2021

Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level

Coleman McKoy
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Coleman McKoy

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Deborah Laufersweiler-Dwyer, Committee Chairperson,
Criminal Justice Faculty

Dr. Melanye Smith, Committee Member,
Criminal Justice Faculty

Dr. David DiBari, University Reviewer,
Criminal Justice Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level

by

Coleman McKoy

MA, Utica College, 2015

BS, Grambling State University, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Criminal Justice

Walden University

November 2021

Abstract

Cybercrime has become one of the fastest-growing concerns for law enforcement agencies at the federal, state, and municipal levels. This qualitative case study examined the perceptions of nine law enforcement officers' from Texas regarding combating cybercrime at the local level. The conceptual framework was based on the structural contingency theory and Porter and Lawler's theory of motivation. Data collection consisted of semistructured interviews, where member-checking helped to enhance the trustworthiness. In addition, data gathered from interview transcripts were inductively coded and used to organize data into categories to determine the themes in the study. Most of the participants in this study perceived that law enforcement agencies were not equipped to take a more prominent role in cybercrime investigations because of the lack of experience and resources. Participants also provided recommendations to address cybercrime at the local level, including helping community members understand cybercrime threats while empowering the public to become safer and more secure during online activity. Finally, many of the participants suggested that creating multiple cybercrime task forces located in major cities throughout the United States could serve as a method of combating cybercrime at the local level. This study's positive social change implications include providing information to law enforcement agencies about potential gaps in combating cybercrime at the local level, along with recommendations for more streamlined cybercrime training for law enforcement officers to increase officer efficiencies in cybercrimes.

Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level

by

Coleman McKoy

MA, Utica College, 2015

BS, Grambling State University, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Criminal Justice

Walden University

November 2021

Dedication

I dedicate my dissertation work to my family. A special thank you to my mother, Rosa McKoy, for your words of encouragement and prayers throughout this journey. When I wanted to give up, you always would say the right words for encouragement. I am forever thankful for my loving wife Angel McKoy and our children, Tyrus McCree, and Zachary McKoy, who have whole-heartedly supported me through the entire doctorate program. Angel, you are the love of my life, and there is no way I could have accomplished any of this without you. Thank you for always believing in me and encouraging me to follow my dreams.

Acknowledgments

I want to give thanks to the Lord, through whom all things are possible. If it were not for the Lord by my side, completing this dissertation would have been impossible.

A big thank you to my committee chair Dr. Deborah Laufersweiler-dwyer, for your continued support, patience, and flexibility in helping me navigate through this process. The dissertation was a long process, and I thank you for helping me reach this point. I want to thank Dr. Melanye Smith for your continued support and flexibility in this process. Thank you, Dr. David Dibari, URR, for your hard work and dedication to making students better writers. Thank you, Angie Drennen, with form and style.

Finally, thank you to Dr. Aaron Bartula and Dr. Themba Ngwenya for your inspiration and encouragement. Thank you to all the participants who provided their perspectives, time, and honesty in this study.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Many large-scale crimes are taking place over the internet (Loveday, 2017), and cybercriminals often commit online crimes with no legal repercussions due to their ability to navigate the internet while avoiding identification. For example, Equifax experienced a data breach in 2017 that left over 144 million users vulnerable to identity theft (Novak & Vilceanu, 2019). In 2018, the Marriot Hotel faced a cyber-attack that impacted 500 million users. Based on the continuous media coverage surrounding cybercrime, individuals have become complacent with protecting themselves against cybercrimes (Younies & Al-Tawil, 2020).

Though cybercrime is one of the fastest-growing threats (Harkin et al., 2018), the ability to combat computer crimes has become problematic for law enforcement agencies, both domestic and international (Holt, 2018). Additionally, organizations face challenges in protecting critical infrastructure because cybercriminals target weak spots in a company's defenses through data breaches (Aleem, 2019). As technology continues to advance, local governments are digitizing data online, resulting in data breaches that can stop services for days and sometimes months on local government's data systems (Preis & Susskind, 2020). Consequently, in 2014, President Barack Obama put in place five major legislative proposals for cybersecurity. The initiatives included the National Cybersecurity Act of 2014, Federal Information Security Modernization Act of 2014, Cybersecurity Workforce Assessment Act, Homeland Security Workforce Assessment Act, and the Cybersecurity Enhancement Act 2014 (Promnick, 2017). President Obama's purpose for signing the five legislative bills was to protect federal agencies from

cyberattacks while improving the United States' cybersecurity infrastructure (Bayard, 2019). Although these helped enhance the federal government's cybersecurity infrastructure, many of the laws enacted did not address issues that organizations face regarding liability limitation to protect private organizations that share cybersecurity information with the federal government (Promnick, 2017).

As the federal government continues to build its cybersecurity infrastructure, federal agencies find it challenging to police cybercrime incidents online (Bayard, 2019). In 2019, the United States experienced 162 publicly reported ransomware attacks at the municipal and state levels, which surpassed the total number of attacks in 2013 and 2018 (Freed, 2019). However, local law enforcement agencies that have extreme cybercrime situations rely on organizations such as the Federal Bureau of Investigation (FBI), U.S. Secret Service, and Customs Enforcement's Homeland Security Investigations (Brunner, 2020). Law enforcement agencies statewide have built cybercrime units with police organizations but face the challenge of closing the cyber enforcement gap based on the staff's lack of experience in investigating cybercrimes (Brunner, 2020). States have also been hesitant to acknowledge the need to use cybersecurity strategies. But due to the lack of guidance from the federal government, law enforcement agencies are still working to address cybercrime incidents (Bayard, 2019). With the ongoing cybercrime threats to individual citizens and organizations, law enforcement agencies have shifted their policing strategies to better prepare for computer-related incidents (Hull et al., 2018).

Chapter 1 provides the background of the study regarding law enforcement officers' perceptions in combating cybercrime at the local level. This chapter includes the

study's background, problem statement, purpose statement, and research questions. It also included the theoretical framework, the nature of the study, definitions of key terms, assumptions, scope and delimitations, limitations, and significance of the study.

Background

From the first inception of computers in the 1950s to the development of the internet, society has become dependent on computers and digital devices (Wydra & Hartle, 2015). The American Community Survey estimated that in 2016, 89% of Americans had some form of technology in their household, whether it was a computer or mobile device, which indicates that technology is a part of everyday life in many households (Ryan, 2018). Social media has provided an easy solution to searching through digital information over the internet while having a positive impact on the daily lives of individuals and organizations (Bou-Hamad, 2020). In the past decade, social media has also become an essential part of life that impacts people's cultural, economic, and social lives (Soomro & Hussain, 2019). According to Statista, over 2 billion social media users used the internet worldwide in 2019, which was projected to increase to over 3 billion users by 2021. Internet users use social media sites such as Facebook, Twitter, and YouTube to communicate, post advertisements, and job postings.

As individuals use technology for business and leisure, cybercrimes such as child pornography, hacking, and software piracy will only increase (Willits & Nowacki, 2016). The more individuals use the internet, the more people will become cybercrime victims due to the cyber criminals' ability to target individuals and businesses online (Horsman, 2017). Cybercrime has become interconnected with the daily lives of individuals who use

the internet such as online theft and fraud. Criminals are using social media sites to commit burglary, social engineering, identity theft, and cyberstalking (Soomro & Hussain, 2019). Moreover, criminals are injecting viruses and malware into links, messages, and attachments on social networking websites (Soomro & Hussain, 2019). Cybercriminals generate around 3.25 billion dollars globally each year from online crimes, which accounts for at least 20% of social media infections from add-ons and plug-ins on various social media platforms (McGuire, 2019). Further, the internet provides platforms for distributing images depicting child sexual abuse, which has become widespread, posing a concern for law enforcement officers' ability to handle the influx of cases.

Cybercrimes have caused concerns among governments, organizations, and individual citizens due to the economic impact of losses suffered by cyber-attacks. For example, a cyber-attack on a computer processing network could cost an organization around $50 billion to $120 billion in economic damages (Mee & Schuermann, 2018). Additionally, the banking sector has faced significant losses of $18.37 million, followed by utilities at 17.84 million, software at $17.84 million, automotive at $15.78 million, and insurance organizations faced an average loss of $15.76 million annually due to cybercrimes (Accenture and the Ponemon Institute, 2019). The United States is one of the top countries that suffer expensive cybercrime attacks, which is 50% more than other countries compared to the global average (Accenture and the Ponemon Institute, 2019). In 2020, the American public filed over 700,000 cybercrime complaints that totaled over

$4 billion in losses filed, which increased by 69% from complaints in 2019 from the FBI (FBI Internet Crime Complaint Center, 2020).

Cybercrime is a priority for national and international law enforcement agencies due to the escalating rise in cybercrime cases worldwide. It is critical for law enforcement agencies to protect individuals and organizations from online attacks as more people and businesses become more reliant on modern technology. However, there is a lack of research exploring law enforcement officers' perceptions in combating cybercrime at the local level. There is a need for exploring the perceptions of officers because they are the first indivduals asked to respond to cybercrimes (Harkin et al., 2018). This study aimed to understand law enforcement officers' views regarding combating cybercrimes at the local level. In addition, this research study helped in understanding law enforcment officers perceptions in combatining cybercrime at the local level.

Problem Statement

Cybercrime serves as a massive technical challenge for law enforcement agencies at the federal, state, and municipal levels. Even though the FBI and other special cybercrime units are essential to cybercrimes investigations, local officers are the first to respond and serve as the first point of contact to victims (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2018; Levi et al., 2016). Officers respond to online incidents such as child exploitation and identity theft (Holt et al., 2019). But officers face multiple factors that could deter their perceptions of online fraud and their ability to respond to cybercrimes. Some of the reasons include law enforcement agencies' lack of interest, officers' perceptions that cybercrimes are not their responsibility, and

officers' lack of experience in investigating cybercrimes (Bossler et al., 2019). Further, law enforcement officers have expressed a different opinion when it comes to responding to cybercrimes. Many police officers have described a sense of powerlessness due to their inability to react to computer-related incidents related to more traditional crimes (Hadlington et al., 2018). However, there is a gap in the literature exploring law enforcement officers' perceptions in combating cybercrime at the local level. In addition, there is limited peer-reviewed research that pertain to law enforcement officers' perceptions in combating cybercrime at the local level. This research helped in determining if law enforcement agencies were prepared to combat cybercrimes at the local level.

Purpose Statement

The purpose of this study was to explore law enforcement officers' perceptions in combating cybercrime at the local level. Law enforcement officers included sheriffs and deputy sheriffs, state police officers, detectives, and particular jurisdiction police such as college and university police as well as public-school district police. The population identified in the study included sworn law enforcement officers located in Texas. The implication for positive social change lies in the potential to improve unreported cybercrime incidents at the municipal level and reduce computer crimes while improving the processes for organizations and communities to report computer-related incidents to law enforcement.

Research Questions

The research questions helped guide this qualitative research study:

RQ 1: How do law enforcement officers' who respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally?

RQ 2: What factors, if any, limit law enforcement officers from responding to computer-related incidents locally?

Theoretical Framework

I combined the structural contingency theory and Porter and Lawler's motivation theory to explore law enforcement officers' perceptions regarding combatting cybercrime. The structural contingency theory was conceptualized in 1967 by Lawrence and Lorsch, who created two core assumptions: (a) there is no one single way to structure work in an organization, and (b) different approaches to organizational structures are not all equally effective (Donaldson, 2001). The structural contingency theory also focuses on three contingencies: (a) environment, (b) size, and (c) strategy that helps make the contingencies remain effective (Donaldson, 2001). The structural contingency theory applies to law enforcement organizations based on the assumption that organizations attempt to meet external situational circumstances that may impact the organization (Donaldson, 2001).

The other theory used in the study was Porter and Lawler's (1968) model of motivation, an extension of Victor Vroom's (1964) expectancy theory. Porter and Lawler's model focuses on what motivates an individual to complete a task based on the type of reward the individuals expect to receive upon completing a job task (Kesselman et al., 1974). The lack of required response to cybercrime may be a contributing factor to law enforcement officers' limited amount of interest in responding to technology-enabled

offenses (Holt, 2018). This study is thus based on the model of motivation theory by Porter and Lawler, which states that an individual is motivated on the job based on four key variables: (a) effort, (b) performance, (c) reward, and (d) satisfaction (Jalal & Zaheer, 2017). The two theories applied to the study helped in analyzing law enforcement officers' perceptions to combatining cybercrime at the local level.

Nature of the Study

The qualitative method was used in the study. Qualitative research describes a set of approaches from a natural expression or experiences of an individual, which helps analyze collected data ()Levitt et al., 2018). Qualitative research is a helpful method that provides the researcher with the knowledge and understanding of participant's actions in a detailed manner (Peck & Mummery, 2017). Qualitative designs include a case study, the narrative study, and the phenomenological study. The case study approach helped in providing an in-depth understanding of police perceptions because it focuses on identifying cases such as an event, program, or activity with a real-life approach (Creswell & Poth, 2018). On the other hand, the narrative research approach helps in exploring participants' life experiences expressed in their own words (Ntinda, 2019). This approach was not appropriate because the research does not focus on an individual or biography of a person. Additionally, phenomenology can be used by the researcher while conducting a study regarding participants' lived experiences at or during the time the event occurs (Ashiq et al., 2020). However, this specific approach was not appropriate. The case study approach was the best approach in this study because it enabled me to conduct an in-depth exploration of phenomena, which in this study

included law enforcement officers' perceptions in combating cybercrime at the local level.

Definitions

Attacker/hacker: A user who attempts to gain access to an information system without official authorization (Tagarev, 2016).

Breach: The act of accessing an individual's personal information without consent results in illegal activity and improper authorization (Hemphill & Longstreet, 2016).

Contingency theory: Individuals performing a task in several distinct subsystems, with each subsystem performing a portion of the overall mission within the organization (Lawrence & Lorsch, 1967).

Critical infrastructure: The destruction of systems that impact security and data assets essential for society's functioning (Tagarev, 2016).

Cyber-attack: Cyber-attack exploits computers and networks online by intentionally using malicious devices or other methods (Samtani et al., 2017).

Cybercrime: Criminal activity targets networks and steals confidential data through an information system and communication networks (Bergmann et al., 2018).

Cyber-dependent crime: Any crime through electronic devices over the internet (Furnell & Dowling, 2019).

Threat: Circumstances that impact individuals and organizations' assets through unauthorized access to information systems designed to cause destruction or modification of an information system (Paulsen & Bryers, 2019).

Traditional policing: A strategy that involves police conducting routine law enforcement and reacting to crime after it occurs (Shane, 2010).

Vulnerability: Process resulting from a human-made or natural hazard that can impact information systems (Arghandeh et al., 2016).

Assumptions

This study involved three assumptions. The first assumption was that most law enforcement officers feel that responding to computer crimes at the local level is the federal government's job or the cybercrime taskforce's job. Second, law enforcement officers are not committed to responding to cybercrimes because of the lack of unreported cybercrime incidents by organizations and citizens in the community. Third, I assumed that law enforcement officers do not have the time or resources to address computer crimes because they are familiarized with responding to traditional crimes such as burglary and theft. Although the assumptions listed were not proven, all premises were necessary to the qualitative case study to understand law enforcement officers' perceptions in combating cybercrime at the local level.

Scope and Delimitations

Delimitations are the aspects of a study that are in the researcher's control, where the focus is on the theoretical background, objective, research study, and the study sample question (Forero et al., 2018). The delimitations for this qualitative case study consisted of nine interviews with law enforcement officers. The scope was limited to law enforcement officers in order to keep the research manageable and provide a more detailed analysis. The study population was limited to law enforcement agencies,

including police departments, sheriff departments, university police, and school district police departments within the Texas area.

Other professional populations related to responding to cybercrimes at the local level, such as cybercrime units or task forces within a police department, could have been selected in the study because they were responsible for responding to offenses such as identity theft and cyberbullying. However, the officers who work for the cybercrime units or task forces in a law enforcement agency have the appropriate training and knowledge to investigate computer crimes in a law enforcement agency, as this is their primary responsibility. In addition, law enforcement officers in the United States represented a gap in the literature regarding law enforcement officers' perceptions in combating cybercrime at the local level. The study's findings are generalizable to local law enforcement officers in Texas. Law enforcement agencies in other U.S. regions could likewise find this study's results useful for comparative analysis.

