Evaluation of the Enhancing Cyber-Incident Management Process Using

Feature Models

Case Study -2: Top industries at risk for cyber attacks

Finance, Healthcare, and Education

Company C

Education

Amman, Jordan

2023

**Case Study Evaluation Experiment**

**Participants:** Incident Response Team of Company C

IRT- Member-ID ----------------------------

1. **Objective**

The main objective of this case study is to investigate the applicability of the **Enhancing Cyber-Incident Management Process Using Feature Models** (FBCIP) to real-world incident attacks. This case study assesses the effectiveness of FBCIP processes in five different companies from the top industries at risk for cyberattacks, specifically finance, healthcare, and education. The study evaluates how the use of the proposed process impacts the ability of the incident response team (IRT) of each company to respond swiftly to cyber incidents and mitigate potential damage.

1. **Experiment**

Based on the presentation section, the explanation of the proposed process, and the case study procedure, please resolve the cyber-incident using both the cyber-incident management process and the FBCIMP[[1]](#footnote-1).

A cyber incident in the finance sector refers to any unauthorized access, disruption, or manipulation of financial systems, data, or services through the use of technology. Such incidents can have severe consequences for financial institutions, businesses, and their customers. Here are the incident that the IRT needs to handle:

Description: Manipulating individuals within the educational institution to disclose sensitive information or perform certain actions. An attacker posing as a student convinces a teacher to share login credentials, leading to unauthorized access to the school's systems.

**Thank you for your collaboration and commitment to our shared case study**

1. For confidentiality issues, we hide the name of company. [↑](#footnote-ref-1)