CSE5ISM: CYBERSECURITY INCIDENT MANAGEMENT

Semester 1, 2025

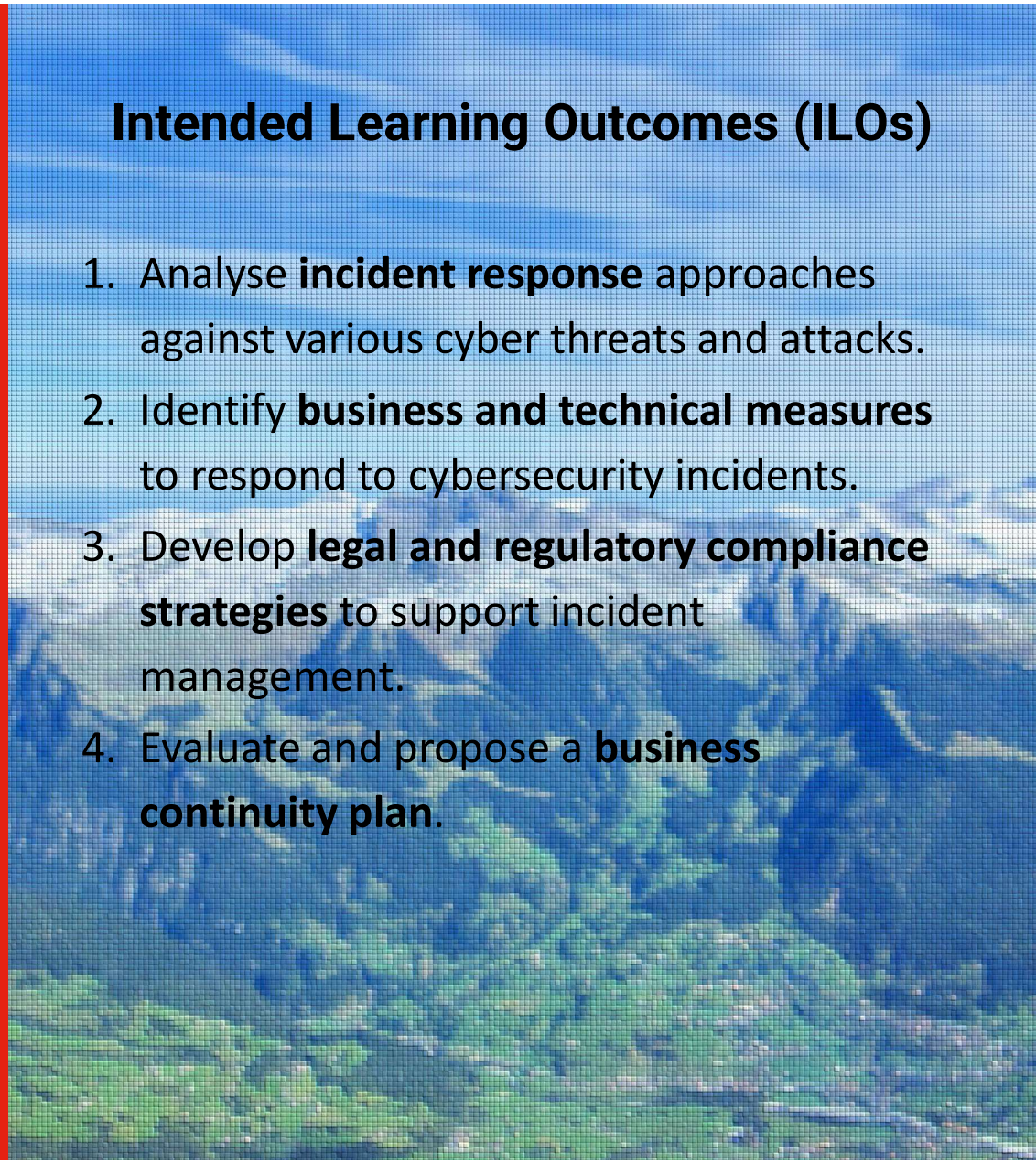
Week 1-2 (lectures and tutorials)

Dr ASM (Kayes) Kayes, Senior Lecturer in Cybersecurity

05 March 2025 (Lecture 1) and 12 March 2025 (Lecture 2 & Tute 1)

What you will learn in this subject

- **Incident response Plan (IRP)**
- Incident management
- **Tools and models** for attack/attacker identification and attribution
- **Business continuity plan (BCP)**
- **Disaster recovery plan (DRP)**
- **Data Breach Response Plan (DBRP)**
- Role played by law enforcement, **legal and regulatory compliance strategies**
- **Crisis Communication Plan (CCP)**
- **Incident Response Team (IRT)** roles and responsibilities



Intended Learning Outcomes (ILOs)

