secure at least two different information assets types' in your workplace.

To do this you will need to first identify what types of information assets there are in the organisation.

This activity requires you to do some internal research and list the types of information assets you have identified.

We have provided space on the following page for you to complete this activity.

Your role in the organisation

Type of industry your employer is in _____

Type of information assets identified

IDENTIFY AND RECORD MECHANISMS BY WHICH INFORMATION ASSETS ARE ACCESSED, TRANSMITTED AND STORED

Organisations differ greatly depending on their operations and industry, so the types of Information assets they have can come in many forms.

As such, the methods in which these information assets are accessed, used and stored can also vary too.

Regardless of these differences, each asset has some sort of 'carrier', be it paper, USB sticks, hard drives, servers, cloud based storage, or portable devices such as laptops, tablets and handhelds.

With so many types of information assets and carriers for that information, keeping track of the details, locations and type of information asset is not always the most straightforward task.

That is why it is always recommended to keep an inventory of information assets.

Categorising inventoried information assets helps establish an organised policy toward asset management.

Information assets and their 'metadata' need to be easy to find and grouping them by their type enables this.

Categories of assets can be classified as such:

- ***People*** **-** Information relating to a person or role
- ***Equipment*** **-** Information regarding specific machines or devices
- ***Environment*** **-** Information linked to geographical factors
- ***Software*** **-** Information on applications or systems
- ***Data*** **-** A stored collection of information, such as a database of clients
- ***Organisation*** **-** Information about the operational and processes of the organisation
- ***Third parties*** **-** Information on third parties or information managed by third parties

Developing an Inventory of Information Assets

An inventory will help an organisation easily identify and record how and where their information assets are used and stored, so long as it is carefully maintained and regularly updated.

The inventory can be developed to include additional fields (such as 'metadata') that provide further information regarding the asset and how such assets can be categorised.

Some of the fields may contain:

- ***Title*** **-** A title acts as an easy and immediate identifier of assets
- ***Description*** **-** Provides further, more detailed information regarding the asset
- ***Owner*** **-** Details who controls the asset. Assets require an owner to make decisions regarding its uses, budget, lifecycle, etc.
- ***Security*** **-** Defined as confidentiality, integrity and availability. Each asset should have identifiers as to which of these types it belongs to
- ***Personal data*** **-** Personal data requires additional protection so it must be understood which assets contain it
- ***Access*** **-** Defines which departments and roles are permitted access to the asset

Information Assets Access Policies and Procedures

As we now know, any asset of an organisation has a value to the organisation and this includes information assets.

The protection and security of information assets is very important and organisations generally put in place information asset access controls.

In many larger organisations, access to the information assets does not mean everyone has access to the all information.

Often you will find that certain employees are restricted in accessing certain information.

Clearance levels would be based wholly on the type and size of the organisation, as well as the number of distinct functions and/or departments within that organisation.

Clearance levels have to take into account the danger of unauthorised copying of information or the malicious destruction of information.

The higher the clearance levels, the less likely for problems resulting from unauthorised access.

Access controls to certain computers, servers, files and folders where confidential and sensitive information is stored is generally done using a username and password system.

Each person allowed access to the certain information is provided a username specific to that person only and a password known only by the user and generally the computer system administrator.

Learning Activity

Task

LEARNING ACTIVITY THREE

As you know, to successfully complete this 'Unit of Competency' you will be required to demonstrate your ability to 'protect and secure at least two different information assets types' in your workplace.

After identifying what types of information assets there are in the organisation, you now need to identify and record how the organisation's information assets are accessed and how they are stored.

This means again it requires you to do some internal research and identify and record how the organisation's information assets are accessed and how they are stored.

It should be noted that some organisations have 'Knowledge Systems' or 'Information Systems' that are use to manage information assets.

If so, keep those systems in mind when completing this activity.

We have provided space on the following page for you to complete this activity.

Description of the organisation's information access controls

How the information assets are stored

IDENTIFY NATURE OF THREATS TO INFORMATION ASSETS AND DETERMINE THREAT IMPACT ACCORDING TO ORGANISATIONAL PROCESSES

As well as being a useful tool to organise and detail information assets, an inventory can also be used to identify threats to and the risks associated with information assets.