Limitations

This study had several limitations. Limitations in a research study represent the weaknesses within the research design that influence the outcomes and conclusion of the research; therefore, the researcher should include the potential impact of the limitations in the study (Ross & Bibler Zaidi, 2019). The study's first limitation was that the qualitative study allowed a smaller sample size instead of quantitative research that requires a larger sample size. The study's sample size included nine law enforcement officers, leading to reliability and validity issues by showing a lack of rigor within the research based on the sample size. Second, the study included law enforcement agencies located in Texas,

limiting the study's generalizability due to more law enforcement agencies needed to strengthen the research. Lastly, the research design included an open-ended research question approach with time constraints to conduct and arrange interviews based on the interviewees' availability. The open-ended research questions can become time-consuming during the inductive coding and the thematic analysis, without having proof of knowing or verifying if the study participants were truthful when answering the open-ended questions based on their lived experiences.

Significance of the Study

Law enforcement officers handle and respond to cybercrime calls; however, officers may be less interested in investigating online crimes and believe that federal law enforcement agencies and specialized cybercrime units should investigate computer offenses (Bond & Tyrrell, 2018). Researchers have not conducted studies that include information from law enforcement officers' perceptions of online crimes such as bullying and harassment (Holt et al., 2018). This study highlights formalized opinions related to law enforcement officers' perceptions in combating cybercrime at the local level. This study's significance includes filling the gap in law enforcement officers' perceptions regarding combating cybercrime at the local level. Further, this study reveals limitations that shape law enforcement officers' views of combating cybercrime at the local level.

Additionally, the outcomes from the study can contribute to positive social changes by empowering law enforcement elected officials, public servants, and community members to know the essentials of including law enforcement personnel in the fight to combat cybercrime. In addition, law enforcement officials can establish

policies and procedures for law enforcement officers and agencies to respond to cybercrime offenses appropriately at the local level. Law enforcement officers' may become aware of cyber threats and assume an active role in supporting federal agencies and task forces in implementing cybercrime measures to improve their cybersecurity posture at the local level. The study's results can thus lead to improved cybercrime resiliency at all law enforcement levels, including the national and international levels for law enforcement agencies' cybersecurity involvement.

Summary

The perceptions of law enforcement officers related to combating cybercrime at the local level have gone largely unnoticed in the current literature. Previous research on combating cybercrime has focused on the federal government and task forces, rather than concentrating on the personal experiences and perceptions encountered by law enforcement officers regarding combating cybercrime at the local level. There is a need to explore more academic research on cybercrime prevention and cybersecurity research to match the cybercrimes that have become problem worldwide (Sarre et al., 2018). This qualitative study addressed officers' perceptions of the law enforcement agency's ability to combat cybercrime at the local level by targeting law enforcement officers in Texas who respond to various criminal incidents. Addressing law enforcement officers' perceptions on cybercrime can contribute to developing and implementing a cost-effective strategy for law enforcement agencies to combat cybercrime at the local level. The next chapter provides a synthesis of the historical and current literature viewpoints

concerning cybercrime factors and law enforcement officers' perceptions in combating cybercrime at the local level.

Chapter 2: Literature Review

Technology has created enormous benefits; however, it has also become a new way for criminals to commit crimes online. Law enforcement officers are accustomed to dealing with conventional crimes, those physically committed against persons or property, which has made it challenging for law enforcement agencies to keep up in reducing computer crimes (Nouh et al., 2019). For instance, academic scholars in England and Wales have indicated that reducing common physical crimes such as property offenses has not decreased, but rather shifted to online offending (Caneppele & Aebi, 2017). The FBI Internet Crime Complaint Center in the United States reported an estimated loss of $1.42 billion to online fraud in 2017 (FBI Internet Crime Complaint Center, 2018). Law enforcement officers find themselves serving dual roles in conducting criminal and cyber investigations. Moreover, law enforcement agencies at all levels have pressure in responding, recovering, preserving, and analyzing digital evidence committed by cybercriminals (Dolliver et al., 2017).

Despite the increase in cybercrimes, state and local governments are hesitant to address cybercrimes because of the lack of knowledge and training officers have regarding cyber investigations (Brunner, 2020). Law enforcement agencies turn to the FBI and the U.S. Secret Service to investigate cybercrimes (Griffith, 2017). However, federal agencies such as the FBI and Secret Service cannot handle every criminal case with a cybercrime element, which places pressure on local law enforcement agencies to handle much of the work in responding to cybercrimes at the local level. State and local governments have implemented cybercrime taskforces for investigating, building, and

prosecuting cases involving computer crimes (Brunner, 2020). But local law enforcement agencies that address cybercrimes could affect law enforcement officers' perceptions of responding to cybercrimes, depending on how well the officers interpret the importance of responding to cybercrimes over traditional crimes (Burruss et al., 2019; Holt, 2019). The response of law enforcement officers is disinterest in responding to computer-related incidents due to a lack of relevant skills in resolving the situation (Conway & Hadlington, 2018). Because cybercrime is on the rise (Levi, 2017), local law enforcement agencies' need to respond to policing cybercrime due to the increased level of cybercrime incidents.

In this study I examined law enforcement officers' perceptions in combatining cybercrimes at the local level. I also investigated why law enforcement officers develop trust or distrust in the agency's ability to address computer crimes. Above all, the perceptions developed from law enforcement officers at the local level regarding response to computer-related incidents create a potential problem in policing cybercrime.

Chapter 2 presents an analysis and synthesis of the study's theoretical framework: structural contingency theory and Porter and Lawler motivation theory. The literature review for this study also includes prior assessments of influential cybercrime factors that impact law enforcement officers' perceptions in combating cybercrime at the local level. Additionally, the literature review examines cybercrime and law enforcement's historical perspective. The history of cybercrime in the literature review provides awareness of social issues that have evolved among law enforcement officials, the public, and law enforcement officers.

Literature Review Strategy

The literature review includes published articles and journals used to provide a historical perspective of cybercrime and its impact on law enforcement officers' perceptions of responding to computer crimes as well as law enforcement agencies' ability to address computer crimes. Peer-reviewed journal articles and book reviews were obtained from Google Scholar and Walden University library using the Criminal Justice Database, Eric database, Emerald Insight, SAGE Journals, Springer e-books, Taylor and Francis Online, and Soc Index databases. During the search for journal articles, the following keywords were used: *cybercrime, policing, computer crimes, victimization, perception, law enforcement officer, police administration, police-reported cybercrime, criminal justice, digital forensics, law enforcement officers, internet crimes,* and *online fraud*. The listed study sources helped in determining if any pertinent information would apply to this study.

Theoretical Framework

Organizational structure theory and institutional theory were among many of the potential ideas sought after in this study. However, Lawrence and Lorsch's structural contingency theory and Porter and Lawler's motivation theory model fit this study. These will be discussed in the following sections.

Structural Contingency Theory

The dynamics of traditional crimes committed online continue to challenge how law enforcement agencies at the municipal, state, and federal levels handle cybercrime investigations. Traditionally, federal law enforcement agencies had the responsibility of

investigating cybercrimes (Brunner, 2020); however, state agencies have emphasized the need to address the cybercrime challenges to reduce future computer crimes. The structural contingency theory was applied to the study to understand law enforcement organizations' impact and role in responding to cybercrimes at the local level. Lawrence and Lorsch (1967) sought to understand how organizations can adapt to meet their immediate environment needs. Moreover, Lawrence and Lorsch's approach helps explain police organizational behaviors surrounding law enforcement agencies' ability to respond to cybercrime, a driving force behind how organizations make their agency decisions based on environmental factors such as responding to cybercrimes (Matusiak, 2019).

Law enforcement agencies' response to cybercrimes convey a broad message to individuals and businesses about the agencies' priorities regarding addressing cybercrimes, which could influence how individual citizens report cybercrimes. When contingencies change in the environment, police departments adjust their organization strategy to respond to their areas of concern (Donaldson, 2001). In other words, police chiefs in law enforcement agencies make changes in the organizational structure, which allows the leaders to maximize their goals for the agency's success (Matusiak, 2019). Additionally, the contingency theory relates to cyber policing because local police departments are likely to devote more resources to policing cybercrimes as threats become more prevalent and costly to society (Willits & Nowacki, 2016).

Differentiation and Integration in Complex Organizations

In 1967, Lawrence and Lorsch conducted a study on differentiation and integration in complex organizations. They explored the relationship between two main

concepts, differentiation, and integration within six organizations, by dividing each subgroup into specific sections. The study's goal was to determine if organizations could meet their environmental requirements while holding positive economic performance within the organization. Moreover, Lawrence and Lorsch noted that differentiation in an organization occurs when each division within a subgroup can develop its own cultures and methods. Lawrence and Lorsch's differentiation and integration in complex organizations study have validity because of the organizational structure that law enforcement agencies operate.

In relation to the current study, law enforcement agencies have the autonomy and the power to develop a culture within the agency that accomplishes the single mission of creating a safe environment for individual citizens and businesses within the community. The study on differentiation and integration revealed possible influences or causations of law enforcement agencies' culture and methods regarding investigating cybercrimes as an organization. Additionally, the research conducted by Lawrence and Lorsch regarding differentiation and integration in complex organizations helped in exploring law enforcement officers' perceptions in combating cybercrime at the local level. With the rapid increase of electronic crimes in the United States, law enforcement agencies could become an integral part of the fight against cybercrime. The structural contingency theory's relationship with law enforcement agencies as an organization extends the necessity to explore law enforcement officers' perceptions in combating cybercrime at the local level.

Porter and Lawler Theory of Motivation

Porter and Lawler's (1968) motivation theory also provided a framework for examining law enforcement officers' motivational factors in responding to computer crimes at the local level. Porter and Lawler proposed that the motivation premises focus on how individuals are motivated based on intrinsic and extrinsic rewards (Lawrence & Lorsch, 1967). Intrinsic motivation refers to an individual working for self-satisfaction as a reward, whereas extrinsic motivation focuses more on the satisfaction that results in tangible or verbal rewards (Gurmeet, 2020). Officers' intrinsic and extrinsic motivators could impact officers' perceptions in combating cybercrime at the local level. An officer's motivation can come from promotions or by just keeping the community safe. Federal agencies such as the FBI and specialized cybercrime units can also influence patrol officers' decisions in responding to computer-related incidents locally. Research has indicated that law enforcement officers feel that responding to cybercrimes is something that they should not be responsible for policing because it was not their responsibility (Black et al., 2019).

Porter and Lawler's theory of motivation was influential regarding a police officer's willingess to respond to cybercrimes locally. Thus, the possible lack of exposure that law enforcement agencies face in response to cybercrimes could influence law enforcement officers' perceptions of responding to cybercrime (Burruss et al., 2019). Additionally, law enforcement officers' exposure to responding to cybercrime was an essential factor to consider in this study.

Literature Review

History of Computer Crimes

Some of the earliest forms of cybercrime took place in the 1970s and 1980s. One example of an early cybercriminal is John Draper, also known as “Captain Crunch” (Ratikant, 2017). Draper was arrested during the 1970s for phone tampering by using a whistle located in a Captain Crunch cereal box to commit his crimes. The whistle that Draper used produced a 2600Hz frequency that enabled him to make free phone calls. As more people continued to use computers and the internet in the 1970s, more criminals were committing cybercrimes, which increased to malware and cyber fraud. In the 1980s, Ian Murphy hacked into the AT&T system, changing the functionality of the organization’s internal clock, which disrupted phone services (Ratikant, 2017). Affitionally, in 1988, Robert Morris created the first computer worm that infected the Advanced Research Projects Agency networks, which shut down 10% of the computer systems attached, causing the creation of the Emergency Response Team Coordination Center, whose responsibility is coordinating cyber-attacks (Grispos, 2019). Further, computer viruses such as ‘Melissa’ and ‘I LOVE YOU’ in 1991 were threats developed for computers, which resulted in email systems failures (Bayard, 2019). By the early 2000s, cyber-attacks from cybercriminals became more targeted and sophisticated.

Hackers in the past used their technical skills to conduct illegal activities online for fun (Paquet-Clouston et al., 2018); however, in the 21st century, hackers are using the internet to gain monetary and political advantages, as computers and internet have revolutionized how the world operates (Jaishankar, 2018). People trust digital devices

like a cell phone to store sensitive information like bank account passwords, email passwords, and email information for easy accessibility (Mirdul & Satvinder, 2019). Cybercriminals disguise their online presence by using spoofed networks to gain access to the victim's electronic device or account, which makes identifying the offender challenging (Dodge & Burruss, 2019). Users also make themselves vulnerable to cyber-attacks by downloading applications and giving third-party organization permissions to access their mobile devices (Mirdul & Satvinder, 2019). For example, in 2018, around 150 million user accounts from the MyFitnessPal mobile application were compromised, which resulted in cybercriminals obtaining stolen usernames, email addresses, and passwords (Kamara & Scott, 2019). Organized gangs in the 21st century are now using computer networks to infiltrate and take advantage of computer users (Kumar, 2019) as well as organizations. In 2014, a group named Guardians of Peace located in North Korea launched a cyber-attack on Sony Entertainment, which wiped out half of Sony's global digital network (Grispos et al., 2017).

The presence of online usage for citizens globally has a significant risk that exposes citizens to threats while using the online services (de Bruijn & Janssen, 2017). Cyber-attacks have become an everyday occurrence with cybercriminals, which involves exploiting citizens during the COVID-19 pandemic in 2020 (Gatlan, 2020). Over the past two decades, the evolution of cybercrime has become more sophisticated for cybercriminals that aim to stay under the radar while attempting to exploit people every day (Boddy, 2018). Countries could also face critical infrastructure consequences resulting in power grids and water supply companies shutting down due to a cyberattack,

impacting the economy (Xingan, 2018). Ever-changing technology has placed an enormous burden on law enforcement agencies that struggle with addressing cybercrime. Computer crimes have become one of the top priorities for federal and local law enforcement agencies due to the steady increase in cybercrime incidents on a national and international level.

Cybercrime Concerns

The Pew Research Center indicated that 42,000 people in 26 countries listed cyberattacks as the third-largest threat in the world behind ISIS terrorism and climate change due to the surge of cybercrime activity across the world (Poushter & Manevich, 2017). Another example of cybercrime activity was the 2016 U.S. presidential election. It became a central theme for potential cyber threats to the nation's voting machines, which raised alarms to government agencies concerning the state of U.S. national security (Berghel, 2017).

As more people continue to use technology, cybercrime will become more prevalent, and the burden of responsibility to investigate cybercrimes will rely on all levels of law enforcement (Burruss et al., 2019). Organizations and individual citizens face computer-related crimes daily; however, law enforcement agencies face challenges in handling crimes, which brings extensive media coverage about policing, coupled with financial cutbacks that result in limited resources (Boddy, 2018). Cybercrimes are on the low priority list for policing, due to police not being able to devote resources due to responding to traditional crimes (Johnson et al., 2020). Criminologists have examined the training, attitudes, and capabilities of policing (Dodge & Burruss, 2019). Due to the surge

of cybercrime activity across the world, many countries have launched actions and educational programs that aim to increase officers' effectiveness and efficiency in response to high-tech crimes online (Cunha et al., 2016).

Jurisdictional Boundaries

As new types of computer crimes emerge, law enforcement agencies face the daunting task of responding to cybercrimes that consist of extracting, analyzing, and processing evidence collected from digital crime scenes (Losavio et al., 2016). In addition, the borderless nature of cyberspace has provided opportunities for users to use the internet for legal and illegal purposes. Today, law enforcement agencies have challenges investigating cybercrimes designated within a particular geographical jurisdiction or patrol territories (Wang et al., 2020). Remote online crimes pose a significant challenge to policing because criminals use the internet as a tool to commit the crime (Finklea, 2017). Therefore, federal and state organizations often work together by focusing on different responsibilities related to investigating computer crimes.

State police agencies focus on cyber-enabled offenses, while federal law enforcement agencies such as the FBI focus on handling more severe and complex computer cases such as malware attacks (Harkin et al., 2018). However, with the lack of a universal definition for cybercrime, federal and state law enforcement agencies find it difficult to prosecute or punish individuals for crimes committed online (Paek et al., 2020). Even though law enforcement officers encounter an enormous amount of cybercrimes, triages are set up to determine what officers can and can not realistically investigate and solve (Macdonald, 2021). For example, if a computer-related offense

occurs, it is undetermined at times if local law enforcement should engage and assist the victim or if the victim should be referred to a federal agency or cybercrime unit to file a incident report (Cross, 2019). Further, cybercrime jurisdiction makes it challenging for cybercrime victims to know where and whom they need to report a computer-related offense.

