Law Enforcement Officers' Reaction on Traditional Crimes to Fight Cybercrime Locally

Coleman McKoy

Department of Computer Information Systems, Parker University, 2540 Walnut Hill Ln, Dallas, TX 75229, **USA**

*Corresponding Contact:
Email: cmckoy@parker.edu

Manuscript Received: 27 Sept 2021 Accepted: 22 Nov 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 study focuses on how law enforcement officers who respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally. Data collection consisted of semi structured interviews, where member-checking helped to enhance the trustworthiness. 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. 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.

Keywords: Law Enforcement Officer, Traditional Crime, Cybercrime, Cybercrime Fight

INTRODUCTION

Many large-scale crimes are committed via the internet (Loveday, 2017), and cybercriminals frequently commit online crimes without facing legal consequences due to their ability to surf the internet while avoiding detection. In 2017, for example, Equifax had a data breach that exposed over 144 million people to identity theft (Novak & Vilceanu, 2019). The Marriot Hotel was hit by a cyber-attack in 2018 that affected 500 million people. Individuals have gotten complacent in their efforts to protect themselves from cybercrime as a result of constant media coverage (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; Manavalan & Chisty, 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).

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).

Objectives of the Study

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.

Research Questions

The research questions helped guide this qualitative research study:

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

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). 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 (Manavalan & Ganapathy, 2014; Brunner, 2020).

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, 2018).

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, 2018). 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).

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; Achar & Tisuela, 2020). 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., 2017).

Jurisdictional Boundaries

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.

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).

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 (Achar, 2019; Levi, 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., 2017). 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.,2017). 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.

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; Achar, 2018). 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.

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, and details about data collection, data analysis, and validity.

Research Design

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

I used snowball sampling with the nine participants or until saturation occurred in the study using semistructured interviews. Semi structured 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. Semi structured

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.

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 saturation was achieved after nine interviews.

DATA ANALYSIS

The collection of data came through in-depth, semi structured interviews that featured 12 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.

The data analysis for this study was guided by the primary research questions:

How do law enforcement officers' that respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime locally?

Figure 1: Word Cloud

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).

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 research questions for this study were:

How do law enforcement officers who respond to traditional crimes describe law enforcement agencies' preparedness to fight cybercrime 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	1,2,3,4,5,6,11 and 12
Cybercrime Awareness	9	6
Cybercrime Training	9	7,8, and 10
Limitation to Responding to Cybercrimes	9	9, 10

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

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."

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

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, which is compatible with the study of Williams (2018). 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.

SUMMARY OF FINDINGS

This study 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:

- What roles do you believe local law enforcement agencies should play in responding to cybercrime?
- What roles do you believe local law enforcement agencies should play in responding to cybercrime?
- What do you think the roles should be for law enforcement officers in preventing and investigating cybercrimes at the local level?
- What are the procedural steps taken by your law enforcement agency when investigating cybercrimes locally?
- What role do you see law enforcement officers playing in policing cybercrime in the future at the local level?

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.

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.

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.

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 (Williams, 2020).

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.

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.

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.

REFERENCES

Achar, S. (2018). Data Privacy-Preservation: A Method of Machine Learning. ABC Journal of Advanced Research, 7(2), 123-129. https://doi.org/10.18034/abcjar.v7i2.654

Achar, S. (2019). Behavioral and Perceptual Models for Secure Data Analysis and Management. *Global Disclosure of Economics and Business*, *8*(2), 143-152. https://doi.org/10.18034/gdeb.v8i2.653

Achar, S., & Tisuela, N. L. (2020). A Review of Hosting Enterprise SaaS with IaC on Multi-cloud Platforms. *International Journal of Reciprocal Symmetry and Physical Sciences*, *7*, 14–23. https://upright.pub/index.php/ijrsps/article/view/72

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

Manavalan, M., & Chisty, N. M. A. (2019). Visualizing the Impact of Cyberattacks on Web-Based Transactions on Large-Scale Data and Knowledge-Based Systems. *Engineering International*, *7*(2), 95-104. https://doi.org/10.18034/ei.v7i2.578

Manavalan, M., & Ganapathy, A. (2014). Reinforcement Learning in Robotics. *Engineering International*, *2*(2), 113-124. https://doi.org/10.18034/ei.v2i2.572

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

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

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

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

Williams, R. T. (2018). Confidence Interventions: Do They Work?. *Asian Journal of Humanity, Art and Literature*, *5*(2), 123-134. https://doi.org/10.18034/ajhal.v5i2.536

Williams, R. T. (2020). The Paradigm Wars: Is MMR Really a Solution?. *American Journal of Trade and Policy*, *7*(3), 79-84. https://doi.org/10.18034/ajtp.v7i3.507

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

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

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. What do you think the roles should be for law enforcement officers in preventing and investigating cybercrimes at the local level?
7. What current training opportunities and availability in cybercrime can officers take during in service trainings?
8. What cybercrime trainings have you taken within the last year of in-service training?
9. In your opinion, what are the major constraints or limitations for law enforcement officers in responding to computer-related crimes at the local level?
10. In your opinion, is cybercrime taken seriously by law enforcement agencies at the local level to investigate?
11. What should law enforcement agencies do to improve the overall effectiveness of combating cybercrime at the local level?
12. What role do you see law enforcement officers playing in policing cybercrime in the future at the local level?

--0--