It's critical that organisations assess the threats to information assets so that they can administer them with the necessary level of protective security measures and a risk inventory of information assets provides a great opportunity to do that.

As we established, if an organisation has information of value, then it is likely to be classified as an information asset.

If it is valuable to the organisation then it's likely to be valuable to others too and this makes it vulnerable to thieves and cybercriminals.

The risk associated with the asset is likely to increase with the more valuable the information is.

A threat is any type of incident that could negatively affect an asset.

For example, it could be lost, stolen, or accessed by an unauthorised party.

Threats can be categorised in the risk inventory as the types of circumstances in which the confidentiality or integrity of an asset can be compromised, whether intentionally, or not.

It is important to identify the nature of any threat to information assets, log them in the risk inventory and then analyse and assess the methods necessary to protect the asset against the threat.

When assessing the nature of threats to assets, the level and types of vulnerability they are susceptible to also need to be considered.

Vulnerabilities are flaws in processes and systems that can be exploited and can be physical or technological in types, or even be vulnerable due to human elements.

Information Asset Vulnerabilities

Physical vulnerabilities can be things such as broken locks which allow access to prohibited areas which house information assets, normally only accessible to individuals with the relevant access clearance levels.

Technological vulnerabilities can relate to things like software or systems that encounter bugs and can be exploited by hackers to access information assets.

Human vulnerabilities can relate to things such as our susceptibility to phishing emails, communication errors and so on.

As well as determining threats to information assets, it's also necessary to review the potential impact if any threat appears.

Loss or leaks of information assets could potentially be catastrophic to an organisation, which further highlights the need to review assets and any potential threats to them.

The sensitivity of certain types of information stored by organisations often mean that there is a high level of security required to meet regulatory privacy compliance laws.

If these preventative measures were not adequate, there could be significant legal and financial ramifications.

There is also the damage done reputationally to the organisation which can often have a more severe impact in the long term.

Learning Activity

Question

LEARNING ACTIVITY FOUR

1) What were the three common types of information asset vulnerabilities as we reviewed in this Section?

2) Certain information is protect by Australian law. What law would that be?

Learning Activity

Task

LEARNING ACTIVITY FIVE

The next assessment requirement is for you to identify and learn about the vulnerabilities and threats to the information assets in your workplace.

The best method to use in this case is to discuss this topic with your employer and/or the IT administrator.

They will be able to help you to understand what information asset is most vulnerable and what the consequences would be if this information asset was under threat and compromised.

Take notes and record your conversation/interview on the next page.

These notes and records will assist you in addressing an assessment requirement.

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Information Asset _____

Vulnerabilities and potential threats

Potential consequences of asset being compromised

Section Two

Protect Assets

PROTECT AND SECURE INFORMATION ASSETS

SECTION TWO—PROTECT ASSETS

Introduction

In Section One, we learned that one of the most valuable assets that any organisation can have is their information assets.

Because information assets are so valuable, it could be under threat and therefore must be protected.

In this section we learn about how this could be done.

Section Learning Objectives

At the completion of this section you will learn information relating to:

- ☆ Identifying and confirming actions, mechanisms and strategies to protect information assets with required personnel
- ☆ Securing assets according to organisational procedures
- ☆ Reporting outcomes and escalate issues to required personnel

Identify and confirm actions, mechanisms and strategies to protect information assets with required personnel

When the threats to information assets have been established, you are then able to more easily identify methods by which to protect them from said threats.

As discussed in the previous section, threats to information assets can materialise due to certain vulnerabilities, physical, technological and human vulnerabilities.

Therefore, the measures put in place for each asset need to adequately protect it against each type of these vulnerabilities.

Physical

These protection measures involve physically restricting people from accessing certain areas, or storage that contain information assets.

One of the key aspects of protecting information assets is restricting access only to those personnel with the correct level of clearance, and physical access control is a common method for doing so.

