BEHAVIOURAL ANALYTICS IN CYBER SECURITY FOR DIGITAL FORENSICS APPLICATION

Martin Luther Bwangah

School of Science, Engineering & Technology, Kabarak University, Nakuru, Kenya

ABSTRACT

The paper emphasizes the human aspects of cyber incidents concerning protecting information and technology assets by addressing behavioral analytics in cybersecurity for digital forensics applications. The paper demonstrates the human vulnerabilities associated with information systems technologies and components. This assessment is based on past literature assessments done in this area. This study also includes analyses of various frameworks that have led to the adoption of behavioral analysis in digital forensics. The study's findings indicate that behavioral evidence analysis should be included as part of the digital forensics examination. The provision of standardized investigation methods and the inclusion of human factors such as motives and behavioral tendencies are some of the factors attached to the use of behavioral digital forensic frameworks. However, the study also appreciates the need for a more generalizable digital forensic method.

KEYWORDS

Digital Forensics, Human Vulnerabilities, Social Engineering, Criminal Profiling, Behavioral Analytics

1. INTRODUCTION

Data and information are among the most vital assets in any modern organization. Human, organizational, and technological aspects play a central consolidative role in information security and digital forensics in safeguarding these important assets. However, the security and integrity of such assets is increasingly threatened by malicious cyberspace users. Even with the adoption of proactive stop-gap measures, the rise in cybercrime has led to significant losses. An assessment of the 2020 Information Systems Audit and Control Association's (ISACA) annual report on the state of cyber security provided an insight into the increasing threat of cybercrime [1]. This report used insight from 2,000 information security experts across seventeen industries, to investigate the cybersecurity landscape. The report concluded that cyberattacks have been on the increase year over year since 2010 [1]. The report also revealed that the threat actors were divided as follows, external cybercriminals (22%,) malicious insiders at (11%,) non-malicious insiders at (10 %) followed by state actors (9 %) then hacktivists at 8%. In the report, the most prevalent attack techniques used were social engineering which stood at 15%, followed by advanced persistent threat at 10%, and subsequently ransomware and unpatched systems at 9% each [1].

The Finance Online Research Center 2022/2023, which reported on 10 cyber security predictions, recognized that cybercrime was the fastest-growing crime globally. Notably, the financial losses suffered by organizations outnumber overall income in the international illegal drug trade [2]. Unfortunately, these attacks also target small enterprises that lack sufficient cyber security capacity to protect themselves. This report also identified the common cyber-attack method facing companies based in the United States. The threats included phishing at 38%, network

intrusion at 32%, inadvertent disclosure at 12%, theft and loss of devices and records at 8%, and system misconfiguration at 5% [2].

Based on the two reports, it is apparent that social engineering attacks based on phishing are a growing threat. The threat involves system intruders targeting employees who connect to their employer's network remotely from home or away from the office. The hackers use manipulation that exploits human error to gain private information, access, or valuables with the intent to use such information against the employee. Such attacks have resulted in huge losses which have shifted focus towards identifying criminal behaviors instead of simply focusing on physical and device security alone.

The study of behavioral tendencies is informed by the fact that most cybercriminal activities are grounded on certain patterns, especially social engineering. This paper proposes the combined use of digital forensics and behavioral analytics to create a digital forensic profiling framework for analyzing evidence. The framework should provide a definitive criminal profile to identify cybercriminals and stop them before they commit further crimes.

1.1. Problem Statement

Specialists in digital forensics have been experiencing unforeseen difficulties because cybercriminals are increasingly using innovative and sophisticated techniques to commit crimes. In many cases, such as social engineering attacks, the evidence is often not enough to minimize the list of possible suspects. These challenges can be solved with a combination of digital forensic processes that include focusing on the criminal's behavior in addition to the conventional analysis process. However, even the addition of human behavior as a factor requires a proper framework that can be used uniformly and effectively.

1.2. Background to the Study

The increased use of digital services across almost all social, economic, and regulatory speeches has made computers a predominant part of human life. However, the same increased use of digital devices has resulted in increased cases of cybercrime activities. As a result, law enforcement and judicial authorities are facing increasing pressure to adopt proactive means of including digital ways of collecting and analyzing evidence in both the physical and cyber spheres. This study acknowledges the shortcomings of past digital forensic and evidence-collection mechanisms. Most of the digital frameworks identified so far failed to acknowledge the strengths of previous frameworks. As such, it has been hard to have a unified digital forensic methodology that would draw consensus among architects of previous frameworks. This assessment sought to collate a comprehensive review of digital forensic framework proposals that are available to the public. It also sought to delineate between those frameworks that have a behavioral evidence analysis aspect and those that lack the same.

