



CSE5ISM CYBERSECURITY INCIDENT MANAGEMENT Week 7-8

Dr Kayes

April 2025 (lectures and tutorials)

Discussion

Week 1 - 6

- IRP phases.
- Business and technical measures.
- Understand the vulnerabilities in business processes, severity hierarchy of information security incidents, classification and categorisation of cybersecurity incidents.
- IRP, BCP & DRP: Are they the same or are they serving different purposes? What are the key risks associated with cyber incidents?
- BCP phases/elements.
- Which international standards are relevant to the design and implementation of incident response and business continuity plannings?

Week 7-8: lecture outline

Legal and regulatory compliance in security incident management

- Understand the **GDPR** (General Data Protection Regulation) and **NDB** (Notifiable Data Breach) regulations
- GDPR (European)
- NDB (Australian)
- Understand the importance of **investigating and documenting** security incidents
- Determine the **appropriate response and cause** adhering to **legal, regulatory, and organisational requirements**
- Formulate **legal and regulatory compliance strategies** to support incident management

Week 9-10: lecture outline

Organize, train and equip Incident Response Team (IRT)

- **Structure** of a typical incident response team
- **Establish a strategy** to organise, train and equip an incident response team in responding to cybersecurity incidents in an **effective and timely manner**
- Periodic **testing, reviewing and revising** (as applicable) the incident response plan
- Establish a **Crisis Communication Plan (CCP)** and processes to manage communication with internal and external entities

Reading Materials

- Privacy Act 1988, No. 119 (Cth) - The Australian Privacy Principles (APPs)
- Notifiable Data Breaches (NDB) scheme in Australia, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
- Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>
- EU General Data Protection Regulation (GDPR), <https://gdpr-info.eu/>

Privacy Act 1988

<https://www.oaic.gov.au/privacy/the-privacy-act/>

- To promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information.
- There are 13 Australian Privacy Principles (APPs) in schedule 1 of the Privacy Act.
- The APP outline how organisations must handle, use and manage personal information or personally identifiable information (PII).
- The Act applies to most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses (collectively called 'APP entities').
- The Privacy Act applies to businesses that are incorporated in Australia. It also applies to businesses outside Australia if they collect personal information from, or hold personal information in, Australia and carry on a business in Australia.
- The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

Organisations providing a health service

- traditional health service providers
 - such as private hospitals
 - day surgeries
 - medical practitioners
 - pharmacists and
 - allied health professionals
- complementary therapists
 - physios
 - naturopaths and
 - chiropractors
- gyms and weight loss clinics
- childcare centres and private schools

Handling of My Health Record (MHR)

- Regulated by Office of the Australian Information Commissioner (OAIC)
- My Health Record
 - Summary of an individual's health information.
 - Who can access: Doctors, hospitals and certain other healthcare providers (such as a physiotherapist), and an individuals.
 - Laws: The My Health Records Act 2012; Health Records Rule 2016 and My Health Records Regulation 2012.
 - Regulates when and how health information included in a My Health Record can be collected, used and disclosed.

Handling of Healthcare Identifiers

- Regulated by Office of the Australian Information Commissioner (OAIC)
- Healthcare identifiers
 - **Individual Healthcare Identifiers (IHI)** – for individuals receiving healthcare in Australia
 - **Healthcare Provider Identifier – Individual (HPI-I)** – for individual healthcare providers, such as GPs, allied health professionals, nurses, dentists and pharmacists
 - **Healthcare Provider Identifier – Organisation (HPI-O)** – for organisations delivering healthcare, such as hospitals and general practices
- Laws:
 - the **Healthcare Identifiers Act 2010** (HI Act)
 - Assigning unique identifiers to individuals, healthcare providers, and healthcare provider organisations.
 - and the **Healthcare Identifiers Regulations 2010**
 - Collection, use and disclosure of identifying information and healthcare identifiers

Privacy Act 1988, No. 119 – 13 The Australian Privacy Principles (APP)

- APPs are obligations for the management of personal information.

