CRICOS Provider No. 00103D | RTO Code 4909 | TEQSA No. PRV12151 (Australian University)

## ITECH1502 Cybersecurity Fundamentals

## Week 1 Lab Activities

**Lab Overview:**

This week’s lab introduces students to the foundational concepts of cybersecurity through hands-on, reflective, and scenario-based activities. Students begin by conducting a **Cyber Hygiene Self-Assessment**, evaluating their personal digital safety practices across areas such as password management, software updates, and online behavior. This is followed by a **Digital Life Exposure Mapping** exercise, where students analyze their daily digital interactions to identify potential risks and existing security mechanisms.

The lab then transitions into **real-world incident analysis**, where students apply the **CIA Triad** (Confidentiality, Integrity, Availability) to evaluate the impact of recent cybersecurity breaches. Finally, students engage in a **defense-in-depth scenario**, identifying control failures in a hypothetical insider breach and proposing layered security solutions.

By the end of the lab, students will have developed a deeper understanding of cybersecurity’s relevance in everyday life, the importance of layered defenses, and the practical application of core security principles.

🔬 **Lab Task 1 – Importance of Cybersecurity in Daily Life**

## ****Activity 1:**** ✅ ****Cyber Hygiene Self-Assessment Checklist****

📌 **Instructions for Students:**  
Go through each item below and mark the appropriate column. At the end, reflect on your current cyber hygiene level and identify 3 key actions you will take to improve your digital safety.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Item** | **✔️ Yes** | **❌ No** | **🟡 Not Sure** |
| **Passwords** | I use **strong, unique passwords** for each account |  |  |  |
| I use a **password manager** to securely store passwords |  |  |  |
| I **regularly change** important passwords (e.g., banking, email) |  |  |  |
| I have **enabled Multi-Factor Authentication (MFA)** on my key accounts |  |  |  |
| **Software & Devices** | My operating system and apps are **updated regularly** (auto-updates enabled) |  |  |  |
| I have **antivirus or endpoint protection software** installed |  |  |  |
| I **review app permissions** on my smartphone periodically |  |  |  |
| I avoid downloading software or files from **unverified sources** |  |  |  |
| **Online Behavior** | I **verify links and sender email addresses** before clicking |  |  |  |
| I use a **VPN** when connected to public Wi-Fi networks |  |  |  |
| I **log out** of devices and accounts after use (especially shared/public ones) |  |  |  |
| I do not share personal information over **unsecured channels** (e.g., SMS, public chat) |  |  |  |
| **Data Protection** | I regularly **back up important data** to secure cloud or external storage |  |  |  |
| My sensitive files are **encrypted** or protected with a password |  |  |  |
| I know what to do if I **lose my phone/laptop** or it gets stolen |  |  |  |
| **Account Awareness** | I **regularly review** account activity logs (e.g., Gmail, Facebook, LinkedIn) |  |  |  |
| I’ve **deleted or deactivated old accounts** I no longer use |  |  |  |
| I understand the difference between **legitimate and phishing emails** |  |  |  |



## 🧠 ****Reflection Questions (To Submit Along with the Checklist):****

1. What areas of cyber hygiene are you doing well?

**I feel confident in my performance when it comes to data protection and password management.**

1. What areas do you need to improve?

**A areas I recognize needs improvement is my online behavior, along with my knowledge and management of software and devices, where I feel I need to improve in.**

1. What actions will you take this semester to enhance your digital safety?

**I will secure my digital safety by using multiple passwords for different software and accounts. I would also like to install virus protection for my data.**

1. Which 3 cyber hygiene practices will you commit to improving this semester?

**Software & devices ,Password and having better account awareness**

1. How might these practices reduce your vulnerability to cyber threats? *(150 words)*

**By using strong, unique passwords and regularly updating them, I significantly lower the risk of unauthorized access to my accounts. Keeping software and devices updated and having antivirus or endpoint protection software installed will lower the attack of hackers. Being more account-aware helps me to identify an unusual attempt from people to access my account which will help me to take quick action. Having all these will help me have safer devices from any threats .**

### 🔍 ****Activity 2: Digital Life Exposure Mapping****

#### Instructions:

Using the table below, **record your digital interactions across a typical day**. Consider the apps you use, information you share, and the security tools that protect (or don’t protect) you.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Time** | **Activity** | **Personal Data Shared** | **Cyber Risk** | **Security Mechanism Present** |
| 08:00 AM | Mobile banking | Phone number, PIN | Account takeover | 2FA, secure app |
| 09:30 AM | Email login | Username, password | Phishing, credential theft | MFA, spam filter |
| 10:30  AM | Social media  Login | Username , password | Potential data risk |  |

#### Discussion Questions:

* Which of your activities pose the highest risk?

**What poses the highest risk is probably the mobile banking as it has the biggest consequences which can be exposing your bank details which can go to losing money.**

* How much of your digital safety is **within your control**?

**I think majority of my action such as my logins and password for our software safety is majority in our control as we have the action to install protections for our logins and have the control to update login detail .**

* Are there interactions where you **trust a third party’s security**?