1.3. Study Objectives

This study sought to: (i) explore the application of behavioral analytics in digital forensics; (ii) explore the existing behavioral evidence analysis framework to establish their strengths and weaknesses.

2. LITERATURE REVIEW

This section provides an assessment of the literature relating to the primary objectives outlined in the introduction section of this research paper. The literature review also covers the concepts of behavioral analytics, cyber security challenges, digital transformation, and the adoption of digital forensics as a solution to emergent cybersecurity challenges. Finally, the assessed literature also addresses the use of digital forensic frameworks for investigations and as a barrier to cybercrime.

2.1. Cybersecurity Challenges in Digitally Dynamic Organizations

Cybersecurity is a growing global concern for personal digital device users, businesses, and state agencies. The cybercrime space has been evolving fast, with the adoption of new digital technologies and practices such as the internet of things and remote work. In a world where most aspects of life are becoming digitalized, one of the greatest difficulties in the field of cybersecurity is guaranteeing the safety of data [3]. However, the aspect of human beings as Information Technology system operators has remained constant. Social engineering, which provides an actual link between criminals and their targets, has also become a prevalent problem due to the operational position held by legitimate system users. Spear phishing and spoofing often serve as the initial vector for intrusive attacks against organizations and individual victims of cybercrime.

2.2. Digital Forensics

In most cases, cybercrime scenes tend to be online or have a digital dimension that requires expert analysis leading to the need for digital forensic analysis. Notably, digital forensics assists authorities in forensically and methodically determining when an event happened, when it occurred, where it transpired, why it ended up happening, and, ideally, who is responsible. Such data is required to certify that the evidence discovered is adequate to indict a person for the unlawful offense perpetrated [4]. All this information is needed to guarantee that there is enough evidence to prosecute and convict a cybercriminal. Digital forensics (DF) is a sub-field of forensic science that focuses on the study of the digital environment. DF, like any other forensic investigation, employs scientific procedures to discover evidence. The primary purpose of DF is to ensure evidence gathered in the investigation is credible and admissible before the court of law[5].

2.3. Behavioral Analytics

Behavioral analytics is a concept that employs principles such as motive, mode of operation, signature behavioral patterns, offender schemas, and victim personas to better probe criminal activity [6]. It is worth stating that hard data is the bedrock of behavioral analytics. Behavioral analytics is a subfield of data analytics concerned with gaining insight into the activities of individuals [6]. Initially oriented towards violent offenders, behavioral analytics has been expanded to cover other aspects of criminology. This field utilizes vast amounts of raw data collected from various platforms and devices including social media, gaming apps, retail websites, and apps [7]. The information is gathered, processed, and then utilized as the basis for making choices, such as how to predict future criminal trends. Behavioral analytics may support a variety of assumptions. The assumptions make iterative testing and assessment a key component of this field.

2.4. The Relationship between Digital Forensics, Criminal Profiling, and Behavioral Analytics

In the field of digital forensics, behavioral analytics involves the logical investigation method that looks at evidentiary material from a particular event and focuses on specific personality and behavioral patterns to figure out what the probable offender is like. Notably, Behavioral evidence analytics (BEA) practice includes four sets of assessments (Figure 1) including equivocal forensic analysis [8], forensic victimology [9], identification of crime scene characteristics (10], and determination of criminal tendencies [8], [11]. These four categories are used to arrive at a comprehensive methodology for investigating crime.