Physical access can be restricted through the use of padlocks and keys for smaller information assets, such as filing cabinets and cupboards that contain paper documents.

They can also be implemented through the use of access cards, password coded doors and even biometrics to restrict access to physical spaces that house larger information assets, such as server rooms and other IT infrastructure.

As well as physically restricting who can reach these spaces it is also possible to track and monitor which individuals have accessed them and further deterrents can be enforced by the use of monitoring tools such as CCTV.

Technological

The technological methods used to secure information assets are associated with the hardware, software and applications designed to protect information systems.

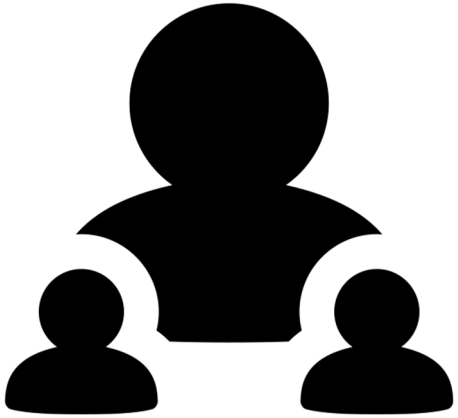
This includes programs such as antivirus and antimalware software and hardware devices, such as firewalls and cryptographic keys.

Organisations usually store large amounts of data somewhere on their extensive IT infrastructure, including devices such as hard drives, servers, workstations and cloud storage.

The information assets stored on these devices contain sensitive and valuable information, from employee and customer details, to business strategies and intellectual property.

In the modern age cybercriminals pose a very real threat and will use all manner of destructive software to target an organisation's assets, mainly because of their value to them.

It should be a top priority for any organisation to protect their digital information assets and they need the necessary software and hardware to do so.



Human

Although there are numerous physical and technological mechanisms that can be employed to protect information assets, they are still at times vulnerable to the effects of human errors.

Workplaces can often be stressful environments which can cause people to be emotional, not concentrate at the tasks at hand, and have lapses in judgement.

Though unintentional, these moments can be the cause of losses to information assets.

Whether it’s leaving a device behind on a train, misplacing something, or even clicking a malicious link in a phishing email, human errors can lead to assets falling into the wrong hands.

Even though you will never be able to fully eradicate human error, there are still ways to combat it and reduce the likelihood of these events happening.

The best strategy to combat human errors is through training.

Training raises awareness about a person's actions, instills good practices and teaches employees of the ways that cybercriminals will try to deceive people.

All organisations should train staff regarding information assets, their value and importance, as well as the best ways to keep them safe and protect them.

Learning Activity

Task

LEARNING ACTIVITY ONE

In the previous Section we had you identify and learn about the vulnerabilities and threats to the information assets in your workplace.

The next assessment requirement is for you to identify and learn about the strategies and mechanisms used to protect the information assets in your workplace.

Again, the best method to use in this case is to discuss this topic with your employer and/or the IT administrator.

They will be able to help you to understand what strategies, mechanisms (including policies and procedures) are in place and used to protect the information assets.

Take notes and record your conversation/interview on the next page.

These notes and records will assist you in addressing an assessment requirement.

Brief summary on strategies in place to protect the organisation's information assets

Brief summary on mechanisms in place to protect the organisation's information assets

Secure assets according to organisational procedures

On the previous pages we have reviewed the possible methods and strategies organisations can adopt in order to protect their information assets.

Which of these methods are implemented depends on the information asset itself, it's type, it's owner and how sensitive or vulnerable the asset is.

The policies and procedures the organisation has in place are what ultimately govern how assets are secured.

- ***Type*** **-** Some assets can only have certain types of protective measures applied to them.

  For example, it's not possible to apply technological methods to information assets stored on paper.

  However, physical methods, such as being kept under lock and key, or being held in restricted areas can certainly be applied to these assets.

  Each organisation should set procedures stating the methods used to secure different types of information assets.

- ***Owner*** **-** The asset inventory provides fields stating who the 'owner' of each information asset is.