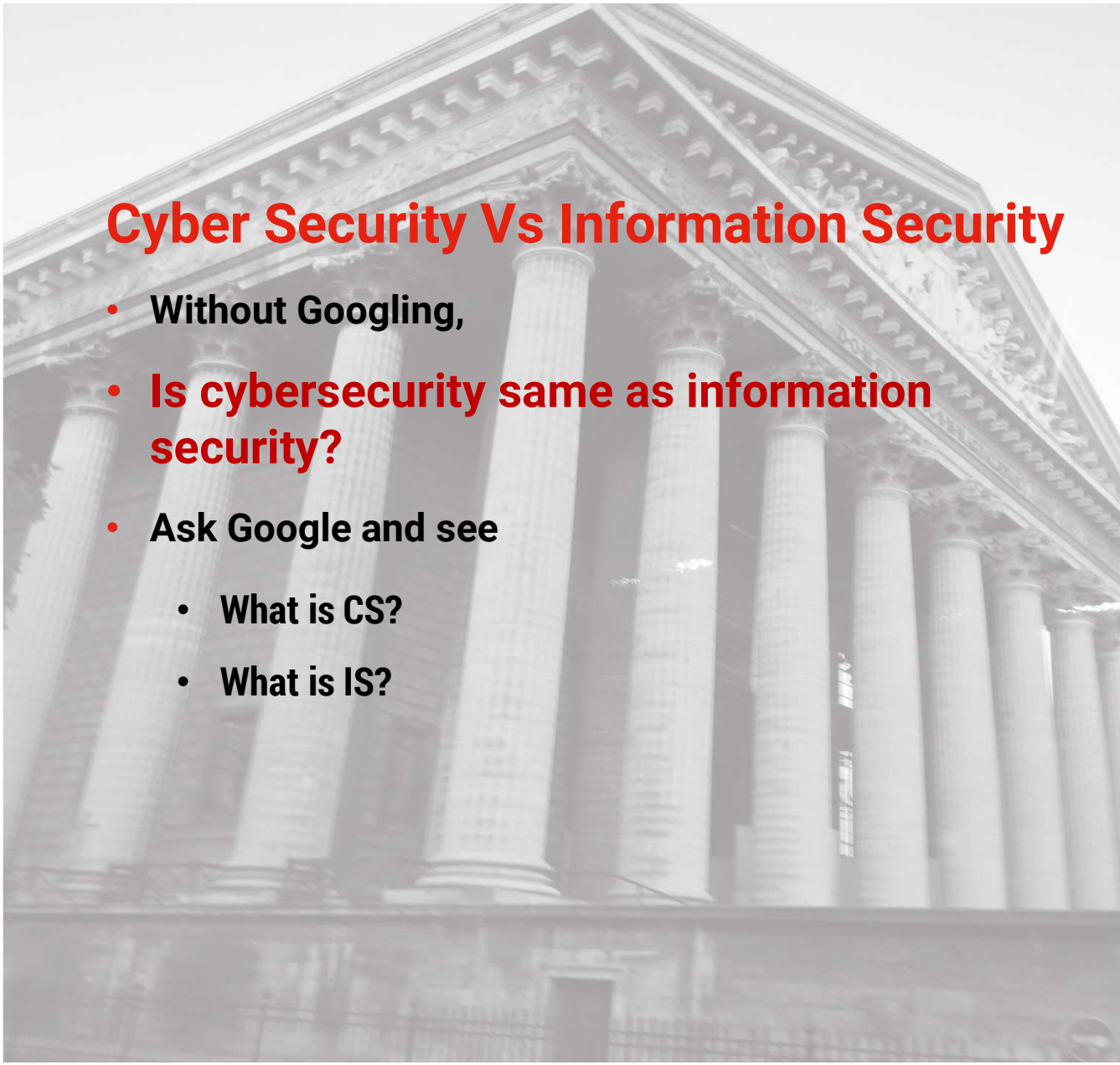
1. Analyse **incident response** approaches against various cyber threats and attacks.
2. Identify **business and technical measures** to respond to cybersecurity incidents.
3. Develop **legal and regulatory compliance strategies** to support incident management.
4. Evaluate and propose a **business continuity plan**.

Weeks 1 & 2: Incident response approach & concepts

Lecture Outline: Incident response approach & concepts

- Revision of Information Security Risk Management: impact and Likelihood
- The ISACA Information Security Incident Management body of knowledge
- Typical Incident Response Framework
- Overview of the ISO/IEC 27035:2016 — Information technology — Security techniques — Information security incident management
- Overview of the NIST 800-61 Computer Security Incident Handling Guide
- Understand the scope of Cybersecurity Incident Management
- Establish Cybersecurity Incident Response Plan/Management KPIs

Discussion



Cyber Security Vs Information Security

- Without Googling,
- **Is cybersecurity same as information security?**
- Ask Google and see
  - What is CS?
  - What is IS?