Therefore, jurisdictional challenges can shape how local law enforcement agencies view cybercrimes, which could impact their perceptions in how they respond to cybercrime at the local level. As a result, law enforcement agencies defer cybercrime incidents to federal agencies because of their worldwide reach and ability to investigate various cybercrimes (Griffith, 2017). Therefore, online crimes committed remotely is problematic to investigate for law enforcement because it slows down the process of apprehending and prosecuting the alleged offender (Cross, 2019).

Prosecuting Cybercrime

The Department of Justice has invested in prosecuting entities associated with foreign states engaged in cybercrime, economic espionage, and sanctions over the past decades. However, countries are creating laws regarding how cybercrimes are handled, making it challenging to apprehend offenders because of the extradition agreements set by foreign legal systems (Holt et al., 2018). But with the lack of extradition agreements between the United States, China, Russia, Ukraine, crimes committed online are difficult to prosecute (Monteith et al., 2021). As a result, keeping pace with prosecuting online crimes is challenging because of the steady advancements of technology and the lack of changes to how online crimes are prosecuted (Maroz, 2019). Therefore investigating

online fraud can cost money and time regarding the prosecutor's hours spent obtaining statements to prosecute a case.

Cybercrime Taskforce in Law Enforcement

When it comes to investigating cybercrimes nationwide, the primary responsibility rests with the FBI because of the organizations' ability to investigate online crimes that are domestic and foreign. The FBI established the National Cyber Investigative Joint Task Force as a presidential directive to disrupt cyber-related threats to the United States (Finklea, 2020). However, federal law enforcement agencies face challenges in addressing the significant workloads of investigating common cybercrimes that impact the United States economy (Brunner, 2020).

The FBI has implemented various taskforces and partnerships throughout the United States to focus on cyber threats. As a result, law enforcement agencies use skilled specialized cybercrime units to investigate computer-related incidents (Holt, 2018). However, law enforcement officials have admitted that internet crimes are challenging to investigate (Lee et al., 2019). Therefore, cybercrime units aim to maintain relationships with organizations and institutions while responding to local cybersecurity threats (Finklea, 2020).

Cybercrime units respond to online cyber offenses committed within a particular jurisdiction in the United States (Harkin et al., 2018). The FBI has around 56 field offices in the United States that respond to and investigate computer crimes. For instance, the National Police Chiefs' Council in the United Kingdom established cybercrime units at all local law enforcement agencies in England and Wales, where the government

provided money to help fund the units at the local level (Gould, 2018). Creating task forces with the support of state and federal agencies is critical in keeping the nation safe and secure from online threats.

Moreover, with the increased volume of cybercrime offenses, the demand for local law enforcement agencies' intervention has increased (Bond & Tyrrell, 2018). As a result, in 2014, Europol created its first international cybercrime task force known as the Joint Cybercrime Action Taskforce, designed to prepare, detect, and execute cross-border cybercrime investigations (Aiken et al., 2019). The J-CAT responsibilities focus on gathering intel from national intelligence databases for future cybercrime threats. The formation of J-CAT represents various countries willing to investigate and prosecute cybercrimes (Flory, 2016). The J-CAT has partnerships with countries like the United States, Europe, Canada, Australia, and Colombia to investigate and prosecute crimes online (Cross, 2020). Although there is no single solution to solving the cybercrime threat, creating cybercrime units is a crucial element that helps law enforcement agencies at all levels effectively respond to fighting cybercrime. Therefore, cybercrime units help reduce cybercrime cases for law enforcement agencies (Willits and Nowacki, 2016).

Law Enforcement Budget

Law enforcement officials face challenging decisions regarding what will or will not go into the annual budget for law enforcement agencies. For example, President Barack Obama allocated around $19 billion to government agencies to combat cybersecurity in 2017, a 35% increase from 2016 (An & Kim, 2018). Additionally, the Department of Justice allocated $121.1 million to federal agencies' to expand cybercrime

operations while providing an additional $2.0 million to local and tribal agencies to help fight cyber threats (James, 2017). The beneficiaries of increased funding for cybercrime prevention are security and intelligence agencies instead of the local police organizations (Dupont, 2017).

The lack of funding for police departments decreases officers' chances of receiving additional cybercrime training because of the higher priorities on traditional crimes at the local level (Belshaw, 2019). Previous research has indicated that law enforcement agencies place lower priorities on cybercrimes because of the extra spending needed to investigate computer crimes (Burruss et al., 2019; Holt, 2019). Due to departmental sizes and the cost of equipment to investigate cybercrimes, the use of software for cybercrime investigation training may not be cost-effective for law enforcement agencies with a limited budget (Keeling & Losavio, 2017). For this reason, the general budget plays a vital role in consideration for law enforcement officials when deciding what is needed or not needed to maintain the agency's daily operations while keeping the community safe (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2018). As a result, law enforcement agencies prioritize community-based crimes that reflect the community's needs because of budget constraints.

Law Enforcement Training

As it relates to law enforcement agencies' preparedness in combating cybercrime at the local level, there is a need for police organizations to provide cybercrime training to law enforcement personnel. Further, cybercrime training provides law enforcement personnel with the necessary skills to effectively respond to computer crimes, despite the

challenges law enforcement organizations face in determining officers' roles in combating computer crime locally (Cockcroft et al., 2018). Cybercrime training has significance in ensuring that police-led approaches address cybercrimes adequately (Koziarski & Lee, 2020). Law enforcement agencies' investigative process when investigating traditional crimes is different from cybercrime investigations; therefore, a need to build on officers' skills and knowledge in investigating advanced crimes is needed (Nouh et al., 2019).

Law enforcement officials need appropriate training in cybercrime-related incidents to help solve a crime, identify the suspect, and make an arrest. However, law enforcement agencies do not have the necessary skills suitable to investigate cybercrimes. Further, officer training focuses on traditional approaches, which are not conducive to addressing the cybercrime landscape (Cunha et al., 2016). As a result, law enforcement officials have displayed an unwillingness to dedicate resources to combat computer crimes (Graham et al., 2019).

In response to escalating cybercrime demands, the Bureau of Justice Assistance created a Law Enforcement Cyber Center with an online portal and clearinghouse designed to help local law enforcement agencies respond to cyber threats through online training (Romanosky et al., 2017). Moreover, the creation of the LECC enhances local law enforcement in preventing and investigating cyber incidents.

Equally important, the National White Collar Crime Center is another organization that provides law enforcement professionals at the state and local level with web-based training modules to understand high-tech cybercrimes (Flory, 2016).

However, fragmentation could pose a problem for creating police training programs for law enforcement because the organization has various departments (Cunha et al.,2016). As a result, local law enforcement agencies are not taking full advantage of the opportunity of using cybercrime training provided by federal agencies and college institutions, which puts law enforcement at a disadvantage in their efforts to combat cybercrime (Flores, 2016). Understanding whether Local law enforcement takes a generalist or specialist approach to find ways to offer officers cybercrime training is significant to understand (Willits & Nowacki, 2016). It is essential to review factors that impact local law enforcement's inability to respond to cybercrimes based on inadequate training (Holt et al., 2018). However, the cybercrime training that local law enforcement receive may be superficial and not practical (Forouzan et al., 2018). Therefore, it is crucial for all sworn law enforcement officers at the state and local levels to receive in-service training for digital evidence collection because it can help officers better understand how to recognize and adequately collect digital evidence (Brunner, 2020).

Cybersecurity Training Using Digital Technology

Crimes that law enforcement officers respond to daily may result in a digital device confiscation at the crime scene. For example, if police responded to a murder where a cellphone was a part of the crime, law enforcement officers would seize the evidence because they were the first to arrive at the crime scene. As a result, computer games could serve as a training tool for law enforcement officers' to explore complex cybersecurity problems (Coull et al.,2017). Furthermore, as a training tool, computer games can simulate real-world situations for participants to build on skills that would

otherwise be difficult to simulate in a classroom setting. For example, in 2014, under the Seventh Framework Programme, the European Commission developed severe gaming solutions that consisted of four comprehensive learning experiences embedded in the games, dedicated to enhancing intelligence analysis for trainees in cybercrime training (Zanasi et al., 2017). Therefore law enforcement officers' training is significant in developing officers' ability to effectively handle digital devices (Coull et al., 2017).

Law Enforcement Officers Perceptions of Cybercrime

Local and state law enforcement agencies have dealt with cybercrime challenges worldwide; however, there is limited research to understand officers' perceptions of serving the role as a first responder to cybercrimes within an agency (Burruss et al., 2017). For instance, cybercrime and fraud in England and Wales accounted for 5.8 million of the 12 million criminal offenses in 2015 (Burruss et al., 2019). However, law enforcement officers sometimes share the same perceived notions as the public regarding what crime is more severe than others regarding cybercrimes, influencing officers' motivation to investigate certain criminal offenses related to cybercrimes (Dodge & Burruss, 2019).

Additionally, law enforcement agencies allocate resources and funding to the more severe crimes that align with the stakeholders' perceptions in the community and the views of law enforcement officers (Dodge & Burrus, 2019). For example, law enforcement administrators find it challenging to use resources to fight cybercrimes because physical crimes require more police services and resources (Willits & Nowacki (2016). Law enforcement officers' job duties include responding to traditional crimes

such as civil disputes, murder, and robbery. For this reason, law enforcement officers may view responding to computer-related incidents as not real police work (Holt, 2019). More importantly, research has shown that law enforcement officers' who respond to computer-related crimes have displayed unenthusiastic attitudes (Holt, 2018).

Law enforcement officers' perception is that responding to computer-related incidents is a time-consuming task that takes up much of their time and that specialized cybercrime units like the FBI should respond to cybercrime incidents based on the lack of skills and resources that law enforcement agencies possess (Hull et al., 2018). In addition, an officers' unwillingness to properly investigate cybercrimes could become a problem for law enforcement response to cybercrime (Burruss et al., 2019).

International Law Enforcement Agencies Policing Cybercrime

Cybercrime is a national and international problem that security agencies and law enforcement officials deem a top priority. Traditional crimes in the United Kingdom., such as burglary, robbery, and theft, were surpassed by online fraud and other cybercrimes that have become a national priority. As a result, the traditional crimes in the United Kingdom decreased, only to see an increased rate of resident victimization regarding online fraud and cybercrimes (Loveday, 2017). Without the necessary skills to investigate cybercrimes, law enforcement in England and Wales view cybercrimes as a frequent concern (Holt et al., 2018). As a result, police constables in England and Wales are critical players in responding to cybercrime (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2018). For example, in 2011, the United Kingdom created policies on policing cybercrime with a National Cyber Security

Strategy roadmap that called for more local constables to respond to severe cybercrimes like economic and organized cybercrimes (Burruss et al., 2019; Holt, 2019). Therefore, International law enforcement agencies' strategy for combating cybercrime in the United Kingdom focuses on preparing officers for cyber threats through education and training. However, as technology improves and becomes more prevalent, cybercrime will continue to be a security threat confronting law enforcement in England and Wales (Levi et al., 2017).

In other countries such as Brazil, law enforcement agencies also face cybercrime challenges. Brazil's law enforcement agencies have limited knowledge and experience regarding high-tech cybercrimes. Therefore partnerships are formed between police academies and educational institutions to offer non-specialist officers cybercrime training (Cunha et al., 2016). More importantly, Brazilian police can only solve 5-8% of cybercrimes because of the prevailing culture of violence in the country. As a result, law enforcement officials in Brazil use most of their resources to fight traditional crimes while reducing the number of resources to enforce cybercrimes (Cunha et al.,2016). International law enforcement agencies face similar challenges in combating cybercrime as law enforcement agencies in the United States. The shortage of technical knowledge and resources can impact how an officer responds to computer-related events.

Hiring Qualified Officers

There is a critical need for cybercrime professionals in public and private sectors in the United States. Law enforcement agencies need skilled professionals to protect critical infrastructures on the state and national levels. The increased level of cyberthreats

over the internet has created an unfilled gap in the cybersecurity workforce, which has led to a shortage of cybersecurity personnel (Vogel, 2016). As cybercrime threats increase, law enforcement assistance is needed around the clock to support cyber threats such as online child exploitation and payment scams (Interpol, 2016). Information security is one of the fastest-growing occupations that is steadily expanding.

Law enforcement agencies can respond to computer-related incidents if they have a well-trained staff (Cunha et al., 2016). However, the International Information System Security Certification Consortium report suggests that the lack of recruiting and training young people is a challenge that continues to exist globally with cybersecurity professionals (Pencheva et al., 2020).

The advancement of technology has created an environment where crime flourishes over the internet (Horsman, 2017). Unfortunately, law enforcement agencies struggle to keep qualified personnel on staff to investigate cybercrimes because private organizations offer better employment opportunities. However, as law enforcement continues to prevent cyber-attacks against critical infrastructures, there is a need for a skilled cyber-literate workforce. For this purpose, cybersecurity professionals have turned to cyber education at colleges to recruit cybersecurity students.

Over the past two decades, cyber-related offenses have increased to the point that universities have created educational and training opportunities for students wanting to pursue a career in the criminal justice field as a way to fill the gap for cybersecurity professionals. Universities have created cybersecurity programs across the country to provide courses for students interested in pursuing a career in the criminal justice field.

Students in the cybersecurity programs could learn about investigating cyber-related offenses like cyberbullying and sexting, cyberstalking, and identity theft crimes (Nodeland et al.,2019). It is essential for law enforcement agencies to recruit technologically competent individuals to become part of the criminal justice workforce and help in combating cybercrimes (Wydra, 2015). Therefore, there is a significant need for law enforcement to recruit qualified personnel to work in the cybersecurity field, which could help close the skills gap in training and knowledge.

Public Trust in Law Enforcement

The relationship between law enforcement and the community has always been a complicated and hazardous situation that has impacted various circumstances surrounding crime, race, and investigations. As first responders, law enforcement officers are the first to arrive at criminal events, civil unrest, natural disasters, which is an indication that victims of cyber offenses would contact local police when a computer-related offense has occurred (Dodge & Burruss, 2019). However, law enforcement attempts to address cybercrime over the last two decades have been the common theme that presents challenges (van de Weijer et al.,2020). Victims of cybercrimes are less likely to report future offenses to law enforcement if they know law enforcement cannot investigate computer-related incidents at the local level.

In the United States, only 8% of identity theft victims reported their incidents to police (Harrell, 2019). Another 26 million individuals under the age of 16 and older reported that they were victims of identity theft, and around 10% of identity theft victims have reported experiencing severe emotional distress due to a computer-related incident

(Harrell, 2019). In addition, the United States Attorney's Officer reported that only 15% of cybercrime victims reported their crimes to law enforcement (Leukfeldt & Holt, 2019). However, victims who file computer crime complaints with law enforcement agencies are more likely to be referred to other government agencies that handle computer crime incidents by law enforcement agencies (Cross et al., 2016). Nevertheless, research states that victims are less likely to report illegal computer activity to law enforcement due to the public belief that local departments lack adequate training to investigate cyber offenses (Graham et al., 2019). As law enforcement agencies increase their cybercrime performance, the public will gain satisfaction and confidence based on how well law enforcement handles cybercrimes in the future.

Underreporting of Cybercrime

Analyzing cybercrime victimization and law enforcement's role in the process helps better understand cybercrime exposure on victims of cybercrime incidents. Many organizations, nations, public security agencies, and people worldwide fall victim to cybercrimes every day. As a result of cybercrime victimization, organizations refrain from notifying law enforcement if a data breach occurs because businesses are concerned with losing customer data and diminishing their organization's reputation with the public (Bidgoli et al., 2019). The underreporting of cybercrime is related to how state and local law enforcement agencies collect data regarding cybercrime incidents under the Uniform Crime Report used to compile U.S. crimes committed each year (Brunner, 2020).

However, the U.S. is notorious for not providing national fraud statics for crimes committed (Levi, 2017). The federal government admitted to only capturing 12% of

cybercrimes from self-reporting online databases, failing to measure cybercrimes in a meaningful way (Decker, 2019). Researchers have indicated that victims of cybercrimes are less likely to report cyber offenses to police over traditional crimes due to not trusting police experience in investigating computer-related incidents (Graham et al., 2019). The reasons for underreporting include victims believing that the cybercrime was not severe, unaware of the crime committed, feeling embarrassed about becoming a victim, feeling self-blame for becoming a victim, reporting the cybercrime is a waste of time, and there is a low probability that law enforcement will catch the perpetrator (Bidgoli et al., 2019). Underreporting cybercrimes makes it challenging to determine the real toll cybercrimes have on the economy (Brunner, 2020).