**Yes there is a third party security such as using an iPhone there’s a password security app which store all our login details in this protected app that only we can access through our phone password.**

**Lab Task 2: In this task, you will investigate a recent real-world cybersecurity incident (from the past 5 years), analyse its impact through the lens of the CIA Triad, and reflect on its broader implications.**

1. **Choose a Recent Incident from any one industry** **you care about or plan to work in**Select any publicly documented cybersecurity incident from reliable sources such as academic articles, industry reports, or news media. Examples may include:
   * Medibank Breach (Australia, 2022)
   * Optus Data Breach (Australia, 2022)
   * SolarWinds Supply Chain Attack (USA, 2020)
   * MOVEit File Transfer Vulnerability Exploits (Global, 2023)
   * Uber Breach (2022)
2. **Fill the CIA Triad Analysis Table:** Medibank Breach (Australia, 2022

|  |  |  |  |
| --- | --- | --- | --- |
| **CIA Principle** | **Was it compromised?** | **Evidence from Incident (Brief explanation)** | **Control Gaps or Failures** |
| Confidentiality | Yes / No | What sensitive data was accessed or exposed?  **The cyber threats exposes almost 9.7 millions customer records which contains sensitives health claims** |  |
| Integrity | Yes / No | Was any data or system integrity compromised?  **Yes the attackers being able to access to sensitive information ,comprised the integrity of the Medibank business** |  |
| Availability | Yes / No | Were services disrupted or made unavailable? **Yes the services of Medibank was comprised and made available for the attackers to disrupt the information of the customers** |  |

1. **Critical Reflection (200–300 words):**  
   Write a concise reflection addressing:



Which CIA pillar was most impacted and why?

* What could the organization have done differently?
* How does this incident reflect broader trends in cybersecurity?
* Could AI tools have helped prevent or?

**The recent incidents I have done is Medibank data breach at Australia 2022 so these incidents happen when a group of cyber attackers having accessed to almost 9.7 million customer records, including sensitive which is a breached in the integrity of the company and also exposing he data which there found. The CIA pillar that was more impacted is confidentiality a it was breach making It an easier access to authorized individuals causing data leaks, identity thefts, reputation damage for company itself. The incidents itself reflect a positive side to the cybersecurity making a more need for people who is in major in cyber security and causing companies to reply on the cybersecurity. I also believe that Ai tools can help is threat detection & responsee tools that detects any unusual access to the data which therefore alarm the system that its getting breach therefore security protocol is activated to prevent the threats**.

**Lab Task 3:** In this activity, you will analyze a **hypothetical cybersecurity breach** and identify which **administrative, technical, or physical security controls** failed. You will then propose appropriate **defense-in-depth countermeasures** to prevent similar breaches in the future.

### 🧩 ****Scenario:** Insider Breach at MediVault Health Systems**

MediVault is a national health services provider that stores thousands of patient records in a cloud-based system. A recently hired employee, working in the billing department, was able to:

* Access confidential patient records unrelated to their job
* Download and transfer sensitive files to a personal USB device
* Bypass login alerts by accessing the system after-hours using a shared admin account
* The breach went undetected for 3 weeks

A subsequent investigation revealed:

* No role-based access controls were enforced
* USB ports were not disabled on corporate machines
* Shared credentials were used by multiple staff members
* Access logs existed but were never monitored

### ✅ ****Task Instructions:****

1. **Identify Control Failures:**  
   Using the table below, determine which **type(s) of control** (administrative, technical, or physical) failed and explain why.

|  |  |  |
| --- | --- | --- |
| **Failure/Weakness** | **Control Type (Admin / Tech / Physical)** | **Explanation of Failure** |
| Use of shared admin credentials | Tech | Sharing credentials bypasses individual accountability and violates access control best practices |
| Unrestricted file access for billing staff | Administrativie | Lack of role-based access permissions allowed staff to access data beyond what there can access |
| USB data exfiltration | physical | The absence of device control or physical port restrictions enabled unauthorized data transfer. |
| No log monitoring or alerting | Tech | Failure to implement log monitoring can mean suspicious activity can go undetected |

1. **Defense-in-Depth Recommendations:**  
   For each failure, recommend a **layered security control** that could help mitigate the risk.

|  |  |  |
| --- | --- | --- |
| **Layered Security Recommendation** | **Type of Control** | **Justification (1-2 sentences)** |
| E.g., Implement Role-Based Access Control (RBAC) | Administrative | Limits access to sensitive data based on job responsibilities |

|  |  |  |
| --- | --- | --- |
| **Layered Security Recommendation** | **Type of Control** | **Justification (1-2 sentences)** |
| Implement Unique Admin Credentials | Tech | Eliminate the action of sharing access |
| Enforce Role-Based Access Control | Admin | Limit access to information based on job roles |
| Disable USB ports or use endpoint | Physical | Prevent restricted data transfer |
| Deploy SIEM with Real-Time Alerting | Tech | Enables monitoring log and alerts any suspicious activity |

**Critical Reflection (150–200 words):**  
Reflect on:

* Why relying on one type of control is insufficient
* How combining multiple control layers improves security
* What lessons this scenario teaches about real-world breaches

**Relying on one point of control is insufficient because if that control is breach there’s no other layer defense for he breachers so there for a lot of consequence can happen for the business and company which cause a lot of financial issue for the company and with saying that having multiple layers of controls improves the security helping the attacker to either failed there beach or give up cause of the amount of security walls there is . A lessons this scenario teaches about the real world breaches is the different way one can breach and how the principes of defense in depth roles plays in defending any attempt of breaches or attempt to access the data physically.**

## Lab Submission Guidelines

1. All students are required to submit their completed **Week 1 Lab** tasks via **Moodle** by **Sunday, 27 July 2025** 23:59 (local time).
2. Navigate to **Week 1 > Active Learning** in Moodle to access the submission link.