CSIM Vs ISIM

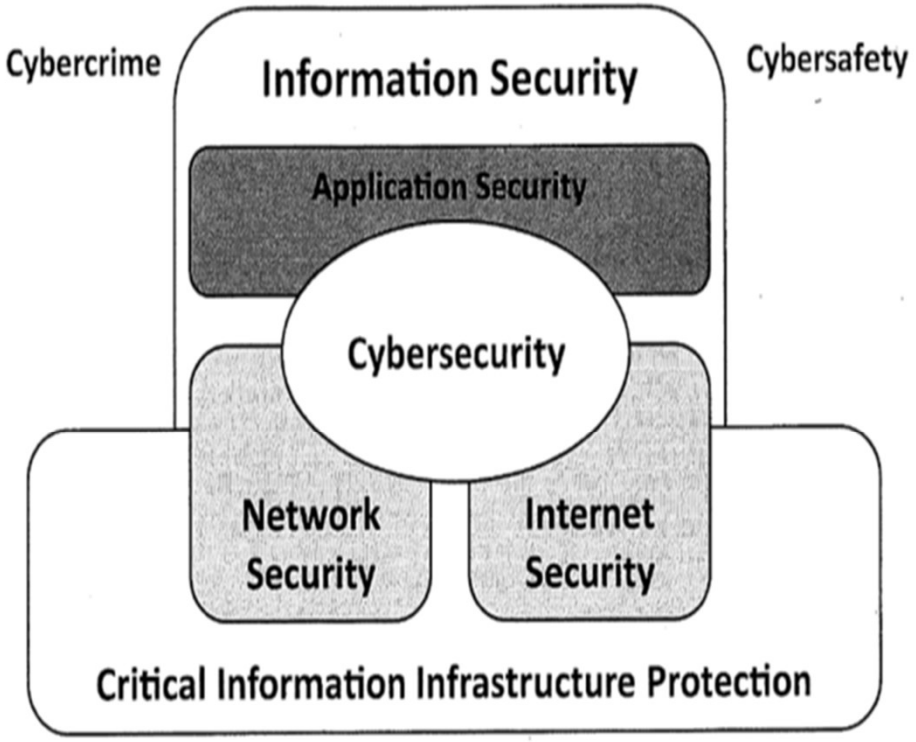


Figure 1 — Relationship between Cybersecurity and other security domains

(Source: 1ISO/IEC 27032:2012, p.11)

- ISIM will protect and respond to the **hardware server hosting important information against threats from natural and man-made disasters**.

- CSIM will protect and respond to the same **hardware server with the specific intention of preventing it from being hacked, while also ensuring that users are not harmed by cyber-theft or denial-of-service attacks**.

ISACA CISM Domain 4

Follow the standards and specifications that are widely used by the cybersecuirty professionals in handling Information Security Incident Management.

Incident management involves all the actions taken prior to (including testing and planning), during, and after an information security incident occurs – ISACA Incident Management and Response.

ISACA CISM Domain Structure

ISACA CISM Domain 4: Task

4.1 Define severity hierarchy, accurate classification and response to incidents.

4.2 Incident response plan.

4.3 Processes to identify incidents.

4.4 Processes to investigate and document incidents.

4.5 Incident notification and escalation processes.

4.6 Training incident response team.

4.7 Test, review and revise the incident response plan periodically.

4.8 Communication with internal and external entities.

4.9 Conduct post incident review.

4.10 Integration among the incident response plan, business continuity plan and disaster recovery plan.

ISACA CISM Domain 4: Knowledge

k4.1 Incident management concepts and practices

k4.2 Incident response plan (IRP)

k4.3 Business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan

k4.4 Incident classification/categorization methods

k4.5 Incident containment

k4.6 Notification and escalation processes

k4.7 Roles and responsibilities in identifying and managing IS incidents

k4.8 Types and sources of training, tools and equipments

k4.9 Forensic requirements and capabilities for collecting, preserving and presenting evidence

k4.10 Internal and external incident reporting

k4.11 Postincident review practices and investigations

k4.12 Techniques to quantify damages, costs and other business impacts arising from information security incidents

k4.13 Technologies and processes to detect, log, analyze and document information security events

k4.14 Internal and external resources available to investigate information security incidents

k4.15 Methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process

k4.16 Techniques to test the incident response plan

k4.17 Regulatory, legal and organization requirements

k4.18 Key indicators/metrics to evaluate the effectiveness of the incident response plan

Discussion: Know the Difference

- Vulnerability
- Incident
- Breach

Know the Difference

- Vulnerability
  - Weakness in internal controls, the information system, the implementation, or system security procedures that can potentially be exploited by threats.
- Incident
  - A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach
  - An incident that results in the confirmed disclosure—not just potential exposure of data to an unauthorized party – privacy breaches – MHR/Westpac PayID/Optus/Medibank data breaches.

About Incident Response

- A cybersecurity management program helps mitigate risk to an organization, but inevitably there will be a breach of controls that requires investigation.
- Preparation is key – you don't want to be figuring out what to do in the middle of an incident.
- Investigations are typically an iterative hunt for clues, building up to a (hopefully complete) picture of what happened.
- Once the incident is understood, remediation can take place and processes improved based on lessons learned.
- We will look at a typical framework of steps that most investigations follow.