Summary

Cybercrime has become a persistent problem for law enforcement agencies that continue to grow in developing nations and nations with higher development levels (Harkin et al., 2018). As federal law enforcement agencies attempt to address cybercrimes, there is a need for an effective enforcement strategy that includes state and local governments partnering together to form a law enforcement approach to the problem (Brunner, 2020). Furthermore, society's dependency on information technology has ushered in new opportunities for cybercriminals to conduct criminal activity (Furnell & Dowling, 2019). As a result, previous research has indicated that law enforcement agencies struggle to address cybercrimes and cannot keep pace with the sophistication of the cyber-attacks launched (Willits & Nowacki (2016).

Therefore, it is vital to understand whether law enforcement agencies can address cyber incidents locally because officers are the first to arrive at a crime scene and collect evidence. This literature review includes a synthesis of many studies conducted on how law enforcement agencies respond to cybercrime. The structural contingency theory and Porter and Lawler's theory of motivation was the framework used to explore officers' perceptions in combating cybercrime at the local level.

Law enforcement officers' perceptions in combating cybercrime give the impression that law enforcement agencies face challenges in responding to computer-related incidents at the local level. These assumptions come from the law enforcement officers' portrayals of what law enforcement agencies can and cannot do regarding response to cybercrimes as a first responder. Chapter 3 of the study includes the selected data collection method, rationale for the research design, interview questions, and the study's targeted population.

Chapter 3: Research Method

The purpose of this qualitative study was to develop an in-depth understanding of law enforcement officers' perceptions in combating cybercrime at the local level. Researchers have indicated that there is a limited number of studies documenting law enforcement officer's perceptions regarding combating cybercrime at the local level (Burruss et al., 2017). This chapter includes an explanation of the case study approach used for this study. It also describes the research design, the research questions that guided the research, and the rationale for using the case study approach. Lastly, I discuss the ethical procedures, the researcher's role, criteria for participant selection, details about data collection, data analysis, and validity.

Research Design

This study consisted of a qualitative intrinsic case study to explore law enforcement officer's perceptions in combating cybercrime at the local level. This qualitative approach was necessary for exploring the participants' experiences in responding to computer-related incidents. The law enforcement officers' perceptions provided feedback on the successes and difficulties officers undergo when investigating or responding to cybercrimes. The case study approach provided logical links between the collected data and the conclusion derived from the study's initial research question (Creswell & Poth, 2018). The research question in a study is an essential factor when using the case study approach because it answers *who*, *what,* and *where* questions (Rashid et al., 2019). In this study, there were two research questions: (a) How do law enforcement officers that respond to traditional crimes describe law enforcement

agencies' preparedness to fight cybercrime locally? and (b) What factors, if any, limit law enforcement officers from responding to computer-related incidents locally? The case study approach provided in-depth knowledge of the phenomenon in detail.

I used snowball sampling with the nine participants or until saturation occured in the study using semistructured interviews. Semistructured questions were appropriate to understand the phenomenon better because a general yes or no question was insufficient to obtain a meaningful understanding of law enforcement officers' responses. Semistructured interviews also allow the researcher to build a rapport with the participant, encouraging a meaningful dialogue between the researcher and the participant (Rubel & Okech, 2017). Further, observing participants in face-to-face interviews allows the researcher to view nonverbal cues, such as body language, which provide additional information that the researcher can add to the interview transcript (Oltmann, 2016). Thus, this qualitative approach helped build a comprehensive view of law enforcement officers' experiences and perceived notions regarding combating cybercrime at the local level.

Rationale

The case study approach helps researchers investigate the behaviors and opinions of the participants in the research (Hammarberg et al., 2016). The intrinsic case study approach provided an in-depth analysis of law enforcement officers' perceptions regarding combating cybercrime at the local level. The intrinsic case study approach was suitable for this study because it allows for multiple data collection methods to answer the questions regarding the participants' experiences and perspectives in the study

(Hammarberg et al., 2016). The phenomenological approach was not appropriate for the current study due to no attempt to test a targeted individual who had experienced a phenomenon through interviews only. Similarly, the grounded theory approach is helpful in research studies; however, there was no attempt to test a theory or a hypothesis. Consequently, the case study approach was appropriate for this study exploring participants' perceptions of combatting cybercrime.

Role of Researcher

The researcher has a vital role in gathering information while shaping the research study (Ravitch & Carl, 2016). As the researcher, my role was the primary data collector (Marshall & Rossman, 2016). I gathered data from law enforcement officers on their personal beliefs regarding combating cybercrime at the local level. My role was to conduct all interviews, collect supporting data, analyze and interpret data, and produce the study's final written document. My role as the researcher also included creating a finding in the study, which determined law enforcement officers' perceptions regarding combating cybercrime at the local level. Moreover, my role include ensuring that the research was ethically conducted and a credible source of information published for future researchers.

The participants in the study were asked open-ended questions based on an interview protocol outline. The interview protocol aligns with the intended interview questions, enhancing the study's data, so it is a helpful approach when interviewing participants (Castillo-Montoya, 2016). The interview protocol ensured consistency and

dependability of the research (Hoover et al., 2018). I informed the participants of the interview protocols used to protect each participant's confidentiality.

Methodology

This section includes participation selection, instruments, data collection plan, and analysis. In addition, this section will provide detailed information regarding the studied phenomenon. The purpose of this qualitative study was to describe the perceptions of law enforcement officers regarding combating cybercrime at the local level. This addressed the current limited exploration of law enforcement officers' opinions regarding combating cybercrimes at the local level.

Participation Selection

The proposed sample size for the study was 15 participants. Sample sizes in a qualitative research study depend on the richness of the data regarding the phenomenon (Malterud et al., 2016). When determining the sample size for a qualitative research study, a significant variable is applied, including the availability of enough in-depth data showing patterns and categories of the phenomenon in the study (Monteith et al., 2021). Data saturation is also a significant factor for a researcher to consider when determining the number of participants for a qualitative study (Malterud et al., 2016). Saturation is complete when the researcher cannot collect new themes or ideas that may emerge within the study (Nascimento et al., 2018).

I used purposive sampling, also known as judgmental or selective sampling, due to the participants' qualities (Etikan, 2016). The purposive sampling technique applied to this study provided the opportunity to select participants from various police departments

to explore officers' perceptions surrounding the phenomenon regarding combating cybercrime at the local level. In addition, purposive sampling allowed me to select participants who met specific criteria guidelines for the study (Etikan, 2016). I recruited participants from five law enforcement agencies, which included police departments, sheriff departments, school district police departments, and university police departments within Texas. However, if there were not enough participation from the selected law enforcement agencies, I planned on using snowball sampling, along with the use of social media platforms such as Facebook to recruit law enforcement officers who meet the study's criteria. To alleviate the ethical issue that may arise with using Facebook participants, prospective participants emailed me for additional information that included the informed consent form. The objective was to gain support from local law enforcement agencies within Texas to participate in this study.

Instrumentation

The primary focus of this study was to explore law enforcement officers' perceptions regarding combating cybercrime at the local level. The interview questions focused on understanding law enforcement officers' perceptions in combating cybercrime at the local level. The study included using a digital audio recording device for face-to-face and telephone interviews as part of the instrumentation. The use of the digital audio device was used for the interviews while recording and transcribing participants' responses. However, based on previous literature reviews regarding the phenomenon studied, there were no signs of an appropriate qualitative data collection instrument for this study.

I developed an instrument to be used based on the research questions. With a researcher-created data collection instrument, a pilot study was necessary to test the instrument's credibility. In the past, pilot studies were associated with the quantitative approach to test particular research instruments. However, the pilot approach is also acceptable in qualitative research for testing research instruments' validation (Majid et al., 2017). The researcher-created data collection instrument ensured alignment between the data collection interview questions and the research questions in the study. The research included three subject matter experts to review the researcher-created data collection instrument for accuracy and credibility.

The three subject matter experts who reviewed the data collection instrument in the study were veteran law enforcement officers who currently worked in the law enforcement field with 5 or more years of service. The three subject matter experts also had similar knowledge and experiences as the other law enforcement officers targeted to participate. The three subject matter experts determined if the instrument questions for the research study needed revisions or modifications prior to implementing the study. Additionally, the subject matter experts provided feedback on potential biases and subject knowledge. Once they had reviewed and provided feedback, the data collection instrument showed accuracy and creditability. The development of this instrument assisted in establishing law enforcement officers' perceptions in combating cybercrime at the local level.

Data Collection

The study consisted of a semi-structured open-ended interview questions, unless other interview procedures such as Zoom or telephone interview were required. Semi-structured interviews involved determining the purpose and the scope of the study while developing prepared questions to help guide the study (DeJonckheere & Vaughn, 2019). Additionally, DeJonckheere and Vaughn (2019) indicated that semi-structured interviews collect information from participants who have personal experiences, attitudes, or perceptions regarding the topic of interest. Interviews as a data collection tool will help explore individual's perceptions regarding the phenomenon studied. Additionally, using the interview method as a data collection tool allowed the researcher to ask follow-up questions to explore the participant's response to the questions that required further investigation. This study's interview questions focused on gaps shown in the literature review that identify unexplored areas of research. Although I had proposed 15 participants to be interviewed for this study, nine participants were interviewed because data satuaration was achieved after nine interviews.

Upon gaining approval from the appropriate department from the five law enforcement agencies selected in Texas, I distributed information letters to interested officers or informational flyers posted within the community or via social media. The study's recruitment process began by emailing potential participants that meet the criteria of having five years of experience to participate in the research study. Additionally, a request was made to five law enforcement agencies for permission to send out participant research flyers to interested participants that wanted to take part in the study. Different

means of communications with the heads of each organization took place through emails and phone conversations to gain approval to send out research correspondence.

Interview Data

As previously stated, I was the only person collecting and managing data throughout the data collection process. During the initial data collecting phase in the research, law enforcement officers within Texas law enforcement agencies such as police departments, sheriffs' departments, university police departments, or school district police departments received an invitation letter to participate in the research study. As the participants submited their email responses of interest, I reviewed the responses and selected the participants based on a selection criterion. Additionally, I sent out an interview invitation email to the prospective participants to choose the interview time and location based on the participant's discretion.

Before the interview, each participant was contacted either by email or telephone to confirm the interview's date, time, and location. Throughout the data collection process, I managed the interview transcripts that were handwritten or recorded to ensure the interview accuracy. Participants who were not comfortable interviewing face-to-face because of the ongoing COVID pandemic had an opportunity to conduct interviews using Zoom or telephone communication. Lewis (2015) noted that an essential factor for participants in a research study is understanding their research role as the researcher gathers information.

Participants received the informed consent form along with the interview questions. Everyone that participated in the study acknowledged their acceptance to the

interview verbally along with their signature on the consent form, stating they understand their rights to decline to participate in the research study. The informed consent form ensured that participants were aware of: (a) the background and the purpose of the study, (b) the procedures used to conduct the study, (c) potential risk and benefits involved in the study, (d) compensation information, (e) confidentiality of the study, and (f) voluntariness of the participants right to withdraw from the study.

The participants who freely volunteered to participate in the study were made aware of the purpose of the investigation conducted, participants' confidentiality procedures, and the participants' right to decline the interview if they felt uncomfortable participating in the interview. Additionally, the participants were made aware of the interview procedures including the interview time, which is up to one hour, and the use of an audio recording device to capture the interview. I also assured the participants that the information collected for the interview is anonymous, and personal identifiable information was not included in the study. The interview method served as an instrument to answer the research questions regarding law enforcement officers' perceptions in combating cybercrime at the local level.

Data Analysis

The data collected from this qualitative case study approach was analyzed using the inductive approach since the phenomenon lacked much-known information. Interviews were recorded via audio with participant permission and the recordings were then transcribed (Hollweck, 2016). My personal computer was used to store data information collected from the participants' interviews. My personal computer was

password protected and secured with anti-malware software. Additionally, interview transcriptions were locked in a filing cabinet, where the information will be stored for five years, where I will only have access. After five years have expired, I will shred all documents, transcripts, and notes in a controlled area, and the digital data collected from the interview will be permanently deleted.

According to Hsieh and Shannon (2005), the conventional content analysis covers existing theories and phenomena's with limited data. The conventional content analysis method was helpful in this study because there was a limited amount of literature that examines the studied phenomenon. The data analysis process aimed to take the participants' interviews and transcribe the responses verbatim by reviewing notes and listening to the previously recorded interviews taken during the in-person interviews.

Moreover, during the data collection process, the researcher identified keywords and themes found in the data collected. The participants' beliefs helped identify any themes that emerged from the data that allowed coding in the data analysis process. Selecting a qualitative data analysis (QDA) software helped in the data analysis process because the software answered the questions regarding how and why a phenomenon should be studied. The QDA provided an in-depth insight into the data collected that would not be possible to recognize if the researcher used the hand-coding method in the data analysis. NVivo was the QDA platform selected in the study to categorize and organize the words and text to create the themes in the study.

Issues of Trustworthiness

Trustworthiness in a qualitative research study explores the validity of the researcher's research findings to establish accuracy. According to Heale and Twycross (2015), validity is the extent of measuring an idea in qualitative research. Trustworthiness has four aspects of qualitative research: a) credibility, b) transferability, c) dependability, and d) confirmability. Ravitch and Carl (2016) noted that these four elements associated with data trustworthiness are critical in helping researchers plan their study.

Credibility

Credibility is the first aspect of establishing a foundation of trustworthiness in research. Shenton (2004) suggested that credibility is a measurement of whether the researcher could learn what they intended to learn in the study. Additionally, Kaminski and Pitney (2004) indicated that triangulation member checks and peer reviews are other strategies that a researcher can use in establishing credibility in a qualitative research study. Triangulation is a strategy that uses a cross-check approach that ensures the accuracy of the study findings. On the other hand, the member checks involve the participants verifying the accuracy of their interview experiences by checking the researcher's data for proper interpretation. However, the peer review allows the researcher to have a qualified external researcher to verify the collected data systematically and conclude that the researcher reached a reasonable conclusion in the study (Kaminski & Pitney, 2004).

Transferability

Transferability is the second component of trustworthiness in a qualitative study known as external validity. Cope (2014) noted that transferability occurs when the criterion occurs. The study's findings have meanings for individuals outside of the study, who can relate the study results to their own experiences. This investigation is more suitable to provide data and education to other law enforcement agencies outside of the study's geographic area. Thus, this study findings can help law enforcement agencies explore law enforcement officers' perceptions in combating cybercrime at the local level. Transferability as validity in qualitative research involves studying one situation and adding it to another similar situation.

Dependability

The third component of trustworthiness in a qualitative study is dependability. According to Anney (2014), trustworthiness in dependability occurs by using an audit trail, stepwise replication, and code-recode strategy to evaluate the study's findings and interpretation. In the audit trail in dependability, documents such as raw data, interviews, and observation notes collected should be kept and reviewed to cross-check the inquiry process for data validation (Lincoln & Guba, 1985). Additionally, the code-recode strategy in dependability helps show validity in a study by coding and recoding the data after multiple observations. If the coding results are accurate and in agreement with the researcher, it enhances the qualitative research while improving the participants' narration in the study (Anney, 2014). The code-recode strategy is achievable in this study by coding the information the first time while waiting for one to two weeks before recording

the data for the second time for a comparison. The researcher will later check for data consistency from the code-recode strategy.

Confirmability

The last component of trustworthiness in a qualitative study is confirmability. Kyngäs et al. (2020) suggested that confirmability in trustworthiness connects the data and the results. Confirmability occurs when other researchers and readers can replicate the study results that are not conscious or unconscious biased (Morar et al., 2016). Enhancement in confirmability occurs using audit trails that include field notes that support the data and findings' connection. While using confirmability, a journal could establish a record of concerns and thoughts from the researcher and the participants relative to the data collected during the collection process.

Ethical Procedures

Ethical considerations will be made to ensure the protection of human subjects during the duration of the research study. The institutional review board (IRB) protects human subjects' involvement by requiring the researcher to obtain approval before interviewing participants in a study. The IRB's job ensures that researchers safely collect data from participants on the academic level while ensuring their rights and privacy are protected. The ethical consideration in this study is critical in ensuring that no harm comes from participants in the study. Participants in the study will have to understand that the study is voluntary.

During the study, the researcher ensured that participants did not receive threats, promises, coercion, or compensation in exchange for an individual to participate.

Participants were also encouraged to stop the interview if they felt uncomfortable answering questions during the interview process. As previously stated, no personal gains for either the researcher or participant occured during the interview process. Participants received the researcher's e-mail address and telephone contact number should they have any questions, concerns, or any other information that they would like to provide. According to Fouka and Mantzorou (2011), collecting a signed informed consent form from participants is a significant ethical concern when conducting research. The informed consent form illustrates that the participants involved fully understand the purpose of the study. The study gained approval from the ethical review board to guarantee that the researcher was adhering to the IRB's ethical requirements to protect participants during the research.

