Assessment 4

Legal Aspects of Computer-Based Crime

Leo Newton

IT-FPX4075 Computer Forensics

Capella University

Professor Kuhlman

11/25/24

**Table of Contents**

Access Control Methods...…………………..……………………………………..3

Engagement…………………….…………………………………………………..4

Technical and Procedural Controls…………………………………………………5

Options…….………………..……………………………………………….……..6

Skills…………….………….………………………………………………………6

Strategies…..……………………………………………………………………….7

Current Evaluation…..…………………………………………………………..….8

References.……………..…………………...……………………………………... 10

**Access Control Methods**

Access control methods and models play a crucial role in ensuring the integrity and admissibility of digital evidence. Robust access controls limit who can access specific systems and data, reducing the risk of unauthorized modifications or deletions that could compromise the evidence. This is particularly important in establishing the authenticity and reliability of evidence presented in court.

* Authenticity: Strong access controls help demonstrate that the evidence collected is genuine and has not been tampered with. By restricting access to authorized individuals, it becomes more difficult for a defendant to claim that the evidence was planted or altered.
* Reliability: Access controls help ensure the reliability of digital evidence by preventing unauthorized changes. If a system is easily accessible by multiple users, it becomes more challenging to prove that the evidence reflects the state of the system at the time of the incident.
* Chain of Custody: Access controls support a clear chain of custody, which is crucial for demonstrating that the evidence has been handled properly and securely from the time of collection to its presentation in court (Solomon et. al., 2011). Documented access logs can provide a detailed record of who accessed the evidence and when, further strengthening the chain of custody.
* Data Integrity: Access controls help maintain the integrity of digital evidence by preventing unauthorized modifications or deletions. This is especially important for sensitive data, such as medical records or financial transactions, where even minor changes can have significant legal implications.
* Legal and Regulatory Compliance: Implementing strong access controls is often a requirement for complying with various legal and regulatory frameworks, such as HIPAA, PCI DSS, and GDPR. Compliance with these regulations can strengthen the admissibility of evidence by demonstrating a commitment to data security and privacy.

**Engagement**

Conducting investigations while upholding due-process rights requires a delicate balance. Investigators must gather evidence thoroughly and efficiently while respecting the rights of the suspect. Key challenges include:

* Obtaining Legal Authorization: Investigators must obtain proper legal authorization, such as warrants or subpoenas, before accessing or seizing digital evidence. This process can be time-consuming and requires careful adherence to legal procedures.
* Protecting Against Self-Incrimination: Suspects have the right to remain silent and not incriminate themselves. Investigators must be careful not to coerce confessions or obtain evidence through illegal means.
* Preserving Attorney-Client Privilege: Communications between a suspect and their attorney are privileged and cannot be used as evidence. Investigators must take precautions to avoid inadvertently accessing or seizing privileged information.
* Maintaining Chain of Custody: A clear and unbroken chain of custody must be maintained for all collected evidence to ensure its admissibility in court (Solomon et. al, 2011). This requires meticulous documentation and secure storage of evidence.
* Balancing Investigative Needs with Privacy Rights: Investigators must balance the need to gather evidence with the suspect's right to privacy. Unreasonable searches and seizures are prohibited, and investigators must only collect evidence that is relevant to the investigation.

**Technical and Procedural Controls**

Technical and procedural controls form the foundation for effective investigations. They provide a framework for securing data, documenting activities, and preserving evidence:

* Access Controls: Restricting access to systems and data minimizes the risk of unauthorized modifications or deletions, preserving the integrity of evidence.
* Audit Logging: Detailed audit logs provide a record of user activity, system changes, and security events, offering valuable insights during investigations.
* Intrusion Detection/Prevention Systems: IDS/IPS can detect and alert on suspicious activity, potentially providing early warning of security incidents.
* Data Loss Prevention (DLP) Systems: DLP tools can prevent sensitive data from leaving the organization's control, protecting against data breaches.
* Security Information and Event Management (SIEM) Systems: SIEM systems collect and analyze security logs from various sources, providing a centralized view of security events and facilitating incident response.
* Incident Response Procedures: Documented incident response procedures provide a structured approach to handling security incidents, ensuring that evidence is properly collected and preserved.