Cybersecurity Incident Response Program

- the process by which an organisation handles a data breach or cyberattack,
- the ways and steps to be taken by the organization attempts to manage the consequences of the attack or breach (the “incident”).
- the goal is to effectively manage the incident
  - To contain or limit the damage to a minimum acceptable level
    - the cost to the business,
    - recovery time,
    - Any collateral damage such as brand reputation; and legal liabilities.

https://www.staysmartonline.gov.au/protect-your-business/recover-when-things-go-wrong/incident-response-plans

ACSC Incident Response Plan (IRP)

- Analysis of the threat environment (likelihood and severity of potential incidents).
- Identification of key assets, data and critical systems.
- Plans for each major incident type and different types of data that could be compromised.
- Key roles and responsibilities of management and staff.
- Key tools including contact lists, checklists and guides for use during the response.
- Process for alerting necessary stakeholders including board members, suppliers, external agencies that may be impacted and the Australian Cyber Security Centre (ACSC).
- Public relations and media management.
- Arrangements to regularly review and exercise the plan.
- Post incident review and reporting. Lessons learned and update the incident response plan to improve effectiveness in the future.
- Others: Personal impact; Legal exposure; Business consultation

Typical Incident Response – steps

1. **Preparation**
2. **A cycle of:**
   - **Detection & Identification of compromised systems**
   - **Intelligence development, Containment**
3. **Remediation**
4. **Recovery/refresh**
5. **Lessons Learned**

Step 1: Preparation

Prepare People

- Select and train staff for appropriate roles.
- Some potentially dedicated e.g. incident responders.
- Some fulfilling other roles between incidents, e.g. Risk team.
- May be a mix of internal staff and outsourced Security Service Providers.
- Practice working together with incident exercises.
- Maintain a directory of contacts and mailing lists of people likely to be involved in responding to, or being notified of, security incidents.

Crisis Team

- Assign a "War Room" with management team to manage serious incidents (Ideally C-Suite members)
- An Incident Manager (facilitator) and a minute taker
- Business Interface Manager
- Incident Response Technical Manager/team lead
- Legal, Compliance, Privacy, Risk
- Media Relations
- Customer Support
- IT Department
- Human Resources Department
- Supplier Management

Prepare Processes

- Playbooks – procedures to follow depending on incident type.
- Communication matrix (who to talk to, when, and ***how*** – more on that later).
- Communication templates (e.g. situation summary, status updates).
- Asset Management (know what infrastructure is where).
- Data Management (know what data is where).
- Crown Jewels (know what systems and data are essential to the business).
- Map IT infrastructure to the business processes and services to help determining business impact during an incident.
- Keep these plans secure - they would greatly benefit attackers!

Prepare Technology - logging

- The most common phrase in breach announcements is:
  - *"We have no evidence of data exfiltration"*
- This is the opposite of:
  - *"We have evidence there was no data exfiltration"*
- In other words, usually there is a lack of logging so investigations are inconclusive.
- So adequate logging from all systems and devices, ideally to centralized servers, is critical to incident response investigations.

Prepare Technology – security infrastructure

- **Security infrastructure**
  - Firewalls.
  - Proxy Servers.
  - Network Intrusion Prevention Systems.
  - Endpoint Detection and Response (EDR) Agents.
  - Antivirus agents.
  - Network and email sandboxes.
  - Full Packet Capture (network “black box flight recorder”).
  - Security Information and Event Management system (SIEM) for centrally capturing, monitoring and correlating alerts from the security infrastructure.

Prepare Technology – tooling

- **Forensic tools for Incident Response, e.g.**
  - Disk imaging.
  - Memory dump analysis.
  - File system analysis.
  - Timelining (arranging events/logs/artefacts in a time sequence).

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Once a security incident is detected/suspected…..

- *There is a risk the hacker will steal data during the investigation.*
- *Identify your Crown Jewels and protect them NOW.*

Detection & Identification

- Security monitoring infrastructure may detect an anomaly.
- More often, however, an external party informs the organization of evidence that suggests they have been compromised.
- We first *try* to determine:
  - What kind of incident has occurred?
    - if any - it may be a false positive (false alarm).
  - What is its scope? What is the root cause?
  - Try to answer: What, When, Where, How, Who, Why (W5H).
  - Many of these questions may only be answered progressively during the investigation.

Live vs Forensic

- A Live response involves triaging and examining systems while they are still running.
  - Advantages: Faster, better context.
  - Disadvantages: May raise doubts about the impact of the investigation itself if any evidence is used later in court – the IR tools can "stomp all over the crime scene".
- A Forensic response involves shutting down systems and taking images (copies) of disks that can be proved (via checksums) to be identical to the original versions.
  - Advantages: More legally sound and complete.
  - Disadvantages: Much slower, may not be practical for large disk farms (Storage Area Networks).

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Intelligence development, Containment

- Looking at the Indicators of Compromise (IOCs - technical clues/alerts), experienced responders will get a feel for the nature of the attack.
- The IOCs may fit the pattern of a known threat actor or malicious campaign (Threat Intelligence).
- Such intelligence may guide placement of containment measures to limit the threat's scope, or at least have a "kill switch" ready in case the situation rapidly deteriorates.
- As evidence is found, it is iteratively fed back into the Detection stage to uncover more compromised systems.

