Cybersecurity Professional Career Paper: Cybercrime Investigator

Student Name: Morgan Brown

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Quinn

Date: April 14th, 2026

Introduction

BLUF: Cybercrime investigators combine technical digital forensics skills with behavioral, social, and organizational analysis to detect, investigate, and prevent cybercrime while navigating evolving technological threats and societal impacts.

Cybercrime investigation is a critical profession within modern cybersecurity as society becomes increasingly dependent on digital systems for communication, commerce, and data storage. Cybercrime investigators are responsible for identifying, analyzing, and responding to illegal activity conducted through computer networks and digital technologies. As cyber threats continue to grow in complexity and frequency, this role has become essential for protecting personal data, organizational assets, and critical infrastructure. Because cybercrime is both a technical and social issue, investigators must combine strong digital forensics skills with an understanding of human behavior and organizational context. This paper examines the career of a cybercrime investigator by analyzing required skills and training, key challenges in the field, and the influence of technology on investigative practices, citing current scholarly research.

Social science principles

Cybercrime investigation is not solely a technical discipline; it is also deeply connected to social science principles that help explain human behavior in digital environments. As discussed in our course material, understanding why individuals engage in cybercrime, including motivations such as financial gain, ideology, curiosity, or social influence, is essential for effective investigative work. Social science research provides a framework for analyzing these behaviors, allowing cybersecurity professionals to better anticipate threats and understand patterns in criminal activity. For example, studies of cybercrime investigation emphasize that effective practice requires not only technical tools but also an understanding of the social and

organizational contexts in which cybercrime occurs (Horan & Saiedian, 2021). This highlights how investigators must interpret human behavior alongside digital evidence when building cases.

In addition, social science principles are increasingly integrated into cybersecurity practices through areas such as human-computer interaction and user behavior analysis. Investigators and cybersecurity professionals rely on these principles to understand how users interact with systems, where vulnerabilities may arise due to human error, and how criminals exploit predictable behavior patterns. Research also shows that the tools used in cybercrime investigations influence how evidence is interpreted and structured, meaning that human decision-making and technological systems are closely interconnected in practice (Steinmetz et al., 2023). This interaction between humans and technology demonstrates why behavioral understanding is just as important as technical expertise in cybersecurity work.

Cybersecurity professionals also apply social science insights when developing strategies for awareness and education. For instance, structured training approaches are used to improve investigator skills and decision-making, ensuring that professionals are better prepared to respond to evolving cyber threats (Alastal & Shaqfa, 2023). Beyond law enforcement, similar principles are applied in public cybersecurity awareness campaigns that educate users about phishing, password security, and safe online behavior. These efforts rely on understanding how people perceive risk and respond to warnings, which is a core focus of social science research. Overall, integrating social science principles into cybersecurity strengthens both investigative effectiveness and preventative strategies by addressing the human factors that contribute to cyber risk.

Application of Key Concepts

Cybercrime investigation is shaped by key course concepts such as cybercriminal subcultures, risk frameworks, human behavior, and cybersecurity culture. Understanding cybercriminal and hacker subcultures helps investigators interpret how offenders communicate, organize, and adapt within online communities. These behavioral insights support investigative work by improving pattern recognition and suspect profiling in digital environments. Professional subcultures within cybersecurity organizations also influence investigative procedures through established norms, ethics, and interagency collaboration practices.

Risk assessment models such as the CIA Triad (confidentiality, integrity, and availability) are central to investigative decision-making. Cybercrime investigators use these frameworks to evaluate the type and severity of system compromise and to prioritize response efforts. Research also shows that effective cybercrime investigation depends on structured, technology-driven evidence collection processes that support accurate analysis of digital incidents (Steinmetz et al., 2023).

Human factors and behavioral theories of cyber offending further contribute to investigative practice by explaining motivations such as financial gain, ideology, and opportunity. Understanding these factors helps investigators interpret victimization patterns and identify likely attack methods. Studies emphasize that successful cybercrime response requires combining technical expertise with awareness of social and organizational context (Horan & Saiedian, 2021).

Professionals apply these concepts through tools such as digital forensics software, log analysis systems, intrusion detection systems, and open-source intelligence (OSINT). These tools support evidence collection, timeline reconstruction, and anomaly detection. Training models

that standardize investigative skills also strengthen professional capacity and consistency in cybercrime response (Alastal & Shaqfa, 2023). Additionally, cybersecurity awareness programs and cyber hygiene initiatives apply behavioral concepts to reduce organizational risk and improve user security practices.

Marginalization

Cybersecurity and cybercrime investigation intersect with issues of marginalization in several important ways, particularly in how unequal access to technology and systemic disparities can increase vulnerability to cyber threats. Individuals and communities with limited access to digital literacy resources or secure infrastructure are often at greater risk of exploitation, identity theft, and online fraud. At the same time, cybercrime investigators must operate within systems that do not always account for these disparities, which can influence how cases are prioritized or understood. Research on cybercrime investigation practices highlights that the tools and technologies used in investigations can shape how evidence is gathered and interpreted, thereby indirectly affecting which cases receive attention and resources (Steinmetz et al., 2023). Additionally, studies emphasize that effective cybercrime response requires not only technical capability but also broader institutional awareness of social context and inequality in digital environments (Horan & Saiedian, 2021).