  The owner is usually a senior individual within the organisation and is responsible for the asset, what is added and removed, how it is stored, as well as who has access and why.

  It is ultimately them who will provide the judgement of the protective measures used to secure the asset as they understand it and its value the most.

- ***Value*** **-** Another policy that may be implemented to determine the methods used to secure assets is its value to the organisation.

  Procedures can be written which classify information assets into levels of priority based on their value to the organisation and have relevant protocols that must be adhered to, based on these values.

  For example, though both assets would need to be secured, the processes and formulas used to create an organisation's cornerstone product would require higher levels of security than the training criteria for new staff members.

Learning Activity

Task

LEARNING ACTIVITY TWO

As you know, the assessment requirement for this unit of training requires you to protect and secure at least two different information assets types in your workplace.

You are now at the stage where you are to locate two types of information assets and take the required steps to protect each information asset type and ensure that each has been secured.

The type of information asset will be those agreed to between yourself and your employer.

Your teacher or trainer will provide your employer with the necessary assessment forms for them to fill in and sign.

These will form part of your assessment evidence.

Report outcomes and escalate issues to required personnel

Implementing protective measures to secure information assets would require a collective effort from those tasked with enforcing these measures and the information asset owner.

Though these personnel may be required to oversee the security and protection of an organisation's information assets, it is the individual asset owner who understands that particular asset the most.

Therefore, the outcomes of the protective measures and any issues that arise during their implementation, need to be reported to the information asset owner and any other required personnel.

These will certainly be more senior personnel who are responsible for making critical business decisions and who fully understand and realise the value of the organisation's information assets and the consequences of them being lost, stolen, or compromised.

For technical issues it would be those persons with the technical expertise to review and resolve any technical issues.

The measures used to protect each information asset need to be documented and reported so that they can be analysed by the asset owner and any other required personnel.

The report should clearly outline what has been done to protect and secure the particular information asset and also provide information on any issues that were encountered, how they were resolved and by whom.

Learning Activity

Task

LEARNING ACTIVITY THREE

As part of the assessment requirements you are to report to the most appropriate person what you have done to secure those information assets. You must also report any problems or issues you may have encountered when protecting and securing those two types of information asset types.

Your teacher or trainer will provide your employer with the necessary assessment forms for them to fill in and sign for this assessment requirement.

These will form part of your assessment evidence.

Section Three

Mitigate or Prevent Damage to Assets

PROTECT AND SECURE INFORMATION ASSETS

SECTION THREE—MITIGATE OR PREVENT DAMAGE TO ASSETS

Introduction

As we have learned, organisations with valuable information assets take the time and make the effort to protect and secure those information assets.

However, just taking the steps in protecting and securing information assets does not mean there will be no more threats or attacks on those assets.

There still needs to be a diligent effort in watching for ongoing attacks and preventing any threats causing damage to the information.

We look at this subject in this section.

Section Learning Objectives

At the completion of this section you will learn information relating to:

- ☆ Identifying signs and evidence that information assets are threatened or undergoing loss or damage
- ☆ Providing first level response to reduce effects, mitigate damage and protect evidence
- ☆ Reporting incident, resulting effects and actions taken to required personnel

Identify signs and evidence that information assets are threatened or undergoing loss or damage

The protective measures mentioned in the previous section not only help secure an organisation's information assets, but also act as monitoring tools.

As valuable information assets are constantly under threat, it's important to regularly and consistently monitor their status and check whether they are suffering loss, or damage.

- ***Physical identifiers*** **-** For physical vulnerabilities different methods of physical access control can be implemented.

  These control methods also log user information and activity.

  This information can be used to correlate patterns on who has accessed information assets, when and how often.

  As well as cross referencing users to see whether they necessarily required access to assets, it also highlights any variations or irregular patterns that may indicate something sinister is happening.

- ***Human identifiers*** **-** Although certain human traits can make information assets vulnerable at times, they can also assist in identifying threats to information assets.

  This can be achieved by reporting suspicious behaviours and incidents such as phishing attacks, requests for unauthorised access, and loss of devices or access cards.