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Remediation

- Once we have the full picture (potentially after many days or even weeks of investigation), we can execute a co-ordinated remediation of the threat combined with closing the vulnerabilities that led to the security incident.
- This is usually done in one hit – taking everything down, rebuilding systems, restoring backups, resetting passwords, patching, blocking known threats, etc, then bringing it all back up again in a clean and more secure state.

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Recovery/refresh

- Normal business operations are restored.
- Using the big injection of funding that typically comes after such a scare, further improve security controls and the overall security posture of the organization.
- Continue to monitor for signs of the threat actor returning.

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Lessons Learned

- What went wrong during the response?
- How can it be improved?
- What went right?
- Improve controls and playbooks based on Lessons Learned.
- Never waste a good incident! (make necessary changes to prevent the same thing from happening again)

Typical Incident Response – steps

1. Preparation
2. A cycle of:
   - Detection & Identification of compromised systems
   - Intelligence development, Containment
3. Remediation
4. Recovery/refresh
5. Lessons Learned

Thank You!

End of Lecture/Week 1

CSE5ISM: CYBERSECURITY INCIDENT MANAGEMENT

Semester 1, 2025

Assignment 1 Activities

Dr ASM (Kayes) Kayes

12 March 2025

A1
Activity 1

Please go through your Assignment 1 (A1) specification from the LMS:

(1) Check the IRP-related reading materials that mentioned in the specification.

(2) Identify the incident that you need to cover in your assignment 1.

(3) Identify some key resources (research and other articles from news, Google Scholar, and/or other portals) that you can refer in your report.

A1 Activity 2

Explore:

(1) The key IRP phases/steps.

(2) The possible KPIs.

(3) The comparative analysis of the existing IRP approaches, and their pros and cons.

A1 Activity 3

Investigate cyber incident:

(1) Medibank Cyber Incident.

(2) Is this a data breach?

(3) What are the root causes of this incident?

(4) Vulnerabilities?

(5) Possible measures by Medibank?

(6) And so on…

A1 Activity 4

Create your template - Assignment 1 report (1000 words, +/- 10% excluding references):

(1) Introduction

(2) Incident Response Planning (IRP) Approaches

(3) Conclusion

(4) References

A1 Activity 5

What to include in your report:

(1) **Criteria 1:** word limit (10% marks)

(2) **Criteria 2:** about incident (15% marks)

(3) **Criteria 3:** about organisation (15% marks)

(4) **Criteria 4:** about IRP phases/steps and relevant KPIs to investigate the incident (50% marks)

(5) **Criteria 5:** relevant references and justification of including them in the body of your report (10% marks)

Assignment 1 (Case Study 1: Westpac PayID Hack)

- Regarding the ACSC guideline, suggest a list of possible critical infrastructure, operation processes and human factors that are involved in the reported scenario of PayID incident. You should propose or argue, stating the appropriate incident response approaches - why or why not them need to be incorporated in the response.
- Study articles about PayID hack reported in the news in June and August 2019.
- A succinct discussion of what had happened to the “PayID hack” during the cyber-attack incidence reported in the news in June and August 2019.
- Describe the environment of the banks for possible critical infrastructure, operation processes and human factors that contributed to the “PayID hack”.
- State the reasons why the proposed incidence response approaches able to deal with the incident effectively.
- Refer to the relevant reading materials with proper justification in the body of the report, to support their argument(s).

Case Study 2: Australian MHR System

- Australian MHR (My Health Record) System - is a new initiative in Australia to put all patients' records (e.g., demographic data, daily medical records, previous medical information, diagnosis data, insurance information, and so on) into one place.
- The MHR is a software system that will allow different parties to communicate securely and provide reliable services to patients.
- A core MHR system is built to collect and maintain data and information about the patients, doctors, nurses, specialists, medical receptionists, and so on.
- The MHR system controls our health information securely in one place. It is really our choice - we can keep our MHR with basic information, or we can allow more information to MHR users or permanently delete the record.
- MHR user is an individual who has right to use patients' health information.
- A doctor can issue a prescription if the patient asks for one. A doctor also can recommend the patient to medical specialists. A doctor can access a patient's medical records that are stored into the MHR database.

Case Study 2: MHR System and Data Breaches

- The number of data breaches involving MHR system reduced marginally from 42 to 38 in 2019 and it has been impacting Australian economy every year.
- According to a review by the national audit office, the MHR system already costed nearly $2 billion, however, it became almost an “opt-out” system.
- A data breach can be seen in multiple ways, such as, according to the MHR affected customers, an unauthorised access to patients’ information and a suspicious fraud due to unauthorised Medicare claim. (data breach, C & I issues; identity theft)
- Other incidents like “wrong parents’ details entered into the database” also seen in the MHR system. (human error)
- In addition, unseen data breaches like unauthorised access to sensitive or private health information without patients’ pre-approvals and sharing health information with untrusted parties, such as with third-party apps and sites and other professionals.