1. open and transparent management of personal information;
2. anonymity and pseudonymity;
3. collection of solicited personal information;
4. dealing with unsolicited personal information;
5. notification of the collection of personal information;
6. use or disclosure of personal information;
7. direct marketing;

8. cross-border disclosure of personal information;
9. adoption, use or disclosure of government related identifiers;
10. quality of personal information;
11. security of personal information;
12. access to personal information; and
13. correction of personal information.

Privacy Amendment (Notifiable Data Breaches - NDB) Act 2017 No. 12, 2017

- The NDB applies to Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of \$3 million or more, credit reporting bodies, health service providers, and TFN recipients.
- applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. (eligible data breaches) – must be notified to affected parties
 - a device containing customers' personal information is lost or stolen
 - a database containing personal information is hacked
 - personal information is mistakenly provided to the wrong person.
- Data breach preparation and response guide
 - discuss the Privacy Act
 - prepare a data breach response strategy
 - guidance on the mandatory (eligible) data breach reporting and assessment

Source: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>

Personal Information Data Breach

- Personal information that a person holds is subject to **unauthorised access or disclosure, or is lost**.
- **Personal information** is
 - information about an identified individual, or
 - an individual who is reasonably identifiable.
 - Partial information of an individual on its own can become personal information when it is **combined** with other information -> reasonably identifiable.
- **Data Breach** is **a malicious action** (by an external or insider party), **human error**, or **a failure in information handling or security systems** can include:
 - **loss or theft of physical devices** (laptops and storage devices) or paper records that contain personal information
 - **unauthorised access** to personal information by an employee
 - **inadvertent disclosure** of personal information due to 'human error', for example an email sent to the wrong person
 - disclosure of an individual's personal information to a **scammer**, as a result of inadequate identity verification procedures

Personal Information Data Breach (cont...)

- **Personal information** is
 - information about an identified individual, or
 - an individual who is reasonably identifiable
 - **Personally Identifiable Information (PII)**
 - **Partial information** of an individual on its own can become personal information when it is **combined** with other information -> reasonably identifiable.
- **Examples:**
 - **Name + Address/Location: PII**
 - **DOB + Name: PII**
 - **ID**

Personal Information Data Breach (cont...)

- An excerpt of the privacy rules to facilitate privacy preservation of the client – “Kayes et al., **Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control**, Future Generation of Computer Systems journal, Elsevier, vol. 107, pp. 307-323, 2020”
- **Examples:**
 - **Name/DOB**
 - **Address/Location**
 - **ID**

Eligible Data Breach - Privacy Amendment (Notifiable Data Breaches) Act 2017

- A. there is **unauthorised access** to, **unauthorised disclosure** of, or **loss** of, **personal information** held by an entity; and
- B. the access, disclosure or loss is likely to **result in serious harm** to any of the individuals to whom the information relates.

An **entity must give a notification if:**

- a) it has **reasonable grounds** to believe that an eligible data breach has happened; or
- b) it is **directed to do so** by the Commissioner.

Watch this video – EU GDPR



<https://www.youtube.com/watch?v=vaYAaFJhYig>

EU General Data Protection Regulation (GDPR)

- Effective from **25 May 2018**
- Apply to ALL Australian businesses,
 - if they have **an establishment in the EU,**
 - if they **offer goods and services in the EU,** or
 - if they **monitor the behaviours of individuals in the EU.**
- Include requirements that resemble those in the Privacy Act 1988,
- and additional measures aim to foster **transparent information handling practices** and **business accountability** around **data handling.**
- Businesses must take steps to implement any necessary changes to ensure compliance.

