School of Informatics & IT

Diploma in Cybersecurity and Digital Forensics

CDF3C01 – Incident Response and Management (ICRM)

Lab 1 – Security Incident Response Policy and Plan I

# Learning Outcomes

By the end of this practical lesson, the student should be able to demonstrate the following items:

* Analyse past case studies that involve cyber-attacks on specific organisations and industries.
* Identify the motivational factors that led to the cyber-attacks.

# Tasks

## Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Internet Crime Complaint Center’s 2020 report found that there were **465,177** reported incidents that year, which works out at **one successful attack every 1.12 seconds.**

## Case Study Research

In groups of 5, conduct research on ONE of the famous cybersecurity case studies listed below:

* Marriott International Cyber Attack
* Saudi Aramco Data Leak
* Twitter Cyber Attack
* SolarWinds Supply Chain Attack
* Capital One Security Breach
* Facebook User Data Leak
* Ukraine Power Grid Cyber Attack

Based on the case study, create a 15-minute PowerPoint presentation to cover the following items:

* Who were the victims of the attacks?
* What technologies and tools were used in the attack?
* When did the attack happen within the network? (min. Date of Attack)
* What systems were targeted?
* What was the motivation of the attackers in this case? What did they hope to achieve?
* What was the outcome of the attack? (e.g stolen data, ransom, system damage, etc)
* If you were a cybersecurity specialist that is tasked to ensure that your organisation is not affected by this attack, what would you recommend the IT team to do?

## 2.3 Case Defense Peer Assessment

During this exercise, the conduct of this assessment will involve 3 groups, in the following format:

|  |  |  |
| --- | --- | --- |
| Group A  (Main Presenters) | Group B  (Audience Group) | Group C  (Assessor Group) |
| Present the Case Study for 15 minutes (not including Q&A) segment. | **Ask questions during the Q&A segment (minimum of 2 questions, maximum of 4 questions).** | **Fill up the Peer Marking Criteria excel spreadsheet (Download it in TP LMS).**  **Assign a timekeeper in the group to take note of the time.** |

Different groups will have the opportunity to assess each other based on the rotations, kindly check with the subject tutor on the arrangement.