Case Study 2: MHR Incidents and Root Causes

- One of the major causes of data breaches is fundamentally the failure of appropriate access control.
- Another subsequent cause of this problem is the unawareness of cybersecurity risks, that is, the lack of user understanding and awareness about the need for proper access control has undoubtedly contributed to the rise of data breaches in MHR system.
- Also, most users (i.e., Australians) incorrectly making access control decisions, typically, they could not appropriately access their electronic health records, or most users had not set a strong PIN number to protect their information.
- Users might select default PIN numbers that make their work life easy, rather than those which might meet security requirements.

Case Study 2: MHR Incidents and Remedy (cont…)

- In the current MHR system, currently medical professionals who have authorities to access patients' health record can ask for more information for treatment and diagnosis purposes, which can be seen as a primary access/use of MHR. The health record cannot be allowed as secondary access like for marketing purpose, which can be seen as a data breach. An appropriate security policy (access control model) should be built/applied.
- Users are skeptical about how access control systems work at all, witness the MHR debacle, where millions of users already opted out of the system;
  - because they either didn't understand how their data were protected;
  - or they didn't trust the traditional access control mechanisms that can protected their data.
- Thus there is a need for an ethical/trustworthy model, that should be incorporated with security policy, as well as cyber awareness training and education.

Incident Response

- **Reactive**
- **Primary focus on what/how/when to react**
- **Technical components**
- **Identify / Detect**
- **Containment**
- **Remedy**
- **Analyse**
- **Report**

Incident Management

- Proactive
- A framework managing the complete life cycle of an incident
- Keeping record of specific information about events occurring that could lead to a loss of operations, services, or functionality
- Comprises the processes of Incident Response (ie. identifying, categorizing, investigating, and remedying any losses)
- Involves deploying plans to respond appropriately to the incident
- Reporting on the outcomes of each response implementation
- Regular enhancements

Incident Response/Management Frameworks

- ISO/IEC 27035:2016: Information Security Incident Management
- NIST 800-61: Computer Security Incident Handling Guide
- ISACA: Incident Management and Response, and
  - ISACA: Responding to Targeted Cyberattacks
- CERT: Handbook for Computer Security Incident Response Teams (CSIRTs)
- CREST: Cyber Security Incident Response Guide
- ENISA: CSIRT Setting up Guide, and
  - ENISA: Good Practice Guide for Incident Management

ISO/IEC 27035:2016: A Summary

- Part 1: Principles of incident management (IM)
  - Basic concepts, benefits, and objectives of IM
  - An overview of different phases in IM (Plan & Prepare, Detection & Reporting, Assessment & Decision, Responses, and Lessons Learnt)
- Part 2: Guidelines to plan and prepare for incident response (IR)

ISO/IEC 27035-1:2016

Objectives of incident management:

- effective detection of information security events
- appropriate assessment of such events
- efficient incident response
- minimization of adverse effect of incidents on business operations
- supportive vulnerability management
- learning from incidents

Goals of incident management:

- improve information security, prioritization of actions, the quality of evidence, risk management, security awareness, security policies and procedures
- reduce business impacts, strengthening focus on prevention, budget, and resource justification

ISO/IEC 27035-2:2016

When is an Incident Response Plan needed?

- an information security event is detected; and
- an information security vulnerability is detected.

Incident Response Plan must cover procedures for:

- vulnerability reporting;
- event/incident reporting; and
- incident handling cycle.

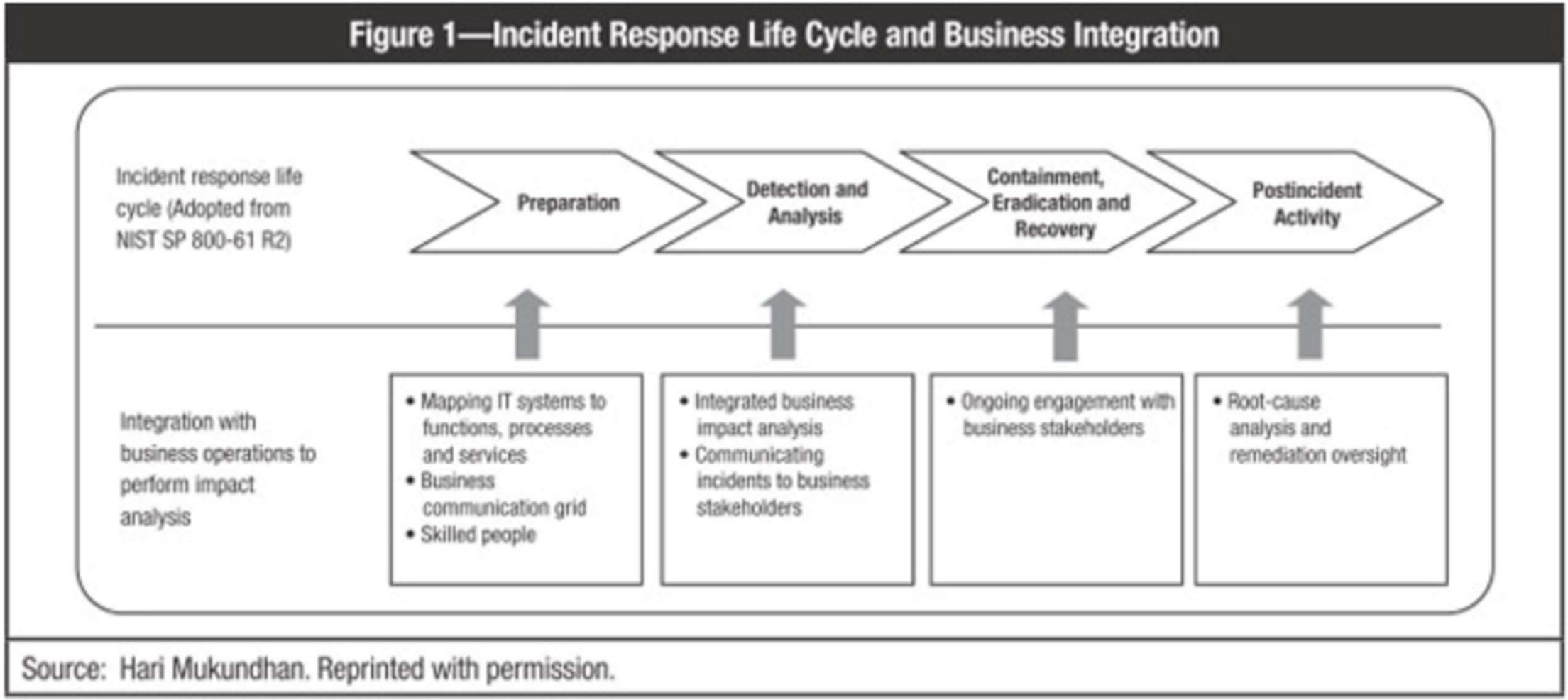
NIST 800-61: Computer Security Incident Handling Guide