Summary

Chapter 3 explained the purpose and goals of this study—to explore law enforcement officers' perceptions in combating cybercrime at the local level. This chapter also included the research design and rationale, the researcher's role, and methodology to test the research questions. Additionally, the recruitment and sampling method as well as the selection process for participants in this study were discussed. A total of 15 law enforcment officers throughout the state of Texas were recruited for participation in this study; however, only nine were needed to attain data saturation. Finally, this chapter also discussed the issues of trustworthiness and ethical considerations. Chapter 4 included a summary of the results of the methodology and an in-depth description of participants' interview responses.

Chapter 4: Results

The purpose of this study was to explore law enforcement officers' perceptions in combating cybercrime at the local level. This qualitative case study focused on the perceptions and beliefs of nine law enforcement officers in Texas regarding cybercrime preparedness within law enforcement agencies locally and limitations, if any, that hinder cybercrime investigations by officers at the local level. The research questions addressed how law enforcement officers describe their agencies' preparedness to fight cybercrime and what factors limit them from responding to computer-related incidents. The collection of data came through in-depth, semistructured interviews that featured 21 interview questions that helped to explore the perceptions and beliefs of the law enforcement officers concerning (a) policing cybercrimes, (b) cybercrime awareness, (c) cybercrime training, (d) limitation to responding to cybercrimes. This chapter describes the research setting, demographics, data collection procedures, the data analysis procedures, the trustworthiness in the study, and the study results.

Research Setting

The settings for data collection varied based on the availability of each participant in the study. Three participants felt comfortable in a quiet meeting room in a restaurant. However, with video conferencing platforms, such as Zoom available to the participants, some were not authorized by their respective law enforcement agencies to have such software installed on their work computers for security reasons. Due to constraints related to travel and time, five participants were interviewed over phone. In addition, one participant responded to the interview via Facetime, as they were on vacation and lacked

access to a laptop or computer. Before each interview, participants received emails with the informed consent form for review. Each participant consented by sending " I agree" via email before beginning the interview. One of the disadvantages of not interviewing six participants face-to-face was the inability to observe body language or facial expressions from the interview questions and the responses provided.

Participant Demographics

Each participant in the study was a certified law enforcement officer with at least 5 years of law enforcement experience who had direct knowledge of responding to crimes at the local level. The actual time employed as a law enforcement officer ranged from 10.5 to 30 years of service in the law enforcement field. Each participant rank ranged from assistance chief, senior sergeant (General Schedule 13), lieutenant, detective, sergeant, and school resource officer. The participant sample had a diverse group of law enforcement officers that consisted of four African American, three Hispanic, and two Caucasian officers, all of whom were male.

Data Collection

Upon receiving approval from the Walden University Institutional Review Board (IRB; approval #06-28-21-0749688), five law enforcement agencies were contacted and asked to provided research recruitment flyers to interested officers in each department via email. However, the five law enforcement agencies did not send the research recruitment flyers to the officers due to the lack of buy-in to the study and its relevance to the day-to-day operations of the law enforcement officers. Obtaining willing participants for this study posed some challenges, which led to an expanded search on social media for

interested participants that met the criteria for the study. Purposeful sampling was the approach applied in collecting participants for the study. In addition, other methods occurred to obtain participants for the study, including cold calling, emailing, and snowball sampling.

Although the five law enforcement agencies declined to send out recruitment correspondence, two participants for the study came from cold calls, and the other seven came from snowballing method. The targeted number for the sample size was 15; however, only nine law enforcement officers responded and agreed to participate in the study who met the criteria. A total of three other participants initially expressed interest in participating in the study but did not complete the process.

The data collection process for the participants was a semistructured interview format that allowed the participants the opportunity to provide in-depth responses. The research instrument applied in the study was researcher-made, which consisted of 21 semistructured interview questions, which were reviewed and approved by three subject matter experts. The semistructured interview format allowed me to expound on participants' responses that needed more clarification. The participants' perceptions and beliefs were vital as they served as a mechanism to validate their responses during the data collection process.

Participants in the study consented to have their interviews recorded for clarification purposes during the transcription and analysis phase with an electronic recording device. Participants' interviews took place face-to-face and by telephone ranging from 25 to 45 minutes. Upon completing each interview, each participant

received a copy of their transcripts to review for accuracy. Participants were also assigned numbers to maintain confidentiality during the transcription and coding phase of the study.

Data Analysis

The data analysis for this study was guided by the primary research questions: (a) How do law enforcement officers' that respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally? (b) What factors, if any, limit law enforcement officers' from responding to computer-related incidents locally? After completing and reviewing all the interview transcripts for accuracy, I analyzed and entered the participants' responses into NVivo 12 data analysis software. The software transcribed the data verbatim, which helped examine word similarities to identify themes. NVivo also provided word frequencies needed to discover the study's themes based on the data collected from the nine interviews (see Figure 1).

Figure 1

Word Cloud

Trustworthiness

Trustworthiness in qualitative research establishes the authenticity of the research outcome through the truthfulness of the research findings (Cypress, 2017) and is measured by four areas: (a) credibility, (b) transferability, (d) dependability, and (e) confirmability. Credibility was established at the beginning and throughout the data collection process in this study. Participants' identifiers were removed during the data collection and analysis phase of the study. Member checking is another method used to strengthen data credibility (Aminet al., 2020). Discussions of my personal and professional experiences related to law enforcement responses to cybercrimes were also limited to minimize biases in how participants responded. Follow-up questions were also asked of the participants to understand some responses or unanticipated responses. Additionally, each participant in the study received a copy of the transcripts within a week of the interviews. The participants were allowed to revise information obtained during the interview process and recontact the researcher to correct or clarify the information.

Transferability

In transferability, the reader decides whether the findings are transferable to their setting, based on the thick description provided by the researcher (Korstjens & Moser, 2017). Researchers in a qualitative study use transferability to help bridge the gap between the participant and the researcher (Ospina et al., 2017). In addition, the results from this study are transferable to the degree that the findings can apply to future studies outside the participant's law enforcement organizations. Lastly, purposive sampling

helped obtain detailed, relevant, and sufficient information that captured themes to identify the potential phenomenon in understanding law enforcement officers' opinions regarding whether law enforcement agencies can investigate cybercrimes locally.

Dependability

Dependability is essential in trustworthiness because it allows other researchers to reach a consistent and repeatable conclusion in the study findings. Dependability is a process that helps the researcher verify that their findings are consistent with the data they collected. If collected data in a study are consistent and answers the research question, dependability in the study is established (Ravitch & Carl, 2016). Dependability ensures that the researcher is not careless or that there was no missing information from the final research study. I carefully reviewed the transcripts and notes numerous times to increase the data's accuracy and minimize or remove mistakes as needed. Participants were asked the same questions from the interview protocol, but some were not necessarily in the same order as the protocol.

Confirmability

Confirmability is used alongside trustworthiness to ensure that the data gathered by the researcher is the participants' narratives rather than the researcher's narrative (Kyngäs et al., 2020). In addition, it verifies that others can verify any biases of the researcher. Confirmability was established in the study by intentionally selecting participants in various law enforcement agencies using the audit trail technique to interpret categories, codes, and themes.

Study Results

This section contains a summary of the findings from the themes that emerged in the interview data. The strengthening of the themes comes from the participants' key points and different opinions on the same topic. The two research questions for this study were: (a) How do law enforcement officers who respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally? and (b) What factors, if any, limit law enforcement officers from responding to computer-related incidents locally?

When initially coding the data from the interview transcriptions, a 1-week period passed to review the data for a second time to determine if the results differed from the previous data collected. However, the results from the data review did not change after reviewing the data multiple times. Several areas of interest were formed in NVivo 12 software helped answer the research questions in the research study. Four main themes emerge while coding and comparing data in NVivo 12: (a) policing cybercrimes, (b) cybercrime awareness, (c) cybercrime training, (d) limitation to responding to cybercrimes. The four themes were broken down into subthemes and analyzed, reported, and supported by the study's responses.

Responses to the Research Questions

The interview questions were initially grouped into two themes (a) law enforcement experiences and (b) limitations to respond to cybercrimes. However, after conducting an in-depth analysis, the two themes expanded into sub-themes that expressed the participants' opinions. Therefore Table 1 depicts the pairing of interview questions

created out of the two initial themes and sub-themes. As a result, many of the interview questions overlapped several of the themes presented in the study.

Table 1

Sub-Themes from Initial Interview Responses

Themes	Participants	Interview Questions
Policing Cyber Crimes	9	1,2,3,4,4,5,6,8,9,10,11,13,14, 20 and 21
Cybercrime Awareness	9	7, 8, and 12
Cybercrime Training	9	15,16, and 18
Limitation to Responding to Cybercrimes	9	17, 18,19,

Law Enforcement Officer Experiences

Participants displayed a wide variety of experiences and roles within their law enforcement agencies. Potential roles included assistance chief, senior sergeant (General Schedule 13), lieutenant, detective, sergeant, and school resource officer. In addition, the educational backgrounds of the participants varied. Over half of the participants had a bachelor's degree, two had their associate degree, and two had a high school diploma. In addition, three participants acknowledged that they had investigated several computer-related offenses at the local level that ranged from romance fraud to real estate fraud. Participants were also diverse in their years of service, with two participants having over 30 years of service, three participants had over 20 years of service, and four participants had over ten years of service as law enforcement officers.

Cybercrime Protocols

Questions 6, 7, 9, 10, 11, 12, 13, 14, and 19 related to officers responding to computer-related incidents locally. Five out of nine participants agreed that law enforcement agencies should have a limited role in investigating cybercrimes at the local level. All five participants also noted that law enforcement officers should take the initial report and channel the information to an agency that handles cybercrime investigations, such as cybercrime units within a law enforcement agency or federal agencies that handle cybercrime responses. Two participants disagreed that officers should have a limited role and believed that it is not much that law enforcement agencies can do in responding to cybercrimes at the local level. In addition, the last two participants felt that law enforcement's role in responding to cybercrimes should include evidence collection. However, all nine of the participants provided an understanding of cybercrime and its impact on society.

The following passages are direct quotes from participants relative to law enforcement officers' responses to computer-related incidents:

LO N5: "I say their role should be just with any other crime, be a point of reference for those people reporting? Your local police department is just your first basis to me as a layman person that can report that something has happened."

LO N7: "I see that law enforcement should really be taking the initial reports and preparing as much information at the local level, and then it would be nice if they would either submit to a repository where maybe the feds would take control or take over. Usually, in some of the bigger, high-profile cases."

LO N8: “We should have a role, but it should be a very limited role. The reason I say very limited role is because the local municipalities do not have the resources, say as the DOD or the Department of Defense, to be effective in fighting it.”

Participants also responded about the type of cybercrimes that police departments receive the most related to cybercrimes locally, and four of the participants identified credit card fraud as the primary type of offense reported by victims. In addition, three participants noted that people taking advantage of the elderly are other types of online crimes reported by victims, followed by two participants identifying online bullying as a type of cybercrime reported by victims to police departments. Finally, when asked about the protocols that officers take when citizens and businesses report cybercrimes, several participants responded by noting,

LO1: “They take the report, they put it in the drawer, and it goes no farther.”

LO4: “A lot of times we'll respond to these types of incidents. We don’t have a lot of information, and a lot of times, the victims don't have a lot of information about what occurred.”

LO8: “You get so many cases, you don't have the time to put in for each case, that's why they put it on their victims to go and gather their own evidence and whatever it is, they may need.”

Many of the participants did confirm that victims who report cybercrimes do not know what to do after becoming a victim, in which a law enforcement officer advises the victims to contact their banks as the first line of defense in recovering any funds stolen from online fraud.

Cybercrime Seriousness

When examining the participants' perceptions regarding the seriousness of cybercrime at the local level, participants provided various responses to Questions 15, 16, and 18. Eight out of nine participants agreed that cybercrime is a serious matter at all levels of law enforcement, but one participant disagreed that law enforcement agencies are not taking cybercrime seriously at the local level. The participant stated, "It is not taken seriously because it's a nonviolent offense. They are not going to prosecute a computer crime, so it is not taken seriously." The following excerpts describe some other comments by participants as it relates to the seriousness of cybercrimes.

LO1: "I think it's taken very seriously. Officers that I have had personal discussions with about it, they're frustrated because their hands are tied, and their ability to cope with it."

LO5: "Each year cybercrime grows."

LO6: "It's not that cybercrime is not taken seriously. It is what cybercrime is being done." So, say you report that your child was talking online, and you believe your child has gone away with a grown person. That call will have an elevated response to law enforcement, instead of hey, I think somebody stole my identity."

Agencies Responsible for Investigating Cybercrimes

Regarding the limitations law enforcement agencies face in responding to cybercrimes, six participants concluded that the responsible agency to investigate cybercrimes should be the FBI. The six participants had a resounding response that

emphasized that law enforcement agencies are the first to respond to a crime. From there, they disseminate information to the appropriate agencies. One of the participants stated, “the local law enforcement is just a stepping stone for something bigger. We can filter as your local PD.” However, the remaining three participants believed that a cybercrime unit is necessary at the local or regional level. The cybercrime unit could help reduce calls that law enforcement agencies receive regarding computer-related incidents.

All nine of the participants did agree that the FBI will not respond to minor computer crimes such as identity theft, cybercrime scams, or social media disputes at the local level. The participants agreed that the FBI would only respond to crimes committed over the Internet are terrorism, computer intrusion that causes millions of dollars in damages, or a significant offense across jurisdictional lines. More importantly, participants noted that law enforcements’ objectives and missions are generated by what society deems as serious crimes, such as robbery and murder, as top priorities for law enforcement to pursue. The participants suggested that cybercrimes are not a top priority for law enforcement agencies. The participants believed that law enforcement agencies attempt to handle the physical crimes within their jurisdiction that they can control instead of computer-related crimes they cannot see or track.

Future Policing

The dynamics of policing are forever changing, and law enforcement agencies across the criminal justice platform are proactive in staying abreast of the new crimes committed by criminals in the new digital age of technology. Question 21 will depict participants' views on law enforcement officers' role in policing cybercrime in the future.

Optimistically, all participants agreed that law enforcement agencies at the local level would play a significant part in the fight against cybercrime in the future. However, many of the participants did believe law enforcement roles in the future will focus on getting enough training for officers to become familiar with cybercrimes. Ultimately the participants suggested that law enforcement agencies depend primarily on the FBI to respond and investigate cybercrimes. The following passages are direct quotes from participants relevant to the future of policing at the local level.

LO1: “I see them stuck in the same rut that they're in right now because I don't think it's goanna move fast enough.”

LO4: “I think we're goanna have a more prominent role.”

LO6: “At the local level, I don't ever think we'll reach the level of maybe like the FBI, Homeland Security.”

Cybercrime Prevention

The participants provided their perspectives on the roles officers should take in preventing and investigating cybercrimes and how to improve the effectiveness of combating cybercrime at the local level, which questions eight and 20 covered. When asked about officers' roles in preventing and investigating cybercrimes, seven of the participants agreed that cybercrime is hard to avoid. However two of the participants believed that being proactive is the solution to officers preventing and investigating cybercrimes locally. All participants noted that law enforcement agencies should provide educational awareness programs that would help educate the public regarding computer-related threats. For example, the participants felt that if the public were provided

education on the various dangers of being online, it would help the public understand what to look for regarding online scams that helped protect individuals from becoming cybercrime victims. The following excerpts describe some of the comments from the participants related to officers' responses in preventing and investigating cybercrimes.

LO1: “There's no way to prevent it at a local level.”

LO4: “It’s a difficult task for officers.”

LO6: “We can educate the individual when we come into contact with them on how to prevent you or your kids or whoever of being victims.”

Cybercrime Training

Officer Training

Participants also had mixed reviews when asked about the types of cybercrime training offered at their local law enforcement agency. Six participants agreed that there is some form of cybercrime training offered online. However, one participant stated, “the training that’s available out there to the police is not adequate. It might give you a few tips you can use, but it stops there.” The other three participants acknowledged that they had received little to no in-service training for cybercrime in their respective agencies. One participant responded to the lack of training by stating, “if you want to do it, you can do it. It is not really a big push for cybercrime as far as training.”

Three participants felt that they had some comfort in their ability to investigate cybercrimes if needed. The other six participants reported that they did not have any confidence in their ability to respond to computer-related crimes. One of the participants

responded by stating, “I have zero training in cyber anything. They usually tell me what to take.”

