2019

Sharing of Threat-Related Information Among Public Safety Agencies in Honolulu, Hawaii

Cortney M. Chambers
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Cortney M. Chambers

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. Paul Rutledge, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Michael Knight, Committee Member,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, University Reviewer,
Public Policy and Administration Faculty

The Office of the Provost

Walden University
2019

Abstract

Sharing of Threat-Related Information Among Public Safety Agencies in Honolulu, Hawaii

by

Cortney M. Chambers

MA, American Military University, 2011

BS, American Military University, 2009

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2019

Abstract

There is a lack of knowledge regarding how public safety organizations communicate threat-related information at the local level. The purpose of this qualitative exploratory case study was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, emergency medical services, and public health) in Honolulu, Hawaii. The conceptual framework for the study was general systems theory. The sample for this study was a subset of 13 individuals from the larger population of approximately 50 subject matter experts who worked within four public safety agencies and had extensive experience analyzing and sharing threat-related information. Purposeful sampling was utilized for the study. Data were collected through in-depth interviews. The findings of this study clearly identified several important themes related to sharing threat-related information between local public safety organizations: information flow, collaboration, participation with the state fusion center, and the complexity of sharing confidential information. I found that Honolulu public safety agencies are currently communicating through information flow within and between organizations; however, this flow of information is intermittent. I also found that threat-related information often contains highly protected, or law enforcement sensitive information, and is difficult to share between agencies. Inadequate threat-related information sharing and poor collaboration among local public safety agencies may put the public at increased risk from violent attacks. The results of this study contribute to positive social change by identifying the benefits and challenges of sharing threat-related information between local public safety agencies.

Sharing of Threat-Related Information Among Public Safety Agencies in Honolulu, Hawaii

by

Cortney M. Chambers

MA, American Military University, 2011

BS, American Military University, 2009

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2019

Acknowledgments

I would like to thank my Lord and Savior Jesus Christ for allowing me to reach this point in my academic career and in my life. I would like to thank my wife Yoko Chambers for supporting me emotionally during this long and difficult journey. I would also like to thank my parents Gene and Jane Chambers and the rest of my family for giving me kind words of encouragement along the way.

I am forever grateful to Dr. Rutledge, Dr. Knight, Dr. Ozymy, and all those at Walden University who contributed to the successful completion of this dissertation.

Table of Contents

List of Tables v

List of Figures vi

Chapter 1: Introduction to the Study 1

Background of the Study 4

Benefits of Collaboration 6

Challenges to Collaboration 8

Problem Statement 9

Purpose of the Study 11

Research Questions 12

Conceptual Framework 13

Nature of the Study 16

Operational Definitions 19

Assumptions 22

Scope and Delimitations 22

Significance 23

Implications for Social Change 24

Summary 24

Chapter 2: Literature Review 26

Literature Search Strategy 28

Conceptual Framework 29

Literature Review 31

Benefits of Sharing Threat-Related Information 32
Fusion Center Facilitation of Information Sharing 41
Challenges of Sharing Threat-Related Information 48
Social Media Use Between Public Safety Agencies 58
Summary and Conclusions 66
Chapter 3: Research Method 69
Research Design and Rationale 69
Mode of Qualitative Analysis 73
Role of the Researcher 74
Methodology 75
Participant Selection Logic 75
Instrumentation 77
Procedures for Recruitment, Participation, and Data Collection 78
Data Analysis Plan 80
Issues of Trustworthiness 82
Credibility 82
Transferability 82
Dependability 83
Confirmability 83
Ethical Procedures 84
Summary 85
Chapter 4: Results 86

Field Test 87
Demographics 89
Data Collection 91
Data Analysis 94
Evidence of Trustworthiness 102
Credibility 102
Transferability 103
Dependability 104
Confirmability 104
Study Results 105
Interview Question 1 105
Interview Question 2 109
Interview Question 3 114
Interview Question 4 118
Interview Question 5 123
Interview Question 6 129
Interview Question 7 134
Interview Question 8 140
Interview Question 9 144
Interview Question 10 153
Summary 163
Chapter 5: Discussion, Conclusions, and Recommendations 165

Interpretation of Findings 166
Limitations of the Study 175
Delimitations of the Study 175
Recommendations 176
Implications 177
Conclusion 179
References 181
Appendix A: Invitation to Participate 195
Appendix B: Interview Protocol 196
Appendix C: Chart Linking Research Questions to Interview Questions 198
Appendix D: Coding Protocol 199
Appendix E: Code Book 200
Appendix F: Field Test 206