- Many U.S. organizations use the NIST Framework
- Four Phases: Preparation -> Detection and analysis -> Containment, eradication and recovery -> Post-incident activity

The specification: NIST 800-61: Computer Security Incident Handling Guide:

- Common Sources of Precursors and Indicators: steps to investigate incidents.
- Incident Data: metrics/KPIS that are useful to apply.
- Incident Handling Checklist: ensuring a business can continue its normal operations after an incident.

A Business-integrated Approach to Incident Response
Hari Mukundhan, 2015



ISO/IEC 27035 vs NIST 800-61

Incident Management Cycle (phases/steps)

- Plan and Prepare
- Detection and Reporting
- Assessment and Decision
- Responses
- Lessons Learnt

- Preparation
- Detection and analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity

ISO/IEC 27035 vs NIST 800-61

Differences

- Emphasizes reporting together with detection
- More detailed in terms of incident categorization and classification
- Little information on information sharing

- Emphasizes analysis together with detection
- Emphasizes on Containment, Eradication, and Recovery
- Provides nine easy to understand steps of incident handling checklist
- One whole chapter on information sharing
- 11 scenarios for incident management planning

ISACA: Incident Management and Response

Phases	Activities
Planning and preparation	Policies, R&D, Checklists, Communication Plan, Awareness Trainings
Detection, triage and investigation	Implement IDS, IPS, & SIEM, Define, Detect & Prioritize events
Containment, analysis, tracking and recovery	Containment Strategy, Forensic Analysis, Recovery Procedures
Postincident assessment	Post-mortem, Reporting & Lessons Learned
Incident closure	Incident response post-mortem analysis & submitting reports to managements & authorities

Cybersecurity Incident Management Metrics / KPIs

Discussions

- Google “Cybersecurity Incident Management Metrics and KPIs” and list the Metrics and KPIs that you can find
- Discuss the Metrics and KPIs that you can find in the NIST 800-61 specification

What makes a good Metric?

- Measurable: items that can be measured
- Acceptable level of cost and time
- Transportable: can be applied to other scenarios and settings
- Relevant: align with core business goals
- Actionable: the metric can cause ongoing improvement
- Reliable: the metric is technically robust and repeatable to capture and can track progress over time
- Readable: specific, easy to understand and help make effective decisions

Metrics / Key Performance Indicators

Tips: beware of using percentages in too many cases; sometimes it is better to use absolute values

- Initial response time
- Average time required to resolve an incident (type, category, priority, impact, …)
- Average cost per incident
- % of incidents resolved at first line support
- % of incidents resolved by group: (level 1 service desk, level 2 support, level 3 support, external experts)
- % of incidents assigned more than twice
- Number of major incidents per month/year
- Size of unresolved incidents backlog
- Customer satisfaction at resolution

- Number of incidents without resolution method
- Number of incidents resolved remotely
- Number of incidents incorrectly assigned
- Number of incidents incorrectly categorised
- Number (or %) of incidents handled by each incident model
- Number and type of reoccurring incidents
- Time available for staff to work on incidents
- Number of resolution within SLA
- Number of incidents with associated problems

Source: ITIL – Incident management: Key Performance Indicators (KPIs) and reports

Activity: Scenarios

- Divide yourselves into equal teams.
- Each team are the Crisis Team of a business of national significance in an industry of your choice (i.e. An International Investment Bank)
- The AFP have passed on information from overseas “partners” that your network is communicating with a known malicious IP address in Eastern Europe.