  However, the effectiveness of human identifiers often comes down to how aware and well trained individuals are.

  This highlights the necessity to provide training to staff on the dangers and threats to information assets, what to look out for and how to identify any suspicious behaviour.

  Though it may not be reasonable to expect every employee to be overly proficient in IT security, by making them aware of the basics and key indicators they too can help protect assets and identify any potential threat to them.

- ***Technological identifiers*** **-** The technological threats to information assets are usually far more extensive and the list of various digital monitoring tools available to organisations highlights this.

It's essential and should be mandatory that antivirus and antimalware programs are constantly running on systems, scanning networks and devices for any potentially harmful software that could damage information assets.

However, there are some other vital security monitoring tools that help organisations further protect their assets.

- ***Vulnerability scanners*** - these perform rigorous examinations of systems to identify weaknesses that might allow security violations.

  They firstly examine system configuration files and system password files for weak passwords, followed by network based assessments that reenact common intrusion scripts and record the responses.

  The results provide a snapshot of system security at a certain point in time.

  Though these tools don't detect attacks in progress, they determine whether an attack is possible, or if one has already occurred.

- ***Firewalls*** **-** these are digital access control mechanisms acting as a barrier between networks, including your internal networks and the internet.

  They accept or reject traffic based on a specific rule set that is defined by an administrator.

  The audit trails and activity logs created by firewalls can be used to monitor and review network traffic.

  Doing so can highlight unusual patterns of usage that can be investigated further to detect whether information assets are under threat.

- ***Intrusion detection systems*** **-** these collect information from various system and network sources, analyse the data streams for signs of misuse or intrusion and report the outcomes.

  These reports, which may be accompanied by an alert, usually need to be investigated before any action can be taken, though some IDS can be programmed to respond automatically to certain events.

Learning Activity

Question

LEARNING ACTIVITY ONE

1) In this Section we learned about three types of information asset ‘threat identifiers’. What were those three ‘threat identifiers’?

2) In this Section we learned about three types of vital ‘security monitoring tools’ that are often used to protect information assets. What were those three ‘security monitoring tools’?

Learning Activity

Task

LEARNING ACTIVITY TWO

In Section Two, Activity Five you identified the organisation's information asset's vulnerabilities and potential threats.

In this Section you will be required to learn about what threats have existed and what steps were taken to prevent the threats from doing damage to the information asset(s) or at the very least, mitigate the damage.

To start off we want you to take the time and interview your employer and/or the organisation's IT administrator and ask what threats to the information assets has the organisation experienced in the past, what was done and what was the extent of the damage.

Take notes and record your conversation/interview on the next few pages.

INCIDENT RESPONSE

Provide first level response to reduce effects, mitigate damage and protect evidence

AND

Report incident, resulting effects and actions taken to required personnel

(Over the next few pages we cover two 'Performance Criteria' points at the same time to avoid repetition)

Despite best efforts to increase security awareness and mitigate risks from threats and vulnerabilities affecting systems, it is still always possible to experience security incidents that threaten the integrity of information assets.

The definition of a security incident will differ for each organisation, but may fall into some of the following categories:

- ***Compromise of integrity*** - If a virus infects an application or system
- ***Damage*** - If a virus destroys information assets
- ***Misuse*** - When an intruder, or a disgruntled employee, accesses assets without authorisation
- ***Alteration*** - When data is manipulated to adversely affect system performance
- ***Denial of Service (DoS)*** - When an attack disables system

Due to their likelihood, organisations would be prepared to deal with security incidents and have policies and procedures already in place that define the actions to be taken during a security incident.

Larger organisations put in place 'Computer Security Incident Response Capability', or CSIRC.

The primary goal of CSIRC should be to mitigate the effects of a security incident and protect information assets from further damage through the following stages.

This requires the assignment of responsibilities, training and awareness of a 'Security Incident Response Team'.

In smaller organisations this could be one or two persons that are part of a small IT administration team with other responsibilities and larger organisations there could be a dedicated 'Security Incident Response Team'.

Whatever the size of the 'response team', there are common tasks performed when a threat is identified.