**Options**

Information security professionals face an ethical dilemma when executives decide not to report potential criminal activity. While loyalty to the organization is important, the ethical and legal obligations to report suspected crimes often outweigh such concerns. Options include:

* Escalating Internally: The security professional can attempt to escalate the issue within the organization, bringing it to the attention of higher-level executives or the board of directors.
* Consulting Legal Counsel: Seeking advice from independent legal counsel can help the security professional understand their legal obligations and potential liabilities.
* Reporting to Law Enforcement: If internal escalation fails, the security professional may choose to report the suspected criminal activity directly to law enforcement. Whistleblower protection laws can offer some protection against retaliation.
* Resigning from the Position: In extreme cases, where the organization refuses to address the criminal activity, the security professional may feel compelled to resign from their position to avoid complicity.

**Skills**

Expert forensic witnesses must possess a unique combination of technical expertise, investigative skills, and communication abilities. Desirable qualifications include:

* Deep Technical Knowledge: A strong understanding of computer systems, networks, operating systems, and forensic tools is essential.
* Experience in Digital Forensics: Practical experience conducting forensic investigations, including evidence acquisition, analysis, and reporting, is crucial.
* Industry Certifications: Relevant certifications, such as Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), or Certified Information Systems Security Professional (CISSP), can enhance credibility.
* Excellent Communication Skills: The ability to clearly and concisely explain complex technical concepts to a judge and jury is critical.
* Strong Analytical and Critical Thinking Skills: Expert witnesses must be able to analyze evidence, draw logical conclusions, and defend their opinions under cross-examination.
* Impeccable Ethical Conduct: Maintaining high ethical standards and objectivity is essential for maintaining credibility and ensuring the integrity of the investigation.

**Strategies**

Encrypted information presents a significant challenge in forensic investigations. Strategies for accessing encrypted data include:

* Exploiting Weaknesses in Encryption Algorithms: Identifying and exploiting vulnerabilities in encryption algorithms can sometimes allow access to encrypted data without the decryption key (Electronic Frontier Foundation, 1998).
* Brute-Force Attacks: Using powerful computers to try all possible decryption keys can sometimes break weak encryption, but this can be time-consuming and resource-intensive.
* Dictionary Attacks: Trying common passwords or passphrases can sometimes decrypt data if the encryption key was based on a weak password.
* Side-Channel Attacks: Exploiting weaknesses in the implementation of encryption algorithms, such as power consumption or electromagnetic emissions, can sometimes reveal information about the decryption key.
* Social Engineering: Attempting to trick the suspect or someone with knowledge of the decryption key into revealing it.
* Seeking Legal Compulsion: Obtaining a court order to compel the suspect to provide the decryption key.

**Current Evaluation**

Widget Factory's current security posture presents several weaknesses that hinder effective investigations:

* Lack of Formal Policies and Procedures: The absence of documented security policies and procedures creates ambiguity and inconsistency in security practices, complicating investigations.
* Inconsistent Security Controls: Variations in security measures across different locations make it difficult to maintain a consistent security posture and complicate incident response.
* Weak Password Policies: Weak password policies increase the risk of unauthorized access and compromise the integrity of systems and data (Solomon et. al., 2011).
* Limited Security Staffing and Expertise: The lack of dedicated security personnel hinders effective incident response and forensic investigations. Reliance on general IT staff for security functions can lead to oversights and missed opportunities to gather crucial evidence.
* Inadequate Training: Insufficient employee training on security awareness, incident reporting, and evidence handling can compromise the integrity of investigations.

These weaknesses significantly limit Widget Factory's ability to conduct effective investigations and pursue legal action against perpetrators. Addressing these shortcomings through the implementation of robust technical and procedural controls, along with dedicated security staffing and comprehensive training programs, is crucial for improving the organization's security posture and investigative capabilities.

**References**

A. K. Khan and H. J. Mahanta. *(2014*). Side channel attacks and their mitigation techniques.  *First International Conference on Automation, Control, Energy and Systems (ACES)*, Adisaptagram, India, 2014, pp. 1-4, <https://www.doi.org/10.1109/ACES.2014.6807983>

Electronic Frontier Foundation. (1998).*Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Reilly & Associates, Inc.

Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., & Barrett, D. (2011). *Computer forensics jumpstart*. John Wiley & Sons, Incorporated.