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 E

Healthcare

Amman, Jordan

2023

**Case Study Evaluation Experiment**

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

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 healthcare refers to any unauthorized or unexpected event involving the compromise, theft, or disruption of healthcare information systems, data, or services due to the actions of cybercriminals, hackers, or other malicious actors. These incidents can have significant consequences, including the compromise of patient data, disruptions in medical services, and potential threats to patient safety. Here are the incident that the IRT needs to handle:

Description: Compromising the security of third-party vendors or suppliers that provide software, services, or equipment to healthcare organizations. Malicious actors insert malware into a software update provided by a healthcare IT vendor, leading to the compromise of healthcare 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)