List of Tables

Table 1. Participant Demographics 90

Table 2. Interview Descriptive Statistics 91

Table 3. Table of Themes 96

Table 4. Table Linking Research Questions to Overarching Themes 102

List of Figures

Figure 1. Comparison of topic frequency in participants' responses to Interview Question 1 108

Figure 2. Comparison of topic frequency in participants' responses to Interview Question 2 112

Figure 3. Comparison of topic frequency in participants' responses to Interview Question 3 117

Figure 4. Comparison of topic frequency in participants' responses to Interview Question 4 122

Figure 5. Comparison of topic frequency in participants' responses to Interview Question 5 127

Figure 6. Comparison of topic frequency in participants' responses to Interview Question 6 132

Figure 7. Comparison of topic frequency in participants' responses to Interview Question 7 138

Figure 8. Comparison of topic frequency in participants' responses to Interview Question 8 142

Figure 9. Comparison of topic frequency in participants' responses to Interview Question 9 150

Figure 10. Comparison of topic frequency in participants' responses to Interview Question 10 160

Chapter 1: Introduction to the Study

Terrorism and violent extremism continue to dominate the 24-hour news cycle. One needs only to review the 2015 Paris attacks that had 130 fatalities ("BBC News," 2015), the 2017 assault at the Las Vegas Harvest Music Festival that had 58 fatalities (Bui, Zapotosky, Barrett, & Berman, 2017), or numerous mall and school shootings across the United States ("Worst Mass Shootings," 2019) to recognize that terrorism and violent extremism are on the rise globally (Husain, 2015). Concurrently, the information revolution is evolving at an exponential rate with more and more activity of daily life conducted online (Huda et al., 2018). With violent extremist organizations now able to communicate and recruit followers via the Internet, it is critical that public safety organizations analyze information from all available sources and share threat-related information between agencies ("Public Safety," 2011).

After the 9/11 terrorist attacks, the National Commission on Terrorist Attacks Upon the United States, commonly known as the 9/11 Commission, developed suggestions to protect the nation from another assault ("National Commission," 2004). Several of the recommendations focused on sharing information between public safety agencies ("State and Major Urban," 2014). Federal, state, and local governments have invested billions of dollars to protect the American public from terrorist and violent extremist attacks (Hesterman, 2019). A primary role of public safety departments is "prevention and protection of the public from dangers affecting safety" ("Public Safety Law," 2014, para. 1).

The benefits of monitoring and analyzing threat-related information are numerous. A 2012 White House publication entitled, *National Strategy for Information Sharing and Safeguarding*, acknowledged that information sharing between public safety organizations increases their ability to prevent threats to the public. Public safety organizations across the United States have developed methods to monitor threat-related information from the Internet and other openly available sources. The challenge is how to effectively share this information between public safety agencies (Carter & Rip, 2013). Before 2001, the nation's public safety organizations worked together when necessary, but rarely shared information. It took several years for public safety agencies to develop relationships, policies, and interoperable communications equipment to facilitate effective information sharing (Carter et al., 2017). Organizational cultures within agencies had to adapt to a new philosophy of interagency cooperation ("Better information sharing," 2015).

Currently, there is not a clear understanding of the benefits and challenges of information sharing between local public safety agencies. Although there is much data about how federal agencies exchange threat-related information (Carter et al., 2017; Bharosa, Lee, & Janssen, 2010; Vacca, 2019), there is a lack of information on how local public safety agencies share this same type of data. Over the last decade, challenges to information sharing between local public safety organizations have emerged, but only a small number of these challenges have been documented in the literature. Information sharing between local agencies is proving to be much more difficult than it once appeared. It is well known that the organizational and political culture of agencies can

impede the process of information sharing (Mah, 2014). Communication equipment technology differences may also limit information exchange but are easier to resolve than cultural issues (Allen, Karanasios, & Norman, 2014). What is not known are the challenges local public safety agencies face when sharing threat-related information between one another for the purpose of promoting public safety. Researchers do not fully understand the benefits and challenges of collaboration among these agencies, due to limited research on this issue (Carter et al., 2017). This lack of knowledge is problematic because local agencies hold the primary responsibility of responding to public safety threats.