We look at those on the next page.

Levels of Response

Again depending on the size of the organisation and the policies and procedures in place, the responses to an information asset security threat could include:

- ***Verify and notify*** **-** Those tasked with responding to an information asset security incident would first verify the occurrence, as well as the source of the security incident.

  If found to be true, then all users within and outside the organisation who may be affected would be notified.

  If the breach involved access to private information, then the senior management would need to be notified immediately in line with legal requirements.

- ***Contain*** **-** Next the team would work to contain the incident and limit any further damage.

  This may involve disabling network or systems access, or installing patches to resolve vulnerabilities.

  It may also require the passwords of breached accounts to be reset, or using access control software to block accounts of any insiders that may have caused an incident.

- ***Assess*** **-** It is vital for the incident to be fully contained so that any damage is limited before an incident is investigated.

  It can also be difficult to understand the severity of an incident and the extent of the damage while the incident is ongoing.

  Once it has been deemed safe to do so, the analysis and status of information assets can begin.

- ***Recover*** **-** When the attack has been neutralised and the extent of the damage understood, any systems or services that require restoration can be recovered and made secure.

As each step and activity takes place it is very important that everything is recorded.

Reporting Information Security Incidents

After a security incident has occurred and been neutralised, the incident will need to be reported.

As we mentioned earlier, a thorough examination into the security incident will need to take place if a report of the incident is to be useful.

This examination and the resulting report are necessary so that lessons can be learned from the experience and the policies and procedures of the information asset security access controls and security tools can be updated if needed.

The report should indicate the following:

- ***How the incident started*** - What were the vulnerabilities that were exploited and how was accessed gained?
- ***Who was made aware of the incident and how*** - What person was notified and how?
- ***How the incident was contained*** - What was done to resolve the issues and the timeline of events?
- ***Whether response was adequate*** - Are the existing procedures appropriate or do they need updating?
- ***Whether vulnerabilities still exist*** - Are there still security issues remaining and how do they get resolved?
- ***Whether assets were affected*** - What is the status of information assets and extent of damage done?

The report should provide a concise analysis of the security incident and measures undertaken so they can be reviewed by the necessary personnel.

Who this personnel is will change depending on the type and size of the organisation, but will almost certainly involve senior management, owners and other stakeholders.

In most cases those receiving the report would not be technically proficient and understand all aspects of cyberattacks, which means that the report needs to explain the incident in layman's terms, without the over use of technical details and use of jargon.

The report needs to be easy to understand for all parties so that the situation can be understood and the most appropriate cause of action taken to secure and maintain information assets.

Learning Activity

Question

LEARNING ACTIVITY THREE

1) In this Section we learned that the definition of a security incident often falls into five common categories. What are those five categories?

2) In this Section we learned that an information asset incident report could include six relevant topic areas. What are they?

Learning Activity

Task

LEARNING ACTIVITY FOUR

Over the previous pages we reviewed how some organisations put in place 'incident response teams' to deal with information asset threats and attacks.

In the space provided below, describe the personnel 'mobilised' to deal with information asset incidents in your workplace.

Tell us the role of each person, in other words what they do when they are required to deal with information asset incident.

Number of persons involved in an information asset incident _____

The role of each person...

One _____

Two _____

Three _____

Four _____

Five _____

Six _____

Section Four

Document Final Condition of Information Assets

PROTECT AND SECURE INFORMATION ASSETS

SECTION FOUR—DOCUMENT FINAL CONDITION OF INFORMATION ASSETS

Introduction

As we now know information assets are key to every organisation's basic operation and must be protected.

We also learned that protecting and securing information assets requires a number of activities and tools, therefore these need to be documented and stored.

This includes any security incidents and the activities that led to a resolution of the incident.

In this final section we look at what documentation, records and reports would need to be saved and stored.

Section Learning Objectives

At the completion of this section you will learn information relating to:

- ☆ Finalising documentation outlining current state of information assets according to organisational procedures
- ☆ Saving, storing and backing up reports according to organisational procedures
- ☆ Maintaining records and reports of information assets according to organisational procedures

Finalise documentation outlining current state of information assets according to organisational procedures

After a security incident it is important to review the protection measures in place to secure information assets so that it can be judged whether they are still adequate and if any improvements to security need to be made.