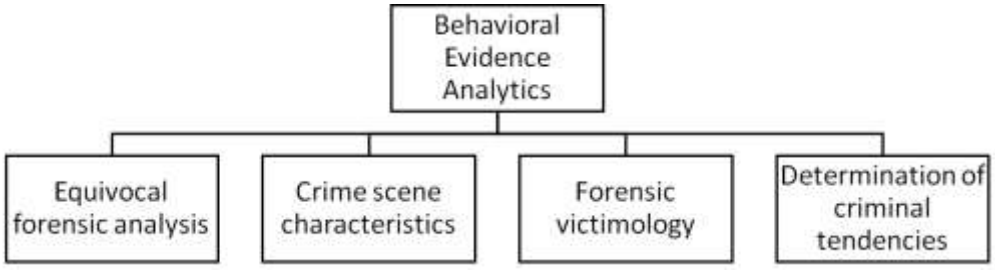

Figure 1. Digital forensic assessment areas

Criminal profiling involves figuring out what kind of an individual or a group of suspects are by using the actions they take while committing a crime(s) [11]. Cybercriminals often have unique goals and motivating factors that form a pattern just like criminals in the physical world. Profiling in digital forensics can be used to identify such patterns, and more investigators are choosing to adopt the same [12]. Furthermore, the overall set of crime investigation processes is often similar to those used in a traditional crime investigation, such as what drove the criminal or why they chose an individual target.

3. DIGITAL FRAMEWORKS

One of the earliest digital forensics frameworks was the US Department of Justice's Digital Forensics Investigation Process Model [13]. This model was a fours stage model consisting of securing and analyzing the incident, recording the incident, collecting evidence, as well as packing, transporting, and organizing digital evidence. A 2002 article introduced a new framework to standardize the DF process, but the seven processes proved too general for proper use [14]. An Integrated Digital Investigation Process consisting of (1) preparation, (2) distribution, (3) physical crime scene examination, (4) digital crime event investigation, and (5) appraisal; was introduced by [15].

Subsequently, a two-tiered model was created to cover primary crime and physical crime scenes distinctly in 2004 [16]. A six-step framework that was aimed at incorporating specificity and practicality in the investigative process followed the 2004 model [17]. The six-step model was woven around preparation, incident response, data collection, analysis, presentation of findings, and incident closure. A minor adjustment that sought to address the legal challenge in the digital evidence analysis process by adding attribution and reconstruction was incorporated into a 2010 model [18]. A 2010 research article proposed the systematic digital forensic investigation model that included eleven phases. The eleven phases included scene preparation, scene lockdown, survey and identification, scene recording, communication blocking, evidence collecting, preservation, inspection, analysis, presentation, and outcome [19].

A 12-step harmonized model that covered both traditional and digital forensic concepts was proposed in 2012 [20]. The steps within this assessment included the identification of incidents, initial response, planning, preparedness, documenting of the event location, and identification of possible evidence. It also involved the gathering of prospective evidence, conveyance of potential evidence, storage of potential evidence, examination of potential evidence, presenting, and result cataloging. While noting that previous frameworks failed to incorporate the practical needs of digital forensic investigators, several researchers proposed the use of an eight-step process that incorporated preparation, identification, incident response, evidence gathering, evaluation, analysis, presentation of information, and closure [21].

All of the frameworks above lacked the inclusion of behavioral aspects in the forensic analysis process. A consequent analysis of previous structures developed a framework tailored toward cyberstalking cases that included aspects of behavioral evidence analysis [22]. This model was broken down into detection and complaint, examination and evaluation. A 2015 assessment provided an alternative BA-focused approach of dealing with sexual crimes that involved six steps beginning with the categorization of cases, contextual analysis, collecting of data, statistical evaluation, chronological analysis, and visualization, as well as decision-making and expert opinion [23]. A more comprehensive analysis [8] combined the concept in [22] with [23] to develop a four-step process consisting of review, recognition and gathering, examination and analysis as well as assessment and presentation. Table 1 below provides a tabulated breakdown of the digital forensic frameworks.

Table 1. Digital forensic framework proposals through the years.