Activity: Scenarios

- Divide yourselves into equal teams.
- Each team are the Crisis Team of a business of national significance in an industry of your choice (i.e. An International Investment Bank)
- The AFP have passed on information from overseas “partners” that your network is communicating with a known malicious IP address in Eastern Europe.
- Discuss and prepare to present:
  - What are your immediate actions?

Activity: Scenarios

- Divide yourselves into equal teams.
- Each team are the Crisis Team of a business of national significance in an industry of your choice (i.e. An International Investment Bank)
- The AFP have passed on information from overseas “partners” that your network is communicating with a known malicious IP address in Eastern Europe.
- Discuss and prepare to present:
  - What metrics will you use to handle this situation?

Activity: Scenarios

- Divide yourselves into equal teams.
- Each team are the Crisis Team of a business of national significance in an industry of your choice (i.e. An International Investment Bank)
- The AFP have passed on information from overseas “partners” that your network is communicating with a known malicious IP address in Eastern Europe.
- Discuss and prepare to present:
  - What internal and external pressure for answers do you expect and how will you manage them?

Activity: Scenarios

- Divide yourselves into equal teams.
- Each team are the Crisis Team of a business of national significance in an industry of your choice (i.e. An International Investment Bank)
- The AFP have passed on information from overseas “partners” that your network is communicating with a known malicious IP address in Eastern Europe.
- Discuss and prepare to present:
  - How will you manage the tasking and reporting back from various teams, and tracking/co-ordination of the overall investigation?

Week 2 Tute Activities (no tute in Week 1):

- Cyber Incidents
- Cybersecurity Incident Response Plan/Management KPIs
- Assignment 1

Tute Activity 1

Watch this video

“Behind the Scenes of a Cyber Incident” (40 minutes)

https://www.youtube.com/watch?v=83BgaI1p614

Discussion:

What are the tactics used by the attackers?

Which tactic is most effective and what is your suggested countermeasures?

ISACA: Incident Management and Response

Tute Activity 2

Discussions

- Read these two sections (from www.isaca.org web or LMS):
  - "*Risk, Security and Privacy-related Aspects of Incident Management and Response*" and
  - "*Strategies for Addressing Risk Associated With Incident Response*"
- Discuss the following:
  - The impact of each risk.
  - Which is the most important strategy? Why?

Tabletop Exercise Scenarios

Tute Activity 3

- Go through exercises 1 to 6 to help prepare your cybersecurity team and discuss
  - https://www.cisecurity.org/wp-content/uploads/2018/10/Six-tabletop-exercises-FINAL.pdf

Tute Activity 4

Prepare for Assignment 1: Incident response approaches (1000 words equivalent – this is a sample example only)

(1) Read the Chapter: "Guidelines for Cyber Security Incidents" contained in the Australian Government Information Security Manual (OCTOBER 2019) which discusses the processes involved in detecting, managing and reporting cybersecurity incidents (see LMS).

(2) Study articles about PayID Hack reported in the news in June and August 2019.

https://www.smh.com.au/business/banking-and-finance/australians-private-details-exposed-in-attack-on-westpac-s-payid-20190603-p51u2u.html

https://www.smh.com.au/business/banking-and-finance/payid-in-new-breach-affecting-customers-at-big-four-banks-20190821-p52jby.html

(3) Regarding the ACSC guideline, suggest a list of possible critical infrastructure, operation processes and/or human factors that are involved in the reported scenario of PayID incident. You should propose or argue, stating the appropriate incident response approaches - why or why not them need to be incorporated in the response.

Watch this YouTube Video:

Tute Activity 5

Question: What kinds of Metrics have been discussed?

https://www.youtube.com/watch?v=O_tFYm5YVXU

Tute Activity 6: Prepare 2-slides: select an appropriate cyber incident and/or data breach, identify 5 to 7 relevant KPIs and justification…

- Read white articles and research materials
- Read incident response approaches and frameworks documents
- Watch videos
- Read lecture slides
- Slide 1: Any example cyber incident and/or data breach
- Slide 2: 5 to 7 KPIs along with justification
- Show your slides

Australia's Cybersecurity Online Resources

- Australia's Cybersecurity Strategy
www.cybersecuritystrategy.dpmc.gov.au
- Australian Center for Cyber Security www.acsc.gov.au
- Australian Computer Emergency Response Team (AusCERT)
www.auscert.org.au
- Australian Cybercrime Online Reporting Network (ACORN)
www.acorn.gov.au
- Australian Internet Security Initiative
www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative
- Australian Signals Directorate – Top 4 Mitigation Strategies
www.asd.gov.au/infosec/mitigationstrategies.htm
- Australian Signals Directorate – CyberSense Videos
www.asd.gov.au/videos/cybersense.htm
- Australian Government – Stay Smart Online
www.staysmartonline.gov.au
- ACCC – Scam Watch www.scamwatch.gov.au
- Australian Computer Society (ACS) www.acs.org.au

See You Next Time

latrobe.edu.au

La Trobe University
CRICOS Provider Code Number 00115M