BB

by Bb Bb

Submission date: 17-May-2021 07:39AM (UTC-0400)
Submission ID: 1587892538
File name: Cybersecurity.docx (15.96K)
Word count: 442
Character count: 2537

Cybersecurity

Name

Institution

Course

Instructor

Date

Cybersecurity

The rate of computer-related crime is on the rise. Cyber-criminals are becoming ingenious and are devising ways of committing crime while covering their tracks. Law enforcement officers have no option but to get adequate cyber-security and computer training to be in a position to counter the actions of cyber-criminals. According to Mayland (2019), police officers lack proper training on cyber-crime and the use of computer technologies. In addition to that, there must be a comprehensive definition of cyber-crime and adequate staffing and training to mitigate the challenges of cyber-criminals at the local, state, and federal levels. Training law enforcement officers is an expensive venture. Also, not every police officer can learn computers. In this regard, the local police departments should hire a computer specialist to help them handle cyber-crime cases. The relevant departments must also have the proper equipment like a robust IT infrastructure to help fight cyber-crime. However, law enforcement agents must be properly trained on identifying and investigating possible computer crimes since if they are unable to identify cybercrimes, there will be no investigations.

First-responders assist forensic investigators in transporting electronic evidence to the laboratories where they are examined. Electronic evidence is regarded as fragile; hence the data stored in such media must not be added, modified or destroyed (Mason et al., 2021). The electronic media should not be folded, bent, or broken during transportation. Where evidence containers are used, they must be properly labeled. Furthermore, while in transit, evidence that is not bagged, like computers and other related hardware, must be properly secured not to fall or vibrate, hence damaging evidence. Responders on a crime scene are guided by procedures and guidelines on collecting, preserving, and prosecuting the evidence in a digital crime scene.

In computer crime, the chain of custody is the coherent series that documents the guardianship, control, transmission, examination, and disposition of electronic evidence in a criminal proceeding (Shah et al., 2017). Each step in the process is essential because if it is broken or altered, the electronic evidence is rendered admissible in a criminal proceeding. In this regard, preserving the chain of custody is crucial because it is about adhering to the accurate and reliable procedure that ensures the quality of electronic evidence collected.

References

Mason, S., Sheldon, A., & Dries, H. (2021). Proof: The Technical Collection and Examination of Electronic Evidence.

Mayland, M. (2019). A Qualitative Exploration Of The Challenges The Danish Police Face In Dealing With Cybercrime.

Shah, M. S. M. B., Saleem, S., & Zulqarnain, R. (2017). Protecting Digital Evidence Integrity and Preserving Chain of Custody. *Journal of Digital Forensics, Security and Law*, *12*(2), 12.

BB

ORIGINALITY REPORT

1%	0%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to American InterContinental University Student Paper	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		