Author(s)	**Year**	**Constituent variables**
Federal Bureau of Investigation [13]	2001	(1) Securing and analyzing the incident, (2) recording the incident, (3) collecting evidence, (4) secure packing and transporting of evidence, (5) organizing digital evidence
Reith, Carr, andGunsch [15]	2002	(1) Preparation of evidence, (2) distribution, (3) physical crime scene examination, (4) digital crime event investigation, and (5) appraisal.
Baryamureeba and Tushabe [16]	2004	(1) Preparation, (2) incident response, (3) data collection, (4) analysis, (5) presentation of findings, (6) incident closure.
Beebe and Clark [17]	2010	(1) Crime scene preparation, (2) scene lockdown, (3) survey and identification, (4) scene recording, (5) communication blocking, (6) evidence collecting, (7) preservation, (8) inspection, (9) analysis, (10) presentation, (11) outcome.
Valjarevic and Venter [20]	2012	(1) Identification of incidents, (2) initial response, (3) planning, (4) preparedness, (5) documenting of the event location, (6) identification of possible evidence (7) gathering of prospective evidence, (8) conveyance of potential evidence, (9) storage of potential evidence, (10) examination of potential evidence, (11) presenting, (12) result cataloguing
Silde and Angelopoulou [21]	2014	(1) Detection and complaint, (2) examination and evaluation
Montasari, Peltola and Evans [22]	2015	(1) Preparation, (2) identification, (3) incident response, (4)evidence gathering, (5)evaluation, (6) analysis, (7) presentation of information, (8) closure
Rogers and Seigfried [23]	2016	(1) Categorization of cases, (2) contextual analysis, (3) collecting of data, (4) statistical evaluation, (4) chronological analysis, (5) visualization

4. RESEARCH METHODOLOGY

This qualitative content analysis study looked at academic peer-reviewed scholarly academic journals, theses, and doctoral dissertations authored or presented between 2001 and 2021 that addressed digital forensics and behavioral analytics. Content analysis has been defined as the impartial, methodical, qualitative research of a document's features [24]. The sources were TW Universal academic database as well as ProQuest Dissertation. TW Universal and ProQuest were used because they provided access to comprehensive academic directories with a large range of full-text academic journals, dissertations, and theses.

5. FINDINGS

Up until 2014, none of the existing frameworks were tested in practical situations. The theories and methods that went into making them were not tested in the real world. Models that outlined the steps used did so with made-up examples and scant information that lacked clarity over how the steps were used. Also, the models that explained these different phases concentrated on what needed to be done during each phase, but they did not give enough information about how to carry out the inquiry. Until 2014, the frameworks didn't take into consideration the individuals engaged in the DF investigation. They also did not consider the behavioral, motivational, or social aspects of criminal behavior that could help find possible evidence during investigations. Critically, each framework is built upon the failures of the preceding frameworks.
Based on the assessment of the various frameworks it was clear that the use of BA in digital crimes may help the investigative process in a variety of ways. Specifically, the use of BA offers a methodical strategy for directing investigators to possible sources of forensic evidence in the analyzed devices. It also gives information on individual offender traits and behaviors, which may help with risk assessment. A key benefit of BA inclusion into the analysis process was the adoption of methodologies that could and were applied in the field. Additionally, the frameworks covered from 2014 onwards had a sense of standardization and were much simpler in comparison to those used before them. The disadvantage of behavioral digital forensic frameworks is their specificity to crime categories. For instance, while [23] and [8] dealt with sexual crimes, the framework in [22] was constrained to cyberstalking.

6. RECOMMENDATION

This research has provided a review of the major digital frameworks provided thus far. The paper has also shown how the inclusion of behavioral evidence analysis has revolutionized the composition of digital forensic frameworks. However, most of the frameworks have remained untested beyond the proposal. Future researchers on the subject should focus on proving the efficacy of some of the frameworks, even if such an assessment will begin in the post-behavioral analysis age.

7. CONCLUSION

The growing complexity and power of digital technologies have made it vital to keep an eye on how cyber techniques are used to deter exploitation. The methodologies used to deal with online crimes must also change to keep up with the adoption of new digital skills. Because of this, digital forensics has needed improvement. When Behavioral Evidence Analysis is added to the digital forensic processes, it makes it easier to solve digitally facilitated crimes and provide future preventive as well as detective mechanisms in behavioral evidence. The suggested BEA model, on the other hand, aims to create a standardized approach that can be employed in all criminal cases. This paper details how well BEA works and spells out how to use it in the digital forensic

process. By tracing the development of current digital investigation frameworks, this paper establishes the importance of behavioral analytics in the digital investigation process.

REFERENCES

[1] Information Systems Audit and Control Association's (ISACA) (2021). *State of cybersecurity 2020*. Available: https:// www.isaca.org/state-of-cybersecurity-2020.

[2] Finance Online (2022). *2022/2023 Cybersecurity trends*. Available: https://financesonline.com/cybersecurity-trends

[3] F. Casino, et al, (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*.

