7-2 Project Two: Digital Discovery Summary

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

9 December 2024

The scenario involving the high-level executive at Ocwen demonstrates clear violations of the company's Acceptable Use Policy (AUP). According to Section 4.1.3 of the AUP, employees may access, use, or share proprietary information only to the extent necessary to fulfill their assigned job duties. Additionally, Section 4.3.1 prohibits using Ocwen computing assets to engage in personal business activities, as this is outside the scope of authorized usage. The executive's alleged activities—conducting side business operations and running personal ads on a dating website—are inconsistent with these guidelines. Furthermore, such behavior exposes Ocwen to reputational and cybersecurity risks, including potential damage to its brand and the risk of network compromise. These factors collectively indicate a breach of the AUP, justifying an investigation into the executive's conduct (Ocwen, n.d.).

Evidence should be gathered systematically by examining at least three specific locations:

1. Company email accounts can provide critical information, as email records may reveal communications related to personal business operations or activity on dating websites. This aligns with Section 4.3.2 of the AUP, which outlines prohibitions against unauthorized use of email accounts.
2. Analyzing the executive's internet browsing history on company devices is crucial, as this could uncover visits to prohibited websites or platforms unrelated to Ocwen's business operations.
3. The hard drives of company-issued computers are to undergo inspection to identify any stored files, applications, or data supporting the allegations.

Section 4.1.5 of the AUP supports these actions, granting authorized personnel the ability to monitor equipment and systems to ensure compliance (Ocwen, n.d.).

Maintaining the chain of custody is fundamental to digital investigations to ensure that evidence remains credible and admissible in legal contexts. This process involves a meticulous record of every action taken with the evidence, from its initial collection to storage, transfer, and presentation in court. Proper documentation includes the origin of the evidence, the method of acquisition, and any individuals who had access to it. For example, suppose an investigator collects an executive's computer hard drive. In that case, they must log details such as the time and date of collection, the method of transportation, and the secure storage location. TechFusion (2022) states that failing to document these steps can lead to evidence being discredited or excluded from legal proceedings. Additionally, the evidence should be stored securely in a locked evidence room or in tamper-evident containers to prevent unauthorized access or alterations. Only authorized personnel should access the evidence, with each access event logged, justified, and documented. Real-world examples emphasize the importance of following these procedures. In the case of *State v. Cook*, mishandling of digital evidence, including poor documentation of its chain of custody, led to its inadmissibility in court. This stresses the importance of clear and comprehensive record-keeping. Section 5.1 of Ocwen's Acceptable Use Policy reinforces this need, highlighting compliance verification and audits as methods to ensure procedural integrity (Ocwen, n.d.). Digital forensics professionals often employ tools such as evidence management systems to streamline and secure the chain-of-custody process, making it easier to track the lifecycle of evidence from start to finish.

Forensic tools play a critical role in conducting thorough and efficient investigations. Software tools like EnCase Forensic are invaluable for analyzing and collecting data from various digital devices. This tool enables investigators to recover deleted files, examine metadata, and detect anomalies that could reveal unauthorized activities. For instance, EnCase was used during the infamous Enron case to extract and analyze emails and financial records, demonstrating its capability to handle large-scale investigations (Digest, 2020). Hardware tools like write blockers ensure data integrity during forensic investigations. The use of write blockers ensures that no changes are made to the original data on a storage device, allowing the integrity of the evidence to remain intact during analysis. A practical example of their use is the Sony Pictures cyberattack investigation, where write blockers helped investigators safeguard critical evidence while analyzing compromised servers and storage devices. These tools facilitate compliance with the principles outlined in Section 4.2.3 of Ocwen's AUP, which requires secured computing devices and enables a deeper level of analysis to uncover the truth behind incidents. For example, EnCase investigators could retrieve browsing histories or deleted email chains that align with allegations of unauthorized activity. When combined with write blockers, these tools help organizations like Ocwen address incidents methodically while ensuring the integrity of evidence. By leveraging such tools alongside robust procedural safeguards, investigators can ensure their findings are defensible and actionable.

References:

Digest, F. (2020, August 21). Most used digital forensics tools - Forensics Digest. *Forensics Digest*. https://forensicsdigest.com/most-used-digital-forensic-tools/?

OCWEN. (n.d.). Acceptable Use Policy. In *OCWEN* (pp. 1–4).

Ultimate Guide - Chain of Custody in Digital Forensics. (2022, July 27). *TechFusion*. Retrieved December 9, 2024, from https://techfusion.com/chain-of-custody-in-digital-forensics/?