Australian businesses that may be covered by the GRPR

- an Australian business with an office in the EU
- an Australian business whose website targets EU customers
 - The web site enables customers to order goods or services in a European language (other than English) or enabling payment in euros
- an Australian business whose website mentions customers or users in the EU
- an Australian business that tracks individuals in the EU on the internet and
 - uses data processing techniques to profile individuals to analyse and predict personal preferences, behaviours and attitudes

GDPR Personal Data

- Applies to “any information relating to an identified or identifiable natural person”.
- Under the GDPR, **additional protections** apply to:
 - the processing of ‘special categories’ of personal data, which includes:
 - personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership**, and the processing of **genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation**
 - Additional protections also apply to similar categories of **‘sensitive information’** in
 - the APP 3.3 (collection of solicited personal information),
 - APP 6.2(a) (use or disclosure of personal information) and
 - APP 7.4 (direct marketing).

GDPR Consent

- Govern the **operations & restrictions on handling personal data**
- Personal data may only be processed under the GDPR, if one of the 'conditions for processing' such as the individual **'has given consent to the processing of his or her personal data for one or more specific purposes'**
- **'Explicit consent'** is generally required to process

GDPR Expanded rights for individuals

- The **right to erasure** (right to be forgotten) gives individuals a right to require data controllers to delete their data in certain circumstances
- Exceptions to this right, including where data processing is necessary to exercise the right of freedom of expression and information.
- The **right to object** at any time to the processing of an individual's personal data (including profiling). If an objection is made, the controller must generally stop the data processing.
- A right to **data portability**—a right to receive personal data an individual has provided to a controller in a 'structured, commonly used, machine-readable format' and to transmit that data to another controller, where the data is processed electronically.
- A right to **restriction of processing**—in certain circumstances an individual has the right to obtain a restriction on processing of their personal data from the controller.
 - For example, if an individual contests the accuracy of their personal data, there may be a temporary restriction on processing to enable the controller to verify the accuracy of the personal data (Article 18).

GDPR Mandatory data breach notification

- In an incident of data breach and the notification:
- Data breach **notification** must be performed by **data controllers** to advise the relevant supervisory authority of a data breach **within 72 hours** of becoming aware of the breach;
- unless the breach is unlikely to result in a high risk to the rights and freedoms of individuals.
- **Data processors** must notify the **controller of a breach** without undue delay (Article 33).
- In addition, when a data breach is likely to result in a **high risk** to the rights and freedoms of natural persons,
 - the **controller** must **notify the individual** without undue delay (Article 34).

ISACA COBIT 5 GDPR Processes

- Source: I. Cook (2019) IS Audit Basics: Assurance Considerations for Ongoing GDPR Conformance, ISACA Journal
- COBIT: Controlled Objectives for Information Technologies
- COBIT 5: released in 2012
- It provides an end-to-end business view of the governance that reflects the role of data/information