[4] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, G. B. Wills,"Security, cybercrime and digital forensics for IoT," in *Principles of internet of things (IoT) ecosystem: Insight paradigm*, Springer, Cham, 2020, pp. 551-577.

[5] D. Paul-Joseph, J. Norman,"An analysis of digital forensics in cyber security," in *First International Conf. on Artificial Intelligence and Cognitive Computing*, Singapore: Springer, 2019, pp. 701-708.

[6] V. Kumar&M. L. Garg, "Predictive analytics: Areview of trends and techniques," *International Journal of Computer Applications*, vol. 182, no. 1, pp. 31-37, 2018.

[7] J. H. Addae, X. Sun, D. Towey,M. Radenkovic, "Exploring user behavioral data for adaptive cybersecurity." *User Modeling and User-Adapted Interaction*, vol. 29, no. 3, 701-750, 2018.

[8] N. Al Mutawa, J. Bryce, V.N. Franqueira, A. Marrington, &J.C. Read, "Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes," *Digital Investigation*, vol. 28, pp. 70-82, 2019.

[9] W. Petherick, "Forensic victimology assessments in child abuse and neglect cases," in *Child Abuse and Neglect*, Academic Press, 2019, pp. 135-149.

[10] R.Y. Patil, &M.A. Ranjanikar, "A new network forensic investigation process model," in *Mobile computing and sustainable informatics*, Singapore: Springer, 2002, pp. 139-146.

[11] A.M. Balogun, T. Zuva. "Criminal profiling in digital forensics: Assumptions, challenges and probable solution," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 2018, pp. 1-7.

[12] D. Möller., *Cybersecurity in digital transformation: Scope and applications*. New York: Springer, 2020.

[13] E. Holder, E.O. Robinson, K. Rose. "Electronic crime scene investigation: An on-the-scene reference for first responders," US Department of Justice Office of Justice Programs, 810, 2009.

[14] M. Reith, C. Carr, G. Gunsch, "An examination of digital forensic models," *International Journal of digital evidence*, vol. 3, no. 3), pp. 1-12, 2002.

[15] B. Carrier, E. H. Spafford, "Getting physical with the digital investigation process," *International Journal of digital evidence*, vol. 2, no. 2, pp. 1-20, 2003.

[16] V. Baryamureeba, F.Tushabe, "The enhanced digital investigation process model," *Digital Investigation*, 2004.

[17] N. L. Beebe, J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," *Digital Investigation*, vol. 2, no. 2, pp. 147-167, 2005.

[18] F. Cohen. "Toward a science of digital forensic evidence examination," in *IFIP International Conference on Digital Forensics*, Berlin, Germany, 2010, pp. 17-35.

[19] A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, "Systematic digital forensic investigation model," *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 1, pp. 118-131, 2011.

[20] A. Valjarevic, H.S. Venter, (2012, August). "Harmonised digital forensic investigation process model," in *2012 Information Security for South Africa*, 2012, pp. 1-10.

[21] R. Montasari, P. Peltola, D. Evans,"Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations," in *International Conference on Global Security, Safety, and Sustainability*, New York, NY, 2015, pp. 83-95.

[22] A. Silde, O. Angelopoulou,"A digital forensics profiling methodology for the cyberstalker," in *2014 International Conference on Intelligent Networking and Collaborative Systems*, Salerno, Italy, 2014, pp. 445-450.

[23] M. K. Rogers, K. Seigfried,"The future of computer forensics: a needs analysis survey. *Computers & Security*, vol. 23, no. 1, pp. 12-16, 2016.
[24] K. A. Neuendorf, "Content analysis and thematic analysis," in *Advanced Research Methods for Applied Psychology*, Oxfordshire, UK: Routledge, 2018, pp. 211-223.

AUTHOR

Martin Luther Bwangah is a cybersecurity specialist and scholar with over 20 years of experience in cybercrime investigations. He holds a BSc. In Information, Technology, and Communication from Maseno University and an MSc. in Data Communication (Computer Networks and Emerging Technologies) from KCA University. He is currently pursuing a doctorate in IT Security and Audit at Kabarak University. Mr. Bwangah works at the Kenya Anti-Counterfeit Authority as a regional head in charge of online intelligence and investigations. He also teaches cybercrime and computer forensics at the United States International University (Kenya) and KCA University. He previously worked in the cyber Crime division of the Kenya National Police service, which he headed for three years.