**CIS-481: Introduction to Information Security**

**InfoSec Chapter Exercise #12 - Option C**

**Team: Project Team 11**

**Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson**

**Logistics**

1. Get together with other students on your assigned team in person and virtually.
2. Review the three options available and decide on only one to pursue as a team.
3. Discuss and complete this assignment in a collaborative manner. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning.
4. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

**Problem 1**

Digital forensics are often used for two key purposes, investigating allegations of digital malfeasance and performing root-cause analysis. Compare and contrast these purposes. *(10 points)*

**Answer:** Digital Forensics is used in order to overlook that in case if an incident or detect the vulnerability of the undergoing crime that is happened within the organization or personnel. Digital Forensics leads to investigation of the cybercrime during or after a digital crime of any type, intensity (damage ratio) it is a physical manifestation to reach to the root of crime. There are actually two key purposes related to it:

* Investigating allegations of digital malfeasance: It is used to overlook the personnel of organization who have the allegation of that (they are responsible for the crime that has been happened) the proper investigation on the allegations are overlook to detect if the people that are considered for the damage by authorities of the organization or an individual should be overlooked. These investigations occur readily after the crime or the damage has been happened. As, in every crime the criminals leave something that leads to a cause to reach them, the investigations on the allegations can also be proven very useful to detect who actually can lead to the actualizing digital malfeasance.
* Root Cause Analysis: It is used to detect how actually the cyber criminals has accessed the sensitive information of the organization, the root cause analysis is occurred after the crime has been happened in order to conduct a proper examination and analysis in order to check who the cyber-criminal got the authentication and authorization of the sensitive data of the organization which leads to check which path has been followed through which the access of digital asset of organization is accessed. It deals to incident response planning; the organization can test their equipment via Root Cause Analysis of the organization.

**Problem 2**

The handling of data acquired during a digital forensics investigation requires special care. During an audit of your organization, potential evidence of fraud and embezzlement are uncovered in the accounting information system. Your digital forensics team is brought in to acquire and analyze the relevant data. Describe any special responsibilities your team has related to the handling of this data given the potential need for legal use in a later prosecution. Be sure to address the chain of custody (chain of evidence) and how your team will demonstrate that any analyzed copy or image of the data is a true and accurate replica of the source evidentiary material. *(15 points)*

**Answer:** The audit of the organization is actually known to be as the financial department of the organization which is mainly known to be as the sensitive data of the organization. In case to overlook the fraud or embezzlement that is occurred or undergoing within the organization. The basic initiative that the digital forensics team should focus on a particularizing responsibility and that responsibilities should be as: Overlooking if misrepresentation or fraud, assuming to be if any is done. To focus on the time-period across which the misrepresentation or fraud is happened to conclude the misrepresentation or the fraud as they occur. The culprits or criminals of the misrepresentation are also focused as a whole. To overlook the misfortune endured because of the extortion to make a proper understanding if the applicable proof that is permissible in court. Measures should be taken to keep such cheats from happening later on. It could reveal and affirm of different sorts in leading criminal operations. Normally, a legal review or so-called forensic review is picked, rather than a customary review, if quite possibly the proof gathered would be utilized at a legal review or a court.