The following excerpts describe some additional comments from the participants related to the participant's training and confidence level regarding cybercrime training.

LO3: “I have a certain level of knowledge with it. I feel comfortable.”

LO4: “I'm familiar with a lot of resources, as far as investigation standpoint, that a lot of patrol officers are not familiar with. I have relationships with federal agencies.”

LO9: “I don't have the training.”

Over half of the participants acknowledged that specialized units usually get the cyber training needed to investigate cybercrimes. In contrast, local beat officers get additional training related to the physical crimes they respond to daily. Lastly, six participants believed that officers do not have the experience to investigate cybercrimes, with one of the participants stating, “We need more experience because it is occurring.” The final three participants felt that more resources are needed to combat computer-related offenses because police lack the funding to conduct additional investigations. However, all participants noted that more cyber training is necessary for officers to respond to incidents better.

Improving Cybercrime Effectiveness

Participants also provided their perceptions of how law enforcement agencies can improve the overall effectiveness of combating cybercrime locally. Thus, eight of the nine participants noted that training and education awareness are two areas of concern that law enforcement agencies should improve. In addition, one of the participants

believed that creating a cybercrime task force would help with improving cybercrime effectiveness at the local level. Finally, many of the participants did agree that officer training is a significant contributor to enhancing the efficacy within law enforcement agencies locally. Below are direct comments from participants regarding law enforcement's effectiveness in combating cybercrime at the local level.

LO2: You've got to train your officers on what to do.

LO5: Even if it's just minimal skill training, you've got to send them out there with the ability and the knowledge to feel secure.

LO6: Education

Likewise, all participants agreed that some form of education should take place internally and externally concerning the dangers of cybercrime. One participant stated, "If you take out one component, which is the victim from the equation, then you don't have a crime." The participants understand the power of education, and all believed that law enforcement agencies and the public need more education on how to handle cybercrimes locally. Participants also concluded that some of the challenges officers face in obtaining cybercrime training are based on the community's needs.

Limitations to Responding to Cybercrimes

Policing Cybercrimes

Questions 17 explain participant's outlook on law enforcement officers' limitations to responding to cybercrimes and what law enforcement agency should be responsible for investigating cybercrimes. Participants responded with mixed responses related to law enforcement officers' limitations in responding to computer-related crimes.

Eight participants believed that law enforcement agencies' limitation to responding to cybercrime is related to the number of resources and training that law enforcement agencies fail to offer at the local level. The other participant believed that politics is a reason for law enforcement agencies not responding to cybercrimes. The participant stated, “Congress, and the people and powers that may be, are going to have to put something together in the system to say, hey, when law enforcement needs this, there is not a no from the powers to be.”

Although eight of the nine participants believed that law enforcement agencies lack the needed resources to police cybercrime at the local level, many participants agreed that responding to cybercrimes is challenging for law enforcement at the local level. For this reason, participants emphasized that the lack of resources was a limitation that prohibited law enforcement agencies from making positive steps in investigating cybercrimes locally. Participants' comments below represent limitations that officers face in responding to computer-related crimes at the local level.

LO4: “We don't always have the resources. Cybercrime is a crime that takes a much longer investigation because it's very difficult to determine who is the suspect.”

LO8: “It takes so much time to work. You're taking manpower away from your patrol element of the departments, which is the most vital asset to a police officer, which is the patrol element.”

LO9: “We cannot play Superman because there's so much crime.”

Politics in Policing

Law enforcement agencies protect the community based on the type of crimes committed within the area. Eight of the nine participants acknowledged that politics play a factor in how law enforcement agencies spend their funding and resources on the community's immediate needs. For example, one participant stated, “There's a lot of discouraging actions that are taken by the judicial system and the DA's office.” The second participant stated, “I think any issue now, in law enforcement is going to be a political issue.” The third participant noted that “If the local entities do not want it, then it is not going to happen.” A final participant noted, “They are going to spend most of their money on dealing with family violence crimes, and not cybercrimes.” A small portion of participants noted that politics has a significant role in the missions and objectives of local law enforcement agencies.

Motivation

Participants received a follow-up question related to officers' motivation in investigating cybercrimes, where five out of nine participants agreed that officers really would like the opportunity to investigate cybercrimes. However, the five participants believed that the lack of support from law enforcement agencies was due to not having the staffing or funding to support a new cybercrime initiative that would require additional time and resources to investigate. Although two participants indicated that law enforcment officers were motivated to respond to cybercrimes; four of the participants disagreed about what motivates officers regarding investigating cybercrimes. One participant concluded that law enforcement officers are not motivated to investigate

cybercrimes due to burnout from working so many cases by stating, “You do need the help because you work your ass off.” Moreover, three other participants believed that responding to cybercrimes would take away from officers responding to physical crimes. These three participants included that if officers spend most of their time investigating computer-related offensives, it will reduce the number of officers patrolling the streets. The following excerpts describe some of the comments from the participants as it relates to officers’ motivation in responding to cybercrimes.

LO2: “I don't think they feel secure, doing it. If you don't feel secure doing something, you're not going to throw your all into it.”

LO3: “You have officers that have been in it for 25 years, and he may be doing the last part of his tenure where he is like, ‘I am not trying to do this, leave this for the youngsters.’”

LO6: “As a local beat officer, I don’t have the time to investigate cybercrimes, that’s the investigations job to do that.”

LO8: “Why are we wasting our time while we put forth this effort when it goes here, and they won't prosecute.”

Many of the participants did acknowledge that law enforcement agencies receive more calls regarding physical offensives than computer-related offensives, which was why cybercrimes were not investigated more by law enforcement agencies locally. For this reason, all nine participants acknowledged that funding and experience were top priorities for officers' motivation in not responding to cybercrimes locally.

Summary

This chapter focused on the analysis, coding, themes, and the results of the data collected from the nine participants during this study. The data included themes specific to two areas of interest. The themes that emerged from the study were law enforcement officers' response to cybercrime and law enforcement agencies' response to cybercrime. However, thematic coding helped gain a better connection from the collected data to produce common themes found in the study. Four themes emerged using thematic coding. The following themes emerged in the data analysis were: (a) policing cybercrimes, (b) cybercrime awareness, (c) cybercrime training, (d) limitation to responding to cybercrimes. The research question: How do law enforcement officers that respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally? was answered by the themes developed through the examination of the interview questions:

1. What roles do you believe local law enforcement agencies should play in responding to cybercrime?
2. What roles do you believe local law enforcement agencies should play in responding to cybercrime?
3. What do you think the roles should be for law enforcement officers in preventing and investigating cybercrimes at the local level?
4. What are the procedural steps taken by your law enforcement agency when investigating cybercrimes locally?

5. What role do you see law enforcement officers playing in policing cybercrime in the future at the local level?

The second research question: What factors, if any, limit law enforcement officers from responding to computer-related incidents locally? was answered by the themes developed through the examination of the interview questions:

1. What are some types of computer-related crimes typically investigated by law enforcement officers at the local level?
2. What current training opportunities and availability in cybercrime can officers take during in-service trainings?
3. In your opinion, what are the major constraints or limitations for law enforcement officers in responding to computer-related crimes at the local level?
4. Who do you believe should be primarily responsible for investigating cybercrime cases?

Participants in the study discussed the role of law enforcement officers responding to cybercrimes, where many agreed that cybercrime is difficult to police at the local level. The participants noted in their responses that law enforcement at the local level should have a limited role in investigating computer crimes. Many participants agreed that law enforcement agencies should take the initial police reports and pass the information to the FBI for investigation.

In addition, participants mentioned throughout several interview responses that law enforcement officers are not motivated to respond to computer-related incidents due

to the lack of training and knowledge that comes with investigations, along with the inability to physically capture the suspect due to the crimes committed online. Officer training in cybercrime was another response by participants that revealed the need for more cyber training to help officers better understand the process for investigating computer-related incidents and training.

More importantly, education awareness was a top issue that the participants believed was an essential factor that could help reduce cybercrimes. The participant responses outlined how law enforcement agencies could educate the public on becoming aware of the dangers of online threats. Although most participants noted that it is challenging to prevent cybercrimes, participants did agree that educating the public as much as possible is an excellent way to reduce computer crimes. Participants also noted that lack of funding and resources is another factor that limits law enforcement from responding to cybercrimes.

Lastly, participants had mixed responses regarding the direction of policing cybercrime in the future. Most of the participants agreed that cybercrime is a problem that needs attention; however, some participants believed that law enforcement at the local level should pass cybercrime cases to other agencies for investigation. The remaining participant's responses determined that cybercrime task forces are needed at the regional level to only respond to cybercrimes within a designated geographical local area. In closing, all participants acknowledge that local law enforcement agencies will play some type of role in combating cybercrime in the future. However, many participants believed that role will continue to be a limited role where law enforcement

agencies assist the FBI. Chapter 5 interprets the research findings, study limitations, recommendations, implications, and conclusion found in this study.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this study was to explore law enforcement officers' perceptions in combating cybercrime at the local level. A qualitative case study approach helped accomplish the study's research goals in investigating nine participants who worked in law enforcement agencies in Texas. The summarization of the nine interviews occurred in Chapter 4, which helped establish the study's themes. The themes were grouped and coded to best answer the research questions, which helped guide this study. This chapter provides the interpretations for the findings of this study, along with the study's limitations and recommendations developed from data analysis. This chapter ends with the study's conclusion.

Interpretation of Findings

After consolidating the initial themes and sub-themes found in Table 1, I analyzed the interview data themes by comparing the themes used in the literature review in Chapter 2. Several themes were common in the literature review and the findings; however, some themes were either present in one theme or absent from the other. As a result, the participants' responses contributed to the themes that were not present in the literature. Therefore, the four themes that emerged from the initial sub-themes found in table 1 were (a) policing cybercrime, (b) cybercrime training, (c) limitations to responding to cybercrimes, (d) future role in policing cybercrime.

Theme 1: Policing Cybercrime

The first theme for this study is policing cybercrime. The literature indicates law enforcement agencies' dependency on the FBI to investigate cybercrimes (Brunner,

2020). Similarly, participants repeatedly discussed the challenges that law enforcement agencies at the local level face when investigating cybercrimes and insisted that the responsibility to investigate cybercrimes should fall on the FBI. For example, participants in the study described difficulty in officers being able to respond to cybercrimes while acknowledging that officers' response to cybercrimes should include a limited role, which involves taking the initial report from the offense and passing the information off to an experienced agency for investigation. Participants believed that law enforcement agencies locally take cybercrimes seriously; however, they believed the FBI is responsible for investigating computer-related offenses. Much focus was not placed on the need for law enforcement officers to respond and investigate cybercrimes at the local level in the literature or interview data. Nevertheless, the need for the FBI to investigate cybercrimes was prominent in both the literature and the interview data.

Both data sources—the literature review and the participants in the study—discussed cybercrimes that law enforcement officers can and cannot investigate or solve (Macdonald, 2021). Thus, law enforcement agencies place a low priority on investigating cybercrimes (Burruss et al., 2019; Holt, 2019), which is a significant factor that impacts policing. The literature suggests the inclusion of these factors regarding what agency should be responsible for investigating cybercrimes. There was a consensus from both the data sources that cybercrime continues to grow and become a problem nationwide. The literature did not mention the need for law enforcement officers to provide cybercrime awareness to the public in reducing cybercrime victims within the community. However,

the participants did mention the need for law enforcement agencies to provide cybercrime awareness for community members.

Another finding in the research was the need for law enforcement agencies to understand the significance of providing cybercrime awareness programs to the community. For example, law enforcement agencies can educate community members of the dangers and ramifications of online activities by providing the public with the tools, information, and resources to protect themselves from being victimized by cybercriminals. In addition, cybercrime awareness programs offered by law enforcement agencies could provide community outreach training opportunities that can help expand the public awareness and crime prevention knowledge for community members. In this case, one participant stated, “We can educate the individual when we come into contact with them on how to prevent you or your kids or whoever of being victims.” Participants concluded that public education regarding cybercrime threats could reduce individuals from becoming cybercrime victims in the future, which would improve law enforcement effectiveness at the local level.

Theme 2: Cybercrime Training

Law enforcement agencies spend countless hours and funds each year to help ensure that their staff receives updates of what is going on in the agency. Participants all identified that up-to-date cybercrime training should be a priority in helping officers obtain more knowledge on prevention and investigation of cybercrimes. As one participant stateds, “the training that’s available out there to the police is not adequate. It might give you a few tips you can use, but it stops there.” Several of the participants

provided examples of the type of training they receive during in-service training that included new laws, revisions in the agency policy, procedures, rules, regulations, and any further technology improvements that officers can use in the apprehension of criminals.

Participants suggested that law enforcement at the federal and local levels are behind in technology and training to capture cybercriminals. Participants believed that there is no push for officers to take cybercrime training at the local level due to the need to respond to traditional crimes such as robbery and domestic violence that have precedent over offenses committed over the internet. The participants believed that more in-service training should include current cybercrime training that helps officers identify the basics of recognizing cybercrime threats other than just identifying what to look for in a suspicious email.

Both the literature and participants emphasized that officers receive more of a traditional approach than a cybercrime approach in their training, unfavorable to law enforcement agencies addressing the cybercrime landscape (Cunha et al.,2016). The literature suggests that law enforcement agencies focus more on traditional training than cybercrime training. Moreover, most participants lacked any serious cybercrime training to react to computer-related incidents if called. Thus, both the participants and the literature expressed the significance of training opportunities for law enforcement related to additional cybercrime training.

One finding in the research was that law enforcement agencies delegate cybercrime training to specialized units in an agency that investigates cybercrimes; however, at the same time, law enforcement agencies assign officers that patrol the

streets training related to crimes not committed online. Thus, the lack of cybercrime training adoption from law enforcement agencies could become a concern because it may inadvertently impact the abilities of law enforcement officers to respond to cybercrimes locally.

Theme 3: Limitations to Responding to Cybercrimes

Law enforcement agencies face many challenges in combating cybercrime locally. Half of the participants indicated that investigating cybercrimes has its limitations, and there is not much that law enforcement agencies can do to combat cybercrime. However, the main complaint from the participants was that law enforcement agencies lack the funding to investigate cybercrimes. With the lack of funding to investigate cybercrimes, law enforcement agencies find it challenging to track down cybercriminals who commit crimes over the internet.

The participants also concluded that there is too much crime for law enforcement agencies at the local level to investigate alone. One participant stated, “We cannot play Superman because there’s so much crime.” For the same reason, participants suggested that investigating cybercrimes takes away from the patrol element of law enforcement, which police officers are considered a vital part of fighting common crimes in the community.

Politics in policing was another point identified by participants as a limitation, with participants stating that politics played a significant role that limits officers from partaking in many cybercrime investigations. In this case, the participants stressed that law enforcement agencies’ budgets dictate how an agency functions, resulting in the

administration deciding the organization's priorities. There was a consensus from the participants that politics in policing also involves what the community wants. For example, if community members and organizations request law enforcement agencies to implement cybercrime units to reduce the number of cybercrimes locally, law enforcement administrators would create a local cybercrime unit or collaborate with other departments to minimize the cybercrime threats in the community.

Lastly, participants identified motivation as a limitation that reduces officers' ability to respond to cybercrimes. Five participants indicated that officers' lack of motivation in responding to cybercrimes was due to staffing deficiencies and funding. For instance, seven participants agreed that law enforcement agencies have many interested individuals who would like to respond to cybercrimes but cannot investigate cybercrimes because law enforcement agencies do not have enough manpower to replace the officers. But officers are less than likely willing to investigate cybercrimes for interested officers because of the agency's inability to move around the funding to support a cybercrime initiative. In addition, officer burnout was another reason participants mentioned officers' lack of motivation to investigate cybercrimes. Nevertheless, participants did note that cybercrime investigations take many staffing hours, including obtaining search warrants for every piece of digital evidence collected at the crime scene, which can become time-consuming and costly. Participants provided scenarios where an investigator takes on a cybercrime case that may take anywhere from 1-3 months to conduct interviews, collect warrants, and write reports, only to find that the court system does not prosecute the criminal case. The consensus from the participants

was that it is challenging to capture a cybercrime criminal. However, it is even more challenging to prosecute a cybercriminal: “As a local beat officer, I don’t have the time to investigate cybercrimes; that’s the investigations job to do that.”