This review needs to be documented so that it can be analysed by certain personnel who can then decide on the necessary changes.

The documentation also needs to establish the current state of the information assets and assess them in accordance to the procedures outlined by the organisation regarding information assets.

It's possible that during the security incident the assets suffered damage or loss and this needs to be quantified so that they can be recovered, restored or reproduced.

When constructing an information asset inventory, the organisation should establish criteria regarding the different states of its assets.

The 'state' refers to its condition and outlines the effects that different conditions have on its state.

As each asset has different values, risks and life cycles associated with it, what defines these states may differ from asset to asset.

The level by which an asset is compromised or damaged, will also be a major contributing factor to its current state.

Documenting the State of Information Assets

In the aftermath of a security incident the documentation outlining the information assets state will also highlight any amendment necessary to an assets criteria.

The value, risks and life cycle associated with a particular asset may change drastically in the wake of an attack.

This criteria is a key indicator for the main purpose of the review - to see whether the current protection measures are adequate.

If the value of an asset and the associated risks increase, then it's evident that the protective measures in place will need to be increased too.

To review, the documentation on the state of the assets needs to establish the following:

- ☆ The extent of damage done to the information asset
- ☆ The current state of the information asset
- ☆ The new criteria related to the information asset (value, risk, life cycle)
- ☆ The necessary security measures to protect the information asset appropriately in the future

Learning Activity

Task

LEARNING ACTIVITY ONE

As we learned on the previous pages, many organisations will have policies and procedures relating to the production of documentation relating to the ‘state’ of specific information assets, especially after a specific asset has been under threat or attacked.

In this activity we want you to do some research in your own workplace and summarise below what policies and procedures are in place for the development of documentation that relates to the ‘state’ of specific information assets.

We have provided space on the next page for you to complete this activity.

Summary of policies and procedures in place for ‘report’ documentation that relates to the ‘state’ of specific information assets...

Save, store and back up reports according to organisational procedures

and

Maintain records and reports of information assets according to organisational procedures

(Over the next few pages we cover two 'Performance Criteria' points at the same time to avoid repetition)

The purpose and importance of creating reports in the wake of a security incident have been highlighted in the previous section.

Simply, they reassess the information assets and establish newer, safe protection methods to help secure information against repeat or future attacks.

However, once the report has been completed, they are still a valuable commodity and something that can be used in the future to help and assist the organisation.

This is why it is important to save, store and maintain reports.

The organisation should have procedures in place that establish protocols for methods used to store records.

This includes details on where they should be stored and who has access - after all, if the reports include details on information assets, that information should be restricted to those with the necessary level of access.

The reports should be saved and stored so that they can be accessed in the future for a number of beneficial reasons, such as a reference tool.

INFORMATION ASSETS REPORTS

Uses of Information Asset Incident Reports

The reports can be used to refer back to and learn from, assessing how incidents were handled, both well and poorly.

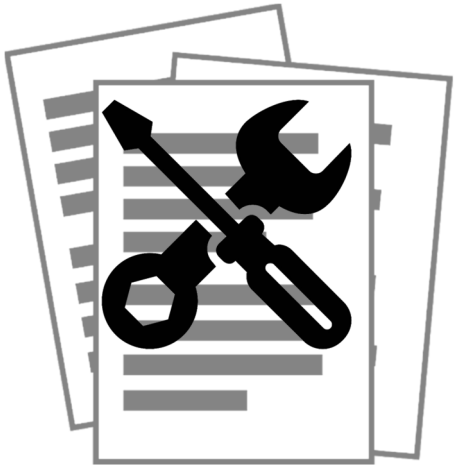
By seeing what was done right the organisation can try and repeat those practices, and change approaches when certain aspects didn't work so well.

The reports can also be used as a training tool for new and existing staff.