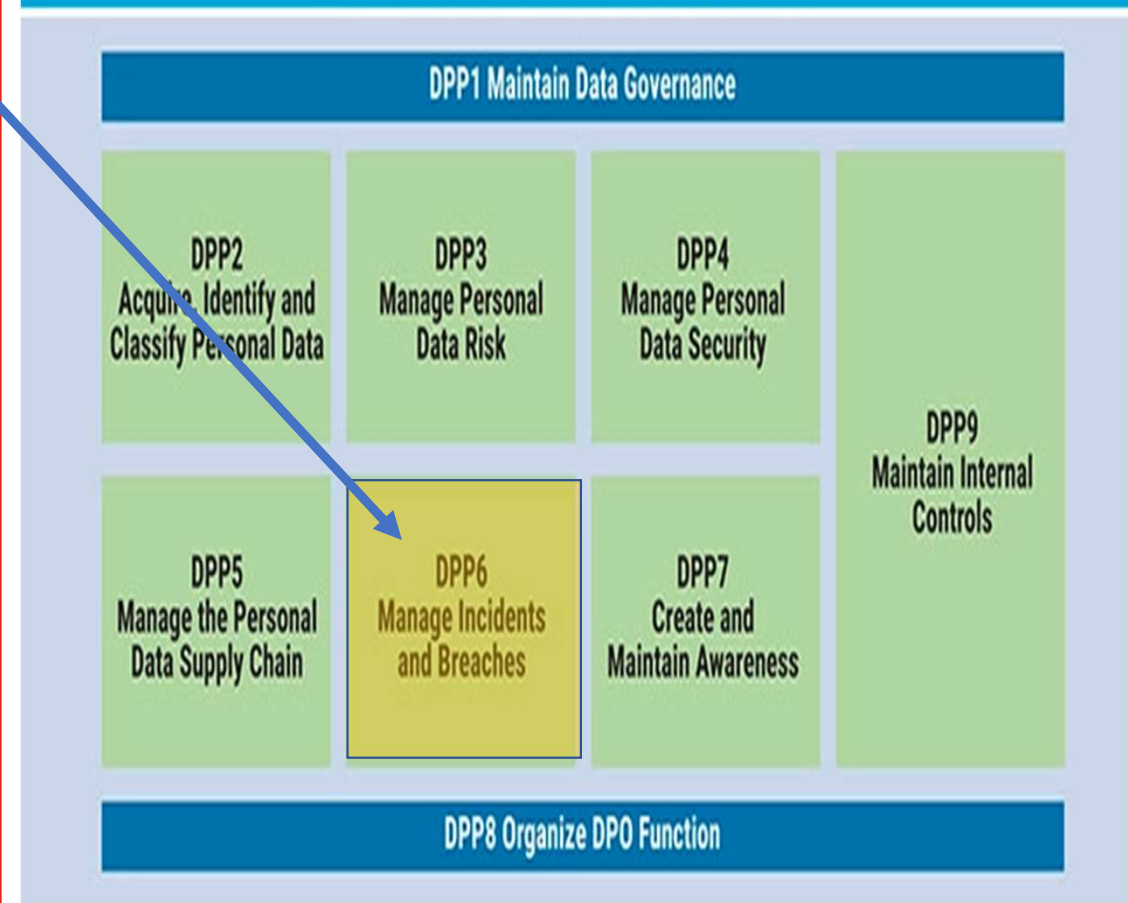
ISACA COBIT 5 GDPR Processes

Source: I. Cook (2019) IS Audit Basics: Assurance Considerations for Ongoing GDPR Conformance, ISACA Journal

DPP6—Manage Incidents and Breaches

- Data protection-related incidents and breaches must be reported in line with GDPR.
- **Notification of supervisory authorities** and **communications with data subjects** actually or potentially affected by the breach.
- **Assurance** concerns include:
 - **Breach notification process** meet GDPR requirements (e.g., within 72 hours)
 - **Notification of data subjects** satisfy the mandatory GDPR requirements
 - **An incident and crisis management process** is in place
 - Processes are in place to **secure evidence and for substantiating or defending against claims** resulting from the incident or breach.

Figure 1—Data Protection and Privacy Process Model



DBIR: Responding to data breach incidents

Contain -> Assess -> Notify -> Review

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

DBIR: Responding to data breach incidents

Contain -> Assess -> Notify -> Review

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

Contain -> Assess -> Notify -> Review

NO

Is serious harm still likely?

YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review


Review the incident and take action to prevent future breaches. This may include:


- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

**Australian Government**
Office of the Australian Information Commissioner

Need Help 


Getting Started

Part one

Part two

Review and submit

[Return to a saved form](#)

Save For Later 

Notifiable Data Breach Form

*Fields marked with * are required*

About this form

Notifiable Data Breach statement

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the Privacy Act 1988.

Part one is the 'statement' about a data breach required by section 26WK of the Privacy Act. If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

Discussion/Examples

Study the Notifiable data breach form.

For **each type of the data breach**, discuss about **how relevant it is for a person** in regard to what situation that each of the six types of the data breach would be affected.