Participants added that officers lack motivation because of the court system’s inability to prosecute criminals that commit crimes over the internet. Despite the time and manpower-hours it takes to investigate a cybercrime that never goes to trial, officers are unmotivated to investigate computer-related incidents. The findings suggested that law enforcement agencies have many law enforcement officers willing to investigate cybercrime but are delayed in helping combat cybercrime at the local level mainly because of funding that provides the additional resources needed to investigate computer crimes. Law enforcement agencies allocate funding to criminal elements that are common threats to the community instead of shifting funding to combat cybercrime offenses that are challenging to prosecute.

Theme 4: Future Role in Policing Cybercrime

Every participant discussed the emergence of cybercrimes and their potential impact on law enforcement agencies at the local level in the future. Most participants agreed that in the future, law enforcement should continue to provide a limited role in cybercrime investigations that requires officers to take down the information and pass it along. In this situation, the participants based their responses on the challenges officers face when attempting to help cybercrime victims recover items stolen online. For this reason, the participants felt they would be doing cybercrime victims injustice by investigating cybercrime incidents in which they had little experience.

Additionally, the same participants believed that law enforcement is behind in investigating cybercrimes, as one of the participants responded by stating, “I see them stuck in the same rut that they are in right now because I don’t think it’s; gonna move fast enough.” Participants concluded that the ongoing cybercrime issues would only continue well into the future.

For this reason, half of the participants acknowledged that creating a cybercrime task force of federal and local law enforcement officers working together could reduce computer crimes in the future. The participants believed that local and federal officers’ working together would be a significant move for law enforcement in general. The participants also stressed that multiple cybercrime units within major metropolitical areas should be considered in the future, which could help reduce the work caseloads for investigators. In closing, all the participants agreed that as cybercrime threats increase, law enforcement at the local level will play a prominent role. Although many of the participants had mixed responses on the roles law enforcement agencies will play in responding to cybercrimes in the future, the participants were aware that the use of technology is changing how policing is conducted by officers.

Hence, the need for law enforcement officers to play a significant role in cybercrime investigation and the federal agency was prominent in the literature but less so in the interview data. However, participants had mixed consensus on what role law enforcement should play in policing cybercrimes in the future. The findings suggested that law enforcement officers believed that creating multiple cybercrime units in different areas throughout metropolitan would help reduce cybercrimes nationwide and at the local

level. Lastly, the findings indicated a need to develop additional cybercrime units where law enforcement agencies can work together across jurisdictions to solve cybercrimes, which could reduce the involvement of local law enforcement officers in responding to computer-related incidents. However, many participants stressed that law enforcement would have a limited role in investigating cybercrimes in the future.

Theoretical Framework

Lawrence and Lorsch's contingency theory was the first conceptual framework for the study. The structural contingency theory suggests that when contingencies change in an environment, organizations adjust their strategy to respond to the area of concern. (Donaldson, 2001). For example, contingency theory relates to law enforcement agencies policing cybercrime at the local level. However, law enforcement agencies will only devote additional resources to policing cybercrime as the threat becomes more prevalent and a concern in the community. In this case, local law enforcement agencies had fewer computer-related incidents reported than the standard calls related to a robbery or individual disputes. Therefore, the contingency theory could indicate that cybercrimes are not investigated by law enforcement agenices, because of the lack computer crimes reported by citizens in the community.

Porter and Lawler's theory of motivation was the second conceptual framework used in the study. Porter and Lawler's theory of motivation suggests that rewards and performance could lead to individuals' satisfaction in the workplace (Kesselman et al., 1974). Additionally, Porter and Lawler's theory of motion includes intrinsic and extrinsic motivation that motivates individuals to complete a task on the job. For this reason,

participants in the study were intrinsically motivated to investigate cybercrimes if it was a required duty to take criminals off the streets. Futhermore, the participants' satisfaction was sparked by providing information to citizens that would prevent them or their family members from becoming cybercrime victims in the future.

Limitations of the Study

This current study provides answers to both research questions; however, several limitations were worthy of discussion. The first limitation in the study was that not all law enforcement agencies who received the invitation to participate accepted the invitation. Although the five law enforcement agencies selected initially did not participate in the study, interested volunteers could have added points of view to the findings that could have been valuable to the study. Secondly, the sample size for the participants in this study was another limitation viewed as a weakness, despite the set standards needed to meet data saturation within a qualitative research study. In contrast, using quantitative research could produce larger sample sizes that are generalized.

Third, the finding from this study is limited to the geographical area of Texas. If the same study occurred in other law enforcement agencies within the United States, the results could produce different results. As a result, the interviews were limited to law enforcement agencies in Texas. A nationwide research study could provide a comparative analysis of law enforcement agencies in other states that could encounter similar concerns and have successfully addressed them through collaborations with other law enforcement agencies.

Lastly, not being able to interview six of the participants face-to-face at a location was a limitation in the study. Face-to-face interaction with the six participants could have captured the participants' body language and facial expressions, leading to more questioning. However, capturing the body language and facial expression during questioning could have indicated the participants comfort or discomfort with the questions asked during the interview.

Recommendations

The results from the study have produced several recommendations for future research regarding this study. First, research regarding officers perceptions of responding to cybercrimes at the local level is limited and virtually unexplored. Second, this study can contribute to the current body of literature in various areas of law enforcement, which could open opportunities for further research in helping explore law enforcement officers' perceptions of responding to cybercrimes locally. For this reason, the first recommendation includes conducting studies specific to law enforcement administrators to understand their perspectives regarding what role, if any will law enforcement play at the local level regarding cybercrime response. Also, this study was limited to only law enforcement officers not familiar with cybercrime investigations.

Future studies could include computer crime detectives within a law enforcement agency establishing their perceptions regarding law enforcement role in responding to cybercrime at the local level. This qualitative research approach provides a deep and rich understanding of the participants perceptions and beliefs for this study. However, a future study could include a quantitative research approach indicating law enforcement

agencies' commitment to responding to cybercrimes at the local level. Finally, more research is needed to understand what the federal government is doing to help state and local governments combat cybercrime.

Implications

This study can help create positive social change by raising awareness of law enforcement officers' challenges in combating cybercrimes locally. In addition, the participants had the opportunity to express their perceptions regarding combating cybercrimes at the local level. Moreover, this study also allowed the participants to acknowledge their current level of experience investigating computer crimes and their personal beliefs regarding law enforcement agencies role in cybercrime investigations. Thus, this study's findings have the potential to create positive social change for law enforcement agencies seeking in-depth contextual information regarding law enforcement officers' perceptions of responding to cybercrimes at the local level.

From the point of view of the law enforcement agencies at the local level, this study could provide cybercrime training and funding to law enforcement personnel to combat cybercrimes. In addition, many of the participants reported that cybercrime training at the local level was minimal because of budget constraints within an agency. Also, the participants noted the need to create multiple cybercrime units located throughout all major cities in the United States. As a result, this study could provide law enforcement agencies with the knowledge of what police officers are looking for from an agency to respond to computer-related incidents that are solvable by officers.

From a community standpoint, law enforcement agencies that provide cybercrime awareness to community members could help bridge the community and law enforcement gap, which agencies may need to rely on one day. Citizens understand that law enforcement agencies respond to various crimes that need immediate responses. However, if community members were aware of the dangers of online activity, cybercrime reduction could occur. The information provided in this study shows that educational awareness for community members could educate the public on what to look for in cyber threats and preventative measures to take from becoming a cybercrime victim. Additionally, this study discovered that many law enforcement officers believe that public education awareness is one of the first tools law enforcement agencies' can use in reducing cybercrimes locally.

Participants' in the study revealed an unexpected sub-theme, which is politics in policing. This study implies that law enforcement agencies would improve their effectiveness in responding to computer-related offenses if law enforcement administrators, political leaders, and community members recommend the need for more law enforcement involvement related to responding to cybercrimes. Further, this study would teach law enforcement agencies' that the negative aspects of not being prepared to combat cybercrime locally far outweigh the costs of providing the funding and resources necessary for officers' to assist in investigating cybercrimes. The participant interviews provided new and unique insight into the perceptions of officers' responding to cybercrime at the local level. The study displayed the participants' passion and commitment to providing safety and security to the citizens and communities they serve.

The potential impact for positive social change in this study could benefit other law enforcement agencies' nationwide.

Conclusion

Almost everything that organizations and individual citizens do today revolves around using digital devices connected to the Internet, which has become a global concern for law enforcement due to the uptick of cybercrimes. Local law enforcement agencies play a significant role in the fight against cybercrime that local governments and communities should acknowledge as a critical need throughout the nation. However, law enforcement lags in determining local police departments' roles and responsibilities in combating cybercrime as technology advances. This study on law enforcement officers perception in responding to cybercrime at the local level revealed the need to increase law enforcement training and awareness regarding the current state of knowledge that officers possess in responding to computer-related offenses. Participants in the study openly acknowledged the need for up-to-date training as it relates to understanding cybercrime. However, it is also clear that law enforcement officers receive limited training regarding cybercrime due to focusing on physical incidents such as violence or violations committed by criminals. In addition, the participants acknowledged that law enforcement training is geared more towards the frequent crimes in the community. This study also revealed the need for local law enforcement agencies to create educational programs that educate the community on the dangers of online activity that could help reduce the number of cybercrime victims.

This study also focused on the behaviors of the participants regarding responding to cybercrimes. Participants indicated that law enforcement agencies take cybercrime seriously; however, cybercrimes are not a high priority for law enforcement at the local level. Participants also provided challenges that local law enforcement agencies face in cybercrime investigations locally. Participants acknowledged that responding to cybercrime discourages officers because the cases are time-consuming, locating the suspect is difficult, prosecuting the suspect is difficult, lack of funding and the responsibility for investigating cybercrimes should fall on the FBI. More importantly, all nine participants agreed that law enforcement agencies lack the experience necessary to investigate or respond to cybercrimes, which is why half of the participants determined that law enforcement should have a limited role in cybercrime investigations.

The research also included the roles that law enforcement will play in responding to cybercrimes in the future. Half of the participants strongly suggested that law enforcement locally will play a prominent role in cybercrime investigations in the future. For this reason, the participants believe that it is vital for law enforcement to maintain a certain level of preparedness to perform their duties effectively. Hence, three participants suggested that law enforcement agencies and the powers to be should create multiple cybercrime units surrounding major metropolitan cities. Three other participants believed that responding to cybercrimes would take away from officers responses to criminal offenses that the community needed officers to investigate.

The final three participants indicated that law enforcement would continue to stay in the same position and face uphill challenges that consist of lack of training, lack of

manpower, and lack of support from government agencies in the future. Although society has become increasingly dependent on using digital devices for personal and business use online, cyber threats have also increased. As a result, cybercrimes are not a core competency for law enforcement based on the collected data from interviews and the literature review.

The results from this study helped fill the gap in the literature regarding the unknown perceptions of law enforcement officers responding to cybercrimes at the local level. Additionally, the findings could have significant implications for future research and positive social change related to officers responding to cybercrime at the local level of law enforcement. Finally, the results from this research study answered the research questions concerning law enforcement officers' perceptions of combating cybercrime at the local level.

In conclusion, the data for this study revealed that law enforcement officers that respond to traditional crimes describe law enforcement agencies preparedness to fight cybercrime locally as a difficult task to accomplish. The participants overall belief is that a department or agency with the experience and resources to investigate cybercrimes should conduct the investigations; therefore, ruling out patrol officers cybercrime involvement due to the lack of training and knowledge needed to perform investigations. In addition, there were serval other factors that participants acknowledged in the research study that limited officers from responding to computer-related incidents locally, including budget concerns, politics, training, and the time it takes to investigate a cybercrime at the local level.

As cybercrime becomes more prominent in the future, law enforcement agencies could provide additional assistance to federal agencies to combat cybercrimes at the local level. Therefore, this research study could have a far-reaching implication for positive social change in the future regarding how law enforcement agencies respond to cybercrimes at the local level.

References

Accenture Security & Ponemon Institute. (2019). *Ninth annual cost of cybercrime study: Unlocking the value of improved cybersecurity protection*. https://www.accenture.com/_acnmedia/PDF-99/Accenture-Cost-Cyber-Crime-Infographic.pdf

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2019). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Crime and Society*, 91–109. https://doi.org/10.4324/9781351207430-7

Aleem, A. (2019). Treading water: Why organisations are making no progress on cyber security. *Network Security*, *2019*(11), 15–18. https://doi.org/10.1016/s1353-4858(19)30133-3

Amin, M. E. K., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in Social and Administrative Pharmacy*. https://doi.org/10.1016/j.sapharm.2020.02.005

An, J., & Kim, H.-W. (2018). A data analytics approach to the cybercrime underground economy. *IEEE Access*, *6*, 26636–26652. https://doi.org/10.1109/access.2018.2831667

Arghandeh, R., von Meier, A., Mehrmanesh, L., & Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, *58*, 1060–1069. https://doi.org/10.1016/j.rser.2015.12.193

Ashiq, M., Rehman, S. U., & Mujtaba, G. (2020). Future challenges and emerging role of academic libraries in Pakistan: A phenomenology approach. *Information Development*, *37*(1), 158–173. https://doi.org/10.1177/0266666919897410

Bachmann, M. (2008). The investigation, prosecution, and defense of a computer-related crime. *International Criminal Justice Review*, *18*(2), 246–247.

Bayard, E. E. (2019). The rise of cybercrime and the need for state cybersecurity. *Rutgers Computer & Technology Law Journal*, *45*(2), 69.

Belshaw, S. H. (2019). Investigating the new criminal neighborhood: The need for dark web education for law enforcement personnel. *International Journal of Information Security and Cybercrime*, *8*(2), 27–38. https://doi.org/10.19107/ijisc.2019.02.03

Berghel, H. (2017). Oh, what a tangled web: Russian hacking, fake news, and the 2016 US presidential election. *Computer*, *50*(9), 87–91. https://doi.org/10.1109/mc.2017.3571054

Bergmann, M., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727

Bidgoli, M., Knijnenburg, B. P., Grossklags, J., & Wardman, B. (2019). *Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting*. https://www.in.tum.de/fileadmin/w00bws/cybertrust/papers/2019-eCrime-Bidgoli.pdf

Black, A., Lumsden, K., & Hadlington, L. (2019). “Why don’t you block them?” police officers’ constructions of the ideal victim when responding to reports of interpersonal cybercrime. *Online Othering*, 355–378. https://doi.org/10.1007/978-3-030-12633-9_15

Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. *Computer Fraud & Security*, *2018*(11), 8–10. https://doi.org/10.1016/s1361-3723(18)30108-8

Bond, E., & Tyrrell, K. (2018). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence*, *36*, 5–6. https://doi.org/10.1177/0886260518760011

Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2019). Policing fraud in England and Wales: Examining constables’ and sergeants’ online fraud preparedness. *Security Journal*, *33*(2). https://doi.org/10.1057/s41284-019-00187-5

Bou-Hamad, I. (2020). The impact of social media usage and lifestyle habits on academic achievement: Insights from a developing country context. *Children and Youth Services Review*, *118*, 105425. https://doi.org/10.1016/j.childyouth.2020.105425

Brunner, M. (2020). Challenges and opportunities in state and local cybercrime enforcement. *Journal of National Security Law & Policy*, *10*(3), 1.

Burruss, G. W., Holt, T. J., & Wall-Parker, A. (2017). The hazards of investigating internet crimes against children: Digital evidence handlers’ experiences with vicarious trauma and coping behaviors. *American Journal of Criminal Justice*, *43*(3), 433–447. https://doi.org/10.1007/s12103-017-9417-3

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal*, *43*(1), 105–119. https://doi.org/10.1108/pijpsm-08-2019-0142

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Caserman, P., Cornel, M., Dieter, M., & Göbel, S. (2018). A concept of a training environment for police using VR game technology. *Serious Games*, 175–181. https://doi.org/10.1007/978-3-030-02762-9_18

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2016.2337

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2018). Police cybercrime training: Perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/pay078

Cohen, D. J., & Crabtree, B. F. (2008). Evaluative criteria for qualitative research in health care: Controversies and recommendations. *The Annals of Family Medicine*, *6*(4), 331–339. https://doi.org/10.1370/afm.818

Conway, G., & Hadlington, L. (2018). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online

risk and victimization. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/pay098

Coull, N., Donald, I., Ferguson, I., Keane, E., Mitchell, T., Smith, O. V., Stevenson, E., & Tomkins, P. (2017). The gamification of cybersecurity training. *E-Learning and Games*, 108–111. https://doi.org/10.1007/978-3-319-65849-0_13

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.