In reviewing the literature, I found no studies that focused on the specific benefits and challenges of sharing information between local public safety organizations in Honolulu, Hawaii. Hawaii presents a unique case because unlike the contiguous 48 states and Alaska, should something happen, mobilizing help from the mainland is logistically more complicated. Understanding how threat information is shared in Hawaii is thus critical because of its isolation. The findings of this study may help to fill this gap in knowledge.

All modes of communication between agencies must be utilized to provide for a collaborative approach to preparing for and responding to events that affect public safety. A unique and evolving information resource used by public safety organizations (law enforcement, fire services, emergency medical services [EMS], and public health) is known as open source information. It is essentially any information that is openly available to the public ("Intelligence," 2013). Public safety organizations in most U.S.

metropolitan areas are now equipped to monitor open source information on the Internet and analyze it for potential threats to the public. If impending threats are discovered, it is important that the information is effectively shared with other public safety organizations in the region. The benefits and challenges that these organizations face when sharing threat-related information between agencies was the topic of this study.

Chapter 1 will include a discussion of the background and the need for information sharing and collaboration between agencies and the rationale to public safety. I will discuss the problem for the study and the purpose and provide a brief overview of the benefits and challenges that public safety agencies face. The chapter also includes an overview of general systems theory ("General Systems Theory," 2014), which served as the conceptual framework for the study, and how it relates to sharing of information and collaboration. The nature of the study is also discussed. Limitations, delimitations, and assumptions are presented. Chapter 1 concludes with a rationale for performing the study and an introduction to the literature review in Chapter 2.

Background of the Study

Valuable threat-related information can be obtained from analyzing publicly available information on the Internet. There is often information uncovered in an initial attack that may have the potential of stopping more attacks when effective collaboration occurs with the appropriate public safety agencies (Chermak et al., 2013). The rapid communication of threat-related information is vital immediately following an attack, but it comes with challenges.

After the San Bernardino (Schmidt & Masood, 2015) and Orlando attacks (Ellis et al., 2016), the connections between these two terrorist plots, occurring in vastly different areas of the United States, became evident to law enforcement agencies. This knowledge reinforced why it is so important to analyze threat-related information before and after an attack. The benefits of monitoring and analyzing open source information are immense but are still not completely known (Carter et al., 2017). Much work still needs to be done to meet the challenges involved in collaboration among public safety agencies (Carter et al., 2017). Public safety agencies across the nation must adapt to a new asymmetrical threat environment and elevate threat-related information sharing to a high priority within their organizations.

Before 2001, U.S. public safety organizations worked together when necessary, but rarely shared information. Shortly after the September 11th attacks, the 9/11 Commission pointed to a series of suggestions, that if implemented, would better protect the nation. Many of the recommendations pertained to increased "sharing of threat-related information between federal, state, local, tribal, and private partners" ("State and Major Urban," 2014, para. 1). The 9/11 Commission acknowledged that it was vitally important that this information sharing occur between all agencies that are responsible for the public's safety, not only law enforcement organizations ("National Commission," 2004). A 2012 White House Publication entitled, *National Strategy for Information Sharing and Safeguarding*, affirms that the nation's security "depends on our ability to share the right information, with the right people, at the right time" (p. 1). Chermak, Carter, Carter, McGarrell, and Drew (2013) argue that the use of intelligence methods has

enhanced law enforcement agencies ability to prevent threats to the public throughout the U.S.

Hu, Knox, and Kapucu (2014) explained that it took nearly a decade for public safety organizations to see the benefits of exchanging threat-related information and "shift from a centralized command and control system to a more collaborative approach" (p. 699). New policies had to be developed and implemented, communications equipment had to be purchased or retrofitted with interoperable capabilities, and organizational cultures had to adapt to a philosophy of information sharing (Hu et al., 2014). Although there are a multitude of social media communication platforms that are consistently used by the public, there continues to be increased scrutiny of public safety organizations' sharing of threat-related open source information due to privacy concerns (Carter et al., 2017). Public safety organizations monitoring of social media has raised privacy concerns throughout the nation. Therefore, it is important that agencies develop privacy policies and make them available on their websites notifying the public of how they plan to monitor social media data.