☐ Financial details

☐ Tax File Number (TFN)

☐ Identity information

(e.g. Centrelink Reference Number, passport number, driver license number)

☐ Contact information

(e.g. home address, phone number, email address)

☐ Health information

☐ Other sensitive information

(e.g. sexual orientation, political or religious views)

Legal and regulatory compliance strategies in Incident Management

- Understand the legal and regulatory requirements
- GDPR Requirements
 - GDPR has a significantly more **stringent set of regulations and a much steeper penalty for non-compliance** (up to 4 percent of annual global turnover or 20M Euro, whichever is greater).
- NDB Requirements
 - An organisation has **30 days** to assess whether a data breach is likely to result in serious harm.
 - The organisation must promptly notify any individual at risk of serious harm and must also notify OAIC.
- Privacy Act 1988 (13 APPs)
- There are many other security standards/acts that businesses must meet (subject to business type),
 - AUSTRAC AML/CTF governance obligations
 - The Payment Card Industry Data Security Standards (PCI-DSS) for organisations that handle credit card information

Other Acts

- **Security of Critical Infrastructure Act** 2018 No. 29, 2018
 - managing **risks** to critical infrastructure assets for national security purposes.
- **Spam Act 2003** No. 129, 2003 (Cth)
 - **unsolicited commercial electronic messages** must not be sent.
 - Commercial electronic messages must include **information about the individual or organisation who authorised the sending** of the message.
- **Cybercrime Act 2001** Act No. 161 of 2001
 - It is a crime to use **telecommunications services to modify any data held on a computer** without any authorisation, or whether such modification impairs the reliability, security or operation of the data.
 - It is a crime to **facilitate the modification of the data and to possess or control such data**.
- **Common Law Requirements**: The Roadshow Films Pty Ltd v Telstra Corporation Ltd [2016] FCA 1503
 - ISPs have **a duty to take reasonable steps to disable access to overseas websites**, known as online locations, that infringe or facilitate the infringement of copyright.

Legal Considerations When Creating an Incident Response Plan

Bryan Chou (2016) Legal Considerations When Creating an Incident Response Plan

<https://www.sans.org/reading-room/whitepapers/legal/legal-considerations-creating-incident-response-plan-37487>

- The IRP should include the following information, at a minimum:
- applicable law or regulation
- data breach trigger
- person or organisations to contact
- collecting evidence and information to include in reporting requirements
- follow specific steps for preserving the integrity of the data and documenting the chain of custody
- law enforcement should be contacted to improve the chances of prosecution

Incident Report

- Provide an **accurate picture of incident**
- Enables the organisation to prepare and respond appropriately.
- All staff to report all security Incidents
- Provide **Incident Recording**
 - The security personnel detecting, or receiving, information relating to a security incident
 - prompt compilation and submission of a security incident report in the prescribed format,
 - Alert more member of the organisation
- Ensure a formal security incident reporting procedure is followed

Contact Information and Incident	
Last Name: _____	First Name: _____
Job Title: _____	
Phone: _____	Alt Phone: _____
Mobile: _____	Pager: _____
Email: _____	Fax: _____

Incident General Information			
Incident #: _____	Source of Incident: _____	<input type="checkbox"/> External <input type="checkbox"/> Internal	Type of Incident: Malware
Date/Time of Incident Occurred: _____		Date/Time of Incident Detected: _____	
Campus/Site: _____		Severity Level: Low	
Impact Category: Campus Only	Confidential/Personal Identifiable Information Affected? <input type="checkbox"/> Yes <input type="checkbox"/> No		
Systems and Services Impacted: [Affected systems and services]			

Incident Summary
Comments

Incident Mitigation
Comments:

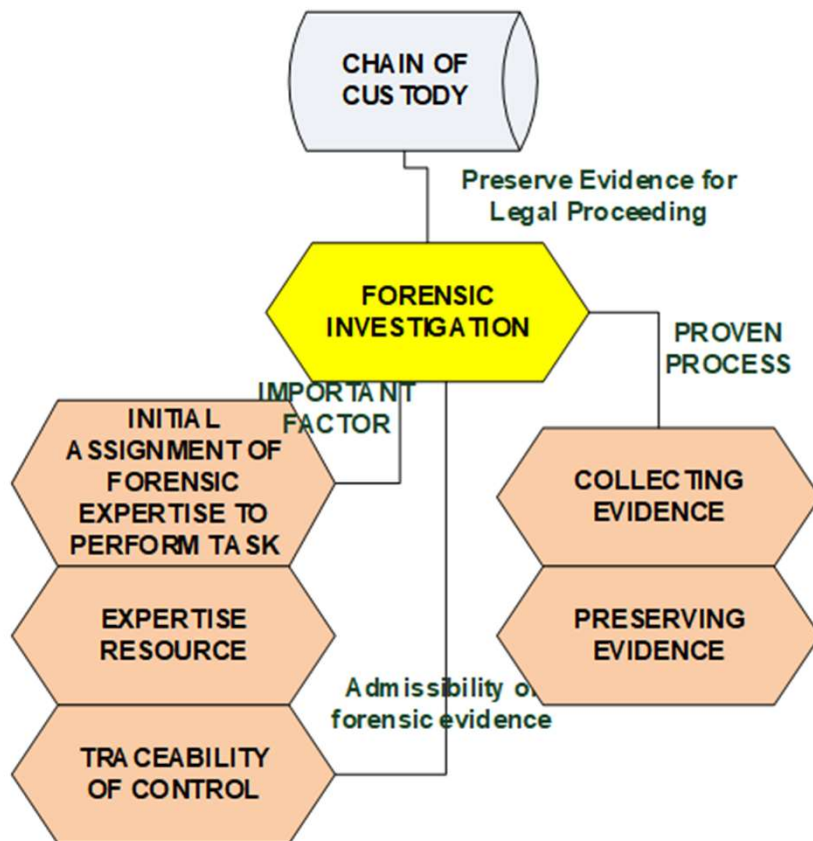
Recommendation
Comments: [Follow-on actions recommended to be taken, if any.]

Additional Comments/Notes
Comments: [Any additional notes, information or observations related to the security incident or this report.]

NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

- using **forensic techniques** to assist with computer **security incident response**
- practical **guidance** on performing **computer and network forensics**
- **processes** for performing effective forensics activities in support of incident response,
- provides **advice** regarding different data sources, including files, operating systems, network traffic, and applications.
- Provide **scenarios** involving the use of forensic techniques are also included as the basis for tabletop exercises.
- Provide advice regarding **techniques** to deal with data from many sources
 - For example, data can be stored or transferred by standard computer systems, networking equipment, computing peripherals, personal digital assistants (PDA), consumer electronic devices, and various types of media, among other sources.
- Enables digital forensic techniques can be used for purposes, such as **investigating crimes and internal policy violations, reconstructing computer security incidents, troubleshooting operational problems, and recovering from accidental system damage.**
- This guide provides detailed information on **establishing a forensic capability**, including the development of **policies and procedures**.