They establish the reasons for how the security incident occurred, highlight the vulnerabilities or flaws that caused it, outline the methods used to contain it and whether any of these were successful, or not.

By having a reference tool to show the do's and don'ts in the event of a security incident, the organisation can use previous attacks to their advantage.

Used for these purposes, the report becomes a valuable commodity and has in turn become an information asset itself.



Maintenance of Information Asset Records and Reports

On the previous pages we have highlighted the importance of maintaining records.

These records become information assets themselves as they continue to serve the organisation, even after their initial purposes for creation has expired.

By continuing to help the organisation by being used as a reference tool, learning aid and training guide the reports help the organisation secure information assets for the future.

However, it's not just the reports of security incidents that need to be thoroughly maintained.

To protect information assets as well as possible, the records and reports of assets need to be continually updated to reflect the current environment and to protect against insiders, environmental hazards and the continually evolving threats from cybercriminals.

As information assets must have levels of access control assigned to them, the maintenance of asset records must be conducted by those individuals with the necessary level of clearance, in accordance with the organisations procedures.

To put simply, an individual must have the required level of access in order to maintain a particular information asset record.

The information on the required level of access and which personnel are included in that group, should be listed in the relevant field of the information asset inventory.

The records used to maintain and record information on assets, namely the asset inventory, need to be constantly monitored and updated.

These updates should reflect any changes to the status or criteria of information assets and the new methods and strategies that must be employed to assure they are adequately protected.

For example, if a new computer virus is in circulation, or a cybercriminal group has begun targeting specific industries, then the organisation needs to be aware and prepared for the potential threat against them.

By maintaining the records of information assets consistently and regularly, the procedures designed to protect assets will be up to date, sufficient and readily available for the personnel involved in securing them, namely those in the computer security incident response team.

Learning Activity

Question

LEARNING ACTIVITY TWO

What were the four common uses for information asset incident reports as we reviewed in this Section?

Learning Activity

Task

LEARNING ACTIVITY THREE

We also learned that many organisations will have policies and procedures relating to the reporting and record keeping of the maintenance activities of information asset protection and security.

In this activity we want you to do some research in your own workplace and summarise below what policies and procedures are in place for the reporting and record keeping of the maintenance activities of information asset protection and security.

We have provided space on the next page for you to complete this activity.

Summary of policies and procedures in place for reporting and record keeping of the maintenance activities of information asset protection and security...

SELF ASSESSMENT

Self assessment is where you ask yourself certain questions to ensure you have understood what you have learned while reading this manual and completing the learning activities. This unit requires you the student or trainee at the completion of your training to have a certain level of 'Required Knowledge' in which you would need to have acquired and in which you will be assessed on. This self assessment section reviews this required knowledge by way of questions and if you are able to say YES to all of them you can be confident your assessment will be satisfactory.

- ☆ This training unit had four sections each reviewing on how to protect and secure information assets. After reviewing the information in Section One, are you confident that you understand and could:
    1) Identify information assets in the organisation?
    2) Identify and record mechanisms by which information assets are accessed, transmitted and stored?
    3) Identify nature of threats to information assets and determine threat impact according to organisational processes?
- ☆ After reviewing the information in Section Two, are you confident that you understand and could:
    1) Identify and confirm actions, mechanisms and strategies to protect information assets with required personnel?
    2) Secure assets according to organisational procedures?
    3) Report outcomes and escalate issues to required personnel?
- ☆ After reviewing the information in Section Three, are you confident that you understand and could:
    1) Identify signs and evidence that information assets are threatened or undergoing loss or damage?
    2) Provide first level response to reduce effects, mitigate damage and protect evidence?
    3) Report incident, resulting effects and actions taken to required personnel?
- ☆ After reviewing the information in Section Four, are you confident that you understand and could:
    1) Finalise documentation outlining current state of information assets according to organisational procedures?
    2) Save, store and back up reports according to organisational procedures?
    3) Maintain records and reports of information assets according to organisational procedures?

If there were any questions that you were unable to confidently say YES to, we encourage you to review the information again in this manual and if needed seek the assistance of your teacher or trainer.

NOTES