Efforts within the cybersecurity profession to address these challenges include improving training frameworks and investigative capacity to ensure more consistent and equitable responses to cybercrime across different populations. For example, structured skill-development approaches for law enforcement emphasize the need for standardized competencies to enable investigators to better serve diverse communities and adapt to varying types of cybercrime incidents (Alastal & Shaqfa, 2023). While diversification initiatives within cybersecurity are still

developing, there is increasing recognition that a more inclusive and socially aware workforce can improve trust, accessibility, and fairness in digital protection efforts. Overall, addressing marginalization in cybersecurity requires both technical advancement and a stronger integration of social science perspectives into investigative practice.

Career Connection to Society

Cybercrime investigators contribute directly to the stability and safety of modern society by protecting the digital infrastructure that supports essential systems such as finance, healthcare, transportation, and government services. As these systems become increasingly digitized, they also become more vulnerable to cyberattacks that can disrupt operations, compromise sensitive data, and undermine public trust. Cybercrime investigators play a central role in responding to these threats by collecting and analyzing digital evidence, identifying perpetrators, and supporting legal action that helps deter future attacks. Research emphasizes that effective investigations rely heavily on the integration of computer technologies into evidence collection processes, as these tools shape how data is gathered and interpreted in real-world cases (Steinmetz et al., 2023). This highlights how investigative work is not only technical but also foundational to maintaining the reliability of systems that society depends on daily.

From a policy perspective, cybersecurity is closely tied to laws and regulations that govern data protection, privacy, and law enforcement authority in digital spaces. Governments continue to develop policies that aim to balance security needs with individual rights, particularly as cybercrime often crosses national boundaries and requires coordinated responses. However, research indicates that cybercrime investigation is challenged by differences in legal frameworks and organizational capacity, which can affect how effectively investigators respond to incidents (Horan & Saiedian, 2021). This creates societal implications, as inconsistent policies may lead to

uneven levels of protection across regions and populations. Strengthening investigative capacity and standardizing approaches to cybercrime response are, therefore, essential not only for improving enforcement outcomes but also for ensuring that public trust in digital systems is maintained.

Scholarly Journal Articles

The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis (Steinmetz et al., 2023)

My first source, Steinmetz et al. (2023), provides key insights into how cybercrime investigators rely on computer technologies to structure and support evidence gathering during investigations. The study, based on interviews with 47 investigative personnel, finds that digital tools significantly shape how investigators collect, interpret, and manage evidence, particularly in cases involving large volumes of data, encryption, and jurisdictional challenges (Steinmetz et al., 2023). This source is relevant to the paper because it highlights the practical, day-to-day responsibilities of cybercrime investigators and demonstrates that their work is heavily influenced by evolving technological systems. It also shows that investigative outcomes are not only dependent on individual skill, but also on the tools and organizational systems available to professionals in the field.

Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool (Alastal & Shaqfa, 2023)

My second source, Alastal & Shaqfa (2023), supports the analysis of social science principles by focusing on the skills, training, and capacity-building required for effective cybercrime investigation. The authors propose a structured checklist designed to improve the technical and practical competencies of police officers handling cybercrime cases (Alastal &

Shaqfa, 2023). This source is especially relevant to social science concepts because it emphasizes how institutional training, education systems, and professional development shape investigator readiness and performance. It also indirectly relates to marginalized groups by suggesting that inconsistent training and unequal access to resources may result in uneven investigative capabilities across different regions or agencies, potentially affecting how effectively certain communities are protected from cybercrime.

Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions (Horan & Saiedian, 2021)

My third source, Horan and Saiedian (2021), contributes to the understanding of how cybercrime investigation connects to broader societal systems and public policy. It outlines the evolving landscape of cybercrime, including the need for investigators to adapt to new digital threats and the growing importance of digital forensics and open-source intelligence in investigations (Horan and Saiedian, 2021). The article also emphasizes challenges such as cross-border crime and legal inconsistencies, which directly connect cybersecurity work to government policy and international cooperation. This is important for understanding how cybercrime investigators operate within societal structures, as their effectiveness is influenced by laws, regulations, and global coordination efforts that shape how digital crime is addressed across different jurisdictions.

Conclusion

All in all, cybercrime investigators play a vital role in modern society by addressing the growing complexity of digital threats that affect individuals, organizations, and critical infrastructure. This career requires a combination of technical expertise, analytical thinking, and an understanding of human behavior, as cybercrime is shaped by both technological systems and

social factors. Throughout this paper, effective cybercrime investigation depends on structured training, evolving investigative tools, and the ability to interpret behavior within digital environments. The profession is also deeply connected to broader societal systems, including law, policy, and organizational security practices, which influence how cyber threats are identified and managed. As cybercrime continues to evolve, the role of cybercrime investigators will remain essential in maintaining digital trust, supporting public safety, and strengthening cybersecurity resilience across society.

References

Alastal, A. I., & Shaqfa, A. H. (2023). Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. *Journal of Data Analysis and Information Processing*, *11*(02), 121–143. https://doi.org/10.4236/jdaip.2023.112008

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580–596. https://doi.org/10.3390/jcp1040029

Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2023). The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis. *Criminal Justice Review*, *50*(1), 073401682311610. https://doi.org/10.1177/07340168231161091