Forensic Investigation

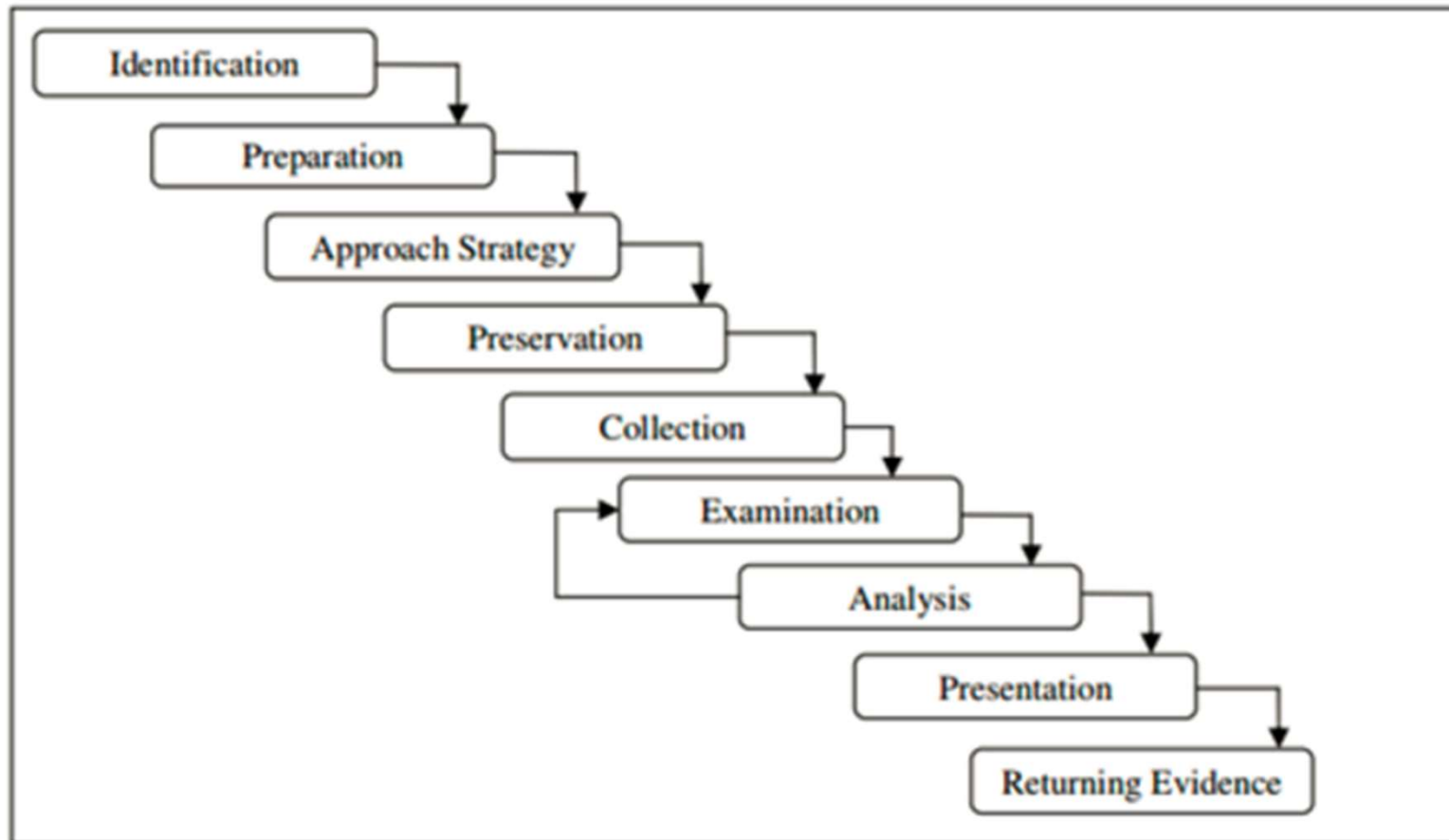


- The **science** of **identifying, preserving, recovering, analysing and presenting facts** about **digital evidence** in the areas of computer hardware and operating systems, digital storage media, networks, and applications
- The **process** of **uncovering and interpreting electronic information**
 - To **preserve any original evidence**
 - To **perform structured investigation**
 - To **capture, identify, and validate** the digital information for the purpose of **reconstructing past events**

The three **A**s of Digital Forensic Investigation

- **Acquiring** the evidence while ensuring that the integrity is preserved
- **Authenticating** the validity of the extracted data, which involves making sure that it is as valid as the original
- **Analysing** the data while keeping its integrity

Digital Forensic Investigation Model (ADFM)



- <http://resources.infosecinstitute.com/digital-forensics-models/#gref>

Tute ACTIVITIES (Week 7-8)

These tutorial activities are focused on evaluating and proposing a business continuity plan.