Cross, C. (2019). "Oh we can't actually do anything about that": The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Cunha, I., Cavalcante, J., & Patel, A. (2017). A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution. *International Journal of Electronic Security and Digital Forensics*, *9*(3), 209. https://doi.org/10.1504/ijesdf.2017.085195

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research. *Dimensions of Critical Care Nursing*, *36*(4), 253–263. https://doi.org/10.1097/dcc.0000000000000253

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Decker, E. (2019). Full Count?: Crime rate swings, cybercrime misses and why we don't really know the score. *Journal of National Security Law & Policy*, *10*(5), 83.

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Dodge, C., & Burruss, G. (2019). Policing cybercrime. *The Human Factor of Cybercrime*, 339–358. https://doi.org/10.4324/9780429460593-15

Dolliver, D. S., Collins, C., & Sams, B. (2017). Hybrid approaches to digital forensic investigations: A comparative analysis in an institutional context. *Digital Investigation*, *23*, 124–137. https://doi.org/10.1016/j.diin.2017.10.005

Donaldson, L. (2001). *The contingency theory of organizations* (1st ed.). SAGE Publications.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116. https://doi.org/10.1007/s10611-016-9649-z

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of Sexual Behavior*, *41*(6), 1319–1320. https://doi.org/10.1007/s10508-012-0016-6

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Federal Bureau of Investigation Internet Crime Complaint Center. (2018). *2017 internet crime report*. https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf

Federal Bureau of Investigation Internet Crime Complaint Center. (2020). *Internet crime report 2020*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Finklea, K. (2017). *Dark web* (7-5700) [R44101]. Congressional Research Service.

Finklea, K. (2020). *Justice department's role in cyber incident response* [R44926]. Congressional Research Service. https://fas.org/sgp/crs/misc/R44926.pdf

Flory, T. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2016.1374

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, *18*(1). https://doi.org/10.1186/s12913-018-2915-2

Freed, B. (2019, October 22). *Ransomware attacks map chronicles a growing threat*. State Scoop. https://statescoop.com/ransomware-attacks-map-state-local-government/

Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13–26. https://doi.org/10.1108/jcrpp-07-2018-0021

Gatlan, S. (2020, February 1). Coronavirus phishing attacks are actively targeting the US. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/coronavirus-phishing-attacks-are-actively-targeting-the-us/

Gould, A. (2018). Cybercrime: The police response. *ITNOW*, *60*(4), 44–45. https://doi.org/10.1093/itnow/bwy102

Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police. *Policing: An International Journal*, *43*(1), 1–16. https://doi.org/10.1108/pijpsm-07-2019-0115

Griffith, D. (2017, November 3). Fighting cybercrime at the local level. *Police Magazine.* https://www.policemag.com/342353/fighting-cybercrime-at-the-local-level

Grispos, G. (2019). Criminals: Cybercriminals. *Encyclopedia of Security and Emergency Management*, 1–7. https://doi.org/10.1007/978-3-319-69891-5_80-1

Grispos, G., Glisson, W. B., & Storer, T. (2017). Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation*, *22*, 62–73. https://doi.org/10.1016/j.diin.2017.07.006

Gurmeet, S. (2020). Motivation manifesto. *Nolegein Journal of Performance Management & Retention Strategies*, *3*(1), 12–17.

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/pay090

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction, 31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519–536. https://doi.org/10.1080/15614263.2018.1507889

Harrell, E. (2019). *Victims of identity theft, 2016* [NCJ251147]. Bureau of Justice Statistics.

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services. (2018). *State of policing: The annual Assessment of Policing in England and Wales*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2017-2.pdf

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140–157. https://doi.org/10.1177/0002716218783679

Holt, T. J. (2019). Cybercrime subcultures. *The Human Factor of Cybercrime*, 159–172. https://doi.org/10.4324/9780429460593-7

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online

incidents. *Policing and Society*, *29*(8), 906–921. https://doi.org/10.1080/10439463.2018.1450409

Hoover, S. M., Strapp, C. M., Ito, A., Foster, K., & Roth, K. (2018). Teaching qualitative research interviewer skills: A developmental framework for social justice psychological research teams. *Qualitative Psychology*, *5*(2), 300–318. https://doi.org/10.1037/qup0000101

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science & Justice*, *57*(6), 448–454. https://doi.org/10.1016/j.scijus.2017.06.001

Hull, M., Eze, T., & Speakman, L. (2018). Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond. *2018 European Intelligence and Security Informatics Conference (EISIC)*. https://doi.org/10.1109/eisic.2018.00011

Interpol. (2016). *Annual report 2016*: *Connecting police for a safer world*.

Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Jalal, R. N.-U.-D., & Zaheer, M. A. (2017). Does job satisfaction mediate the relationship of workload, remuneration and psychological reward with job performance? *International Journal of Academic Research in Business and Social Sciences*, *7*(9). https://doi.org/10.6007/ijarbss/v7-i9/3309

James, N. (2017). *FY2017 appropriations for the department of justice* [R44424]. Congressional Research Service.

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, *84*(5), 427–450. https://doi.org/10.1177/0022018320952559

Johnson, R. R., & Lafrance, C. (2016). The influence of career stage on police officer work behavior. *Criminal Justice and Behavior*, *43*(11), 1580–1599. https://doi.org/10.1177/0093854816657577

Kamra, S., & Scott, J. (2019). Impact of data breaches to organizations and individuals. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3510590

Keeling, D., & Losavio, M. (2017). Public security & digital forensics in the United States: The continued need for expanded digital systems for security. *The Journal of Digital Forensics, Security and Law*, *12*(3), 47–59. https://doi.org/10.15394/jdfsl.2017.1452

Kesselman, G. A., Hagen, E. L., & Wherry, R. J. (1974). A factor analytic test of the Porter-Lawler expectancy model of work motivation. *Personnel Psychology*, *27*(4), 569–579. https://doi.org/10.1111/j.1744-6570.1974.tb01177.x

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Koziarski, J., & Lee, J. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, *43*(1), 198–211. https://doi.org/10.1108/pijpsm-07-2019-0107

Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly*, *12*(1), 1. https://doi.org/10.2307/2391211

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review*, *31*(1), 20–39. https://doi.org/10.1177/1057567719846224

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2016). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change*, *67*(1), 77–96. https://doi.org/10.1007/s10611-016-9648-0

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force Report. *American Psychologist*, *73*(1), 26–46. https://doi.org/10.1037/amp0000151

Lobe, B., Morgan, D., & Hoffman, K. A. (2020). Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods*, *19*. https://doi.org/10.1177/1609406920937875

Loveday, B. (2017). Still plodding along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science & Management*, *19*(2), 101–109. https://doi.org/10.1177/1461355717699634

Macdonald, K. (2021). Cyber investigation: A new frontier for police. *The Journal of Intelligence, Conflict, and Warfare*, *3*(3), 91–94. https://doi.org/10.21810/jicw.v3i3.2754

Majid, M. A. A., Othman, M., Mohamad, S. F., Lim, S. A. H., & Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences*, *7*(4). https://doi.org/10.6007/ijarbss/v7-i4/2916

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, *26*(13), 1753–1760. https://doi.org/10.1177/1049732315617444

Maroz, N. (2019). Regionalization of international cooperation in the fight against cybercrime. *Union of Jurists of Romania. Law Review*, 10(2), 218–227.

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Sage.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370–396. https://doi.org/10.1037/h0054346

Matusiak, M. C. (2018). Environmental predictors of municipal police agency goals. *Police Quarterly*, *22*(1), 112–136. https://doi.org/10.1177/1098611118797068

McGuire, M. (2019, February 27). Social media-enabled cybercrime is generating $3.25 billion a year. *Help Net Security.* https://www.helpnetsecurity.com/2019/02/27/social-media-enabled-cybercrime/

Mee, P., & Schuermann, T. (2018, September 14). How a cyber attack could cause the next financial crisis. *Harvard Business Review*. https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis

Mirdul, S., & Satvinder, K. (2019). Cyber crimes becoming threat to cyber security. *Academic Journal of Forensic Sciences*, *2*(2), 36–40.

Mitsilegas, V., Hufnagel, S., & Moiseienko, A. (2019). *Research handbook on transnational crime*. Edward Elgar Publishing. https://doi.org/10.4337/9781784719449

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, *23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Morar, P., Read, J., Arora, S., Hart, A., Warusavitarne, J., Green, J., Sevdalis, N., Edwards, C., & Faiz, O. (2015). Defining the optimal design of the inflammatory bowel disease multidisciplinary team: results from a multicentre qualitative expert-based study. *Frontline Gastroenterology*, *6*(4), 290–297. https://doi.org/10.1136/flgastro-2014-100549

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18. https://doi.org/10.1080/13814788.2017.1375091

Nascimento, L. de C. N., Souza, T. V., de Oliveira, I. C., dos S., Moraes, J. R. M. M. de, Aguiar, R. C.B … Silva, L. F. da. (2018). Theoretical saturation in qualitative research: an experience report in interview with schoolchildren. *Revista Brasileira de Enfermagem*, *71*(1), 228–233. https://doi.org/10.1590/0034-7167-2016-0616

Nodeland, B., Belshaw, S., & Saber, M. (2018). Teaching cybersecurity to criminal justice majors. *Journal of Criminal Justice Education*, *30*(1), 71–90. https://doi.org/10.1080/10511253.2018.1439513

Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M. (2019). *Cybercrime investigators are users too: Understanding the socio-technical challenges faced by law enforcement [Workshop on Usable Security (USEC]*. arXivLabs.

Novak, A. N., & Vilceanu, M. O. (2019). "The internet is not pleased": Twitter and the 2017 Equifax data breach. *The Communication Review*, *22*(3), 196–221. https://doi.org/10.1080/10714421.2019.1651595

Ntinda, K. (2019). Narrative research. *Handbook of Research Methods in Health Social Sciences*, 411–423. https://doi.org/10.1007/978-981-10-5251-4_79

Oltmann, S. (2016). Qualitative interviews: A methodological discussion the interviewer and respondent contexts. *Qualitative Sociological Research*, *17*(2). https://doi.org/10.17169/fqs-17.2.2551

Ospina, S. M., Esteve, M., & Lee, S. (2017). Assessing Qualitative Studies in Public Administration Research. *Public Administration Review*, *78*(4), 593–605. https://doi.org/10.1111/puar.12837

Paek, S., Nalla, M. K., & Lee, J. (2020). Determinants of police officers' support for the public-private partnerships (ppps) in policing cyberspace. *Policing: An International Journal*, *43*(5), 877–892. https://doi.org/10.1108/pijpsm-06-2020-0088

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2017). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*(1), 1–21. https://doi.org/10.1080/17440572.2017.1411807

Paulsen, C., & Bryers, R. (2019). *Glossary of key information security terms* (NIST IR 7298 Revision 3). National Institute of Standards and Technology Interagency. https://doi.org/10.6028/NIST.IR.7298r2

Peck, B., & Mummery, J. (2017). Hermeneutic constructivism: An ontology for qualitative research. *Qualitative Health Research*, *28*(3), 389–407. https://doi.org/10.1177/1049732317706931

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68–74. https://doi.org/10.1109/msec.2020.2969409

Poushter, J., & Manevich, D. (2017). Globally, people point to ISIS and climate change as leading security threats. *Pew Research Center's Global Attitudes Project.* https://www.pewresearch.org/global/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/

Preis, B., & Susskind, L. (2020). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review*, (1). https://doi.org/10.1177/1078087420973760

Promnick, G. (2017). Cyber economic espionage: Corporate theft and the new Patriot Act. *Hastings Science & Technology Law Journal*, *9*(1), 89.

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. s., & Wasseem, A. (2019). Case Study Method: A Step by-Step Guide for Business Researchers. *International Journal of Qualiitative Methods*, 18, 1-13. Sagepub. https://doi.org/10.1177/1609406919862424

Ratikant, S. (2017). Evolution and shift in trend of cyber crime: An overview. *Cyber Times International Journal of Technology & Management*, *10*(2), 1–4.

Ravitch, S. M., & Carl, Nicole C. Mittenfelner. (2015). *Qualitative research: Bridging the conceptual, theoretical, and methodological*. Sage.

Robinson, O. C. (2013). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25–41. https://doi.org/10.1080/14780887.2013.801543

Romanosky, S., Stanley, K., Taylor, J., & Winkelman, Z. (2017). Law enforcement cyber center: Final technical report. *RAND Corporation*. https://doi.org/10.7249/rr2320

Ross, P. T., & Bibler Zaidi, N. L. (2019). Limited by our limitations. *Perspectives on Medical Education*, *8*(4), 261–264. https://doi.org/10.1007/s40037-019-00530-x

Rubel, D., & Okech, J. (2017). Qualitative research in group work: Status, synergies, and implementation. *The Journal for Specialists in Group Work*, *42*(1), 54–86. https://doi.org/10.1080/01933922.2016.1264522

Ryan, C. (2018). Computer and internet use in the United States: 2016. *American Community Survey Reports.*

https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, *34*(4), 1023–1053. https://doi.org/10.1080/07421222.2017.1394049

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, *19*(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

Skidmore, M., Goldstraw-White, J., & Gill, M. (2020). Understanding the police response to fraud: The challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management*, *40*(5), 369–379. https://doi.org/10.1080/09540962.2020.1714203

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, *24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Tagarev, T. (2016). A generic reference curriculum on cybersecurity. *Information & Security: An International Journal*, *35*, 181–184. https://doi.org/10.11610/isij.3510

Thiagaraj, D., & Thangaswamy, A. (2017). Theoretical concept of job satisfaction - a study. *International Journal of Research -GRANTHAALAYAH*, *5*(6), 464–470. https://doi.org/10.29121/granthaalayah.v5.i6.2017.2057

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/pijpsm-07-2019-0122

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46. https://researchers.mq.edu.au/en/publications/closing-the-cybersecurity-skills-gap

Wang, S.-Y. K., Hsieh, M.-L., Chang, C. K.-M., Jiang, P.-S., & Dallier, D. J. (2020). Collaboration between law enforcement agencies in combating cybercrime: Implications of a Taiwanese case study about ATM Hacking. *International Journal of Offender Therapy and Comparative Criminology*, *65*(4), 0306624X2095239. https://doi.org/10.1177/0306624x20952391

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, *29*(2), 105–124. https://doi.org/10.1080/1478601x.2016.1170282

Woolf, N. H., & Silver, C. (2017). *Qualitative analysis using ATLAS.ti, NVivo and MAXQDA: The five-level QDA method*. Routledge.

Wydra, C., & Hartle III, F. (2015). Educating the technology officer of the future: A needs analysis. *Issues in Information Systems*, *16*(4), 224–231.

Xingan, L. (2018). Crucial elements in law enforcement against cybercrime. *International Journal of information Security Science*, *7*(3), 140–158.

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*,

ahead-of-print(ahead-of-print), 1089–1105. https://doi.org/10.1108/jfc-04-2020-0055

Zanasi, A., Ruini, F., & Bonzio, A. (2017). Intelligence analysts' training through serious games: The Leila project. *International Journal of Safety and Security Engineering*, *7*(3), 380–389. https://doi.org/10.2495/safe-v7-n3-380-389

Appendix: Interview Questions

1. Tell me a bit about your background and experience in the law enforcement field.
2. How long have you worked in the law enforcement field?
3. What is your Rank?
4. What is the highest level of education you have completed?
5. What would you say is the size of your agency?
6. In your opinion, what is cybercrime?
7. What roles do you believe local law enforcement agencies should play in responding to cybercrime?
8. What do you think the roles should be for law enforcement officers in preventing and investigating cybercrimes at the local level?
9. How Confident are you in your own ability to respond to online crimes effectively?
10. What are the procedural steps taken by your law enforcement agency when investigating cybercrimes locally?
11. What are the protocols for first responder officers who responds to computer-related incidents?
12. What procedural steps are taken by your law enforcement agencies when cybercrimes are reported by citizens or businesses?
13. What is the process that victims take when reporting cybercrime incidents to your law enforcement agency?

14. What are some types of computer-related crimes typically investigated by law enforcement officers at the local level?
15. What current training opportunities and availability in cybercrime can officers take during in service trainings?
16. What cybercrime trainings have you taken within the last year of in-service training?
17. In your opinion, what are the major constraints or limitations for law enforcement officers in responding to computer-related crimes at the local level?
18. In your opinion, is cybercrime taken seriously by law enforcement agencies at the local level to investigate?
19. Who do you believe should be primarily responsible for investigating cybercrime cases?
20. What should law enforcement agencies do to improve the overall effectiveness of combating cybercrime at the local level?
21. What role do you see law enforcement officers playing in policing cybercrime in the future at the local level?