- Students are required to interact with lecture materials, discuss case studies, read/watch videos about concepts of business continuity planning.
- Formulate legal and regulatory compliance strategies to support incident management to be incorporated in Assignment 4.
- Assignment 4 is to be prepared for developing a business continuity plan.

Activity 1

• Understand the Data breach preparation and response Plan

Go to the OIAC web site to study the “Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)”

<https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

The scenario is for a Web Hosting ISP in Sydney found a data breach happened two weeks ago with over 200,000 user records being stolen.

Read the whole document. Develop a Data Breach Response Plan and **use the checklist on page 18: Data breach response plan quick checklist** to discuss whether your response plan have addressed the relevant issues.

DBIR: Responding to data breach incidents

Contain -> Assess -> Notify -> Review

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

DBIR: Responding to data breach incidents

Contain -> Assess -> Notify -> Review

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

Contain -> Assess -> Notify -> Review

NO

Is serious harm still likely?

YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Activity 2

- Go to the OAIC web site, read the article “Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation”
- <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>
- Read the section: Mandatory data breach notification; Privacy notices; New direct obligations on data processors; and Sanctions
- The Scenario: An international social media platform “A” sold one million user’s personal information to a marketing company “B”. B has recently experienced an attack losing all the user information.
- Discuss in your group and present the steps involved in the Incident Management process.

Activity 3

• Understand the GDPR Regulations in Cybersecurity Incident Management

- Go to the OIAC web site to study the Privacy business resource 21: Australian businesses and the EU General Data Protection Regulations (GDPR)

<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>

- Discuss and prepare to present:
 - Who and what activities will the GDPR apply to?
 - What information does the GDPR apply to?
 - Contrast the difference between the EU GDPR and Australia Privacy Act
 - In response to a data breach incident, what are the likely chain of events that may have occurred in compliance to the GDPR?

Activity 4

Contrast Data Breach Response Plan from different organisations

- Read the “**Data Breach Response Plan**” issued by the University of Adelaide.

<https://www.adelaide.edu.au/policies/62/?dsn=policy.document;field=data;id=8225;m=view>

- **Compare and contrast** the one “**Code Green: Data Breach/Cyber Incident**” issued by La Trobe University.

<https://www.latrobe.edu.au/emergency/procedures/code-green-data-breachcyber-incident>

- Discuss and Submit your findings to the tutor. The discussion could be based on comprehensiveness, focused area of concerns, level of details, etc.

Activity 5

(1) Study the **Australian National University Incident report into the ANU data breach (2019)**

https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

(2) Briefly describe the tactics and techniques used by the attackers and why the attacks were successful.

(3) Suggest a list of possible critical infrastructure, operation processes and human factors in the case scenario that are being affected.

(4) Propose, argue, the appropriate **GDPR and NDB incidence response approaches** why or why not, may or may not need to be incorporated in the response.

(5) Discuss the importance of **investigating and documenting information security incidents** to determine the appropriate response and cause in this ANU incident.

(6) Discuss the legal, regulatory compliance and organisational strategy to support incident management of this type of data breach.

Activity 6

Work with an open source Security Information and Event Management (SEIM) system:

AT&T Cybersecurity AlienVault® OSSIM

- Go to the AT&T AlienValut OSSIM Web Page
- <https://cybersecurity.att.com/products/ossim>
- You may download the ISO Image or click on the Online Demo button
- Go through each of the topics to familiarise yourself with an SEIM



Navigate Unified Security Management (USM)

Discover key views, dashboards, and more, and learn where to find and how to navigate between them



Detect & Investigate Threats

Quickly detect and investigate intrusions and anomalies across your on-premises and cloud assets, all from a single pane of glass



Identify & Assess Your Vulnerabilities

Understand which of your assets are at risk from vulnerabilities, and identify the level of risk and any available patches



Monitor Your Endpoint Devices

Continually monitor your endpoints to protect against advanced threats that can evade traditional endpoint prevention and protections tools



See You

Next Session

latrobe.edu.au