Benefits of Collaboration

What is known and documented from a thorough review of the current literature are the benefits of sharing threat-related information between public safety agencies, but little is known of the challenges that are faced (Carter et al., 2016). The sharing of information between public safety organizations can increase the agency leaders' ability to identify and prevent threats to the public ("National Strategy for Information Sharing," 2012). The November 2015 Paris attacks involved trained attackers targeting numerous

locations throughout the city. The attackers used high-powered automatic weapons and suicide vests making the attack a complex and well executed operation that took weeks if not months of planning (Witte & Morris, 2015). Following the attack, European security experts pointed out that "poor information-sharing among intelligence agencies, a threadbare system for tracking suspects across open borders and an unmanageably long list of homegrown extremists to monitor" (para. 2) were factors contributing to the deadly attack (Witte & Morris, 2015). French officials maintain that information sharing between public safety agencies may prevent, or at least reduce, the impact of future attacks.

Huyck (2015) pointed out that the specifics of information sharing between public safety agencies have not yet been adequately defined. Information sharing occurs in various forms and at different levels depending on the specific organizations involved (Huyck, 2015). Whenever an attack on the public takes place, the need for the coordination of information sharing across all first responder agencies rapidly increases ("Orlando Terror Attack," 2015). To facilitate the stream of information that is monitored and shared between public safety agencies, coordination has to be facilitated from the top down.

Information exchange at the operational level requires a well-designed communication system that has been developed specifically for the sharing of real-time actionable information between public safety agencies (Huyck, 2015). Also, in order for first responders to share information effectively, they must have rehearsed the procedures multiple times during realistic training scenarios.

Challenges to Collaboration

The challenges of utilizing and sharing threat-related information have also come into play over the last decade, but little is known of these challenges in the literature. Information sharing between local, state, and federal partners is much more difficult than it appears. Agencies organizational culture and political posture often come into play, which can slow down the flow of information between entities (Mah, 2014). Technology differences between organizations can also limit information flow.

A common thread between many of the recent terror attacks is that government agencies had threat-related information linked to the suspects before the attack, but the information was not initially recognized as critical and was not effectively shared to local public safety officials (Ellis et al., 2016). Law enforcement officials are now aggressively identifying potential threats through monitoring open source and social media sources. However, if the information is not shared with other public safety organizations, critical threat information that may be necessary to avert a future attack may remain undeveloped and therefor unusable.

There is significant literature on information sharing between federal and local agencies throughout the U.S., but I found no studies that focus on the specific benefits and challenges of sharing threat-related information between public safety organizations in Honolulu, Hawaii. Hawaii presents a unique case because unlike the contiguous 48 states and Alaska, should something happen, mobilizing help from the mainland is logistically more complicated. Understanding how threat information is shared in Hawaii is critical because of the state's isolation from the rest of the nation. The findings of this

study will help to fill this gap in literature by determining the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii. The participants for this study will be current, or former, subject matter experts (SMEs) experts who have extensive experience working in an information-sharing role in Honolulu public safety organizations. A presentation of the findings of this study will extend the existing literature on the benefits and challenges of information sharing between public safety organizations. It will be interesting to see the challenges and benefits that each report, and how these SMEs believe that the process of sharing information between public safety organizations can be improved.

Problem Statement

The overarching problem addressed in this study is the importance of communication between public safety agencies as they manage serious emerging threat-related issues such as terrorism. After the 9/11 attacks on the United States, the federal government established guidelines to improve the communication and coordination between public safety organizations in order to prevent future terrorist attacks ("Homeland Security," 2016). Public safety organizations throughout the nation have used these guidelines to establish policies in an effort to improve information sharing between agencies.

There is reliable information in the literature about the sharing of information between federal and local agencies (e.g., Carter et al., 2017; Bharosa, Lee, & Janssen, 2010) but there is a lack of knowledge on information sharing between local agencies. This is problematic because local agencies are on the front lines of the struggle against

terrorism and are the nation's first layer of defense. Researchers and policy makers do not understand the benefits and challenges of collaboration among these agencies (Carter et al., 2017), which, given their unique threat setting, should be working closely together. It is not just communication between law enforcement agencies that is important but communication across all public safety agencies, including EMS, fire services, and public health. In an ideal world, local public agencies would have excellent interagency communication, and everyone would respond effectively when a public safety event happens. In reality, policy makers do not know if this is the case because research has not been done in this area.

Research involving terrorist and violent extremist activity has demonstrated a lack of communication and coordination of efforts to thwart attacks ("National Commission," 2004). Examples of this lack of communication are the Boston Marathon (Hu et al., 2014), the San Bernardino (Schmidt & Masood, 2015), and the Orlando terror attacks (Ellis et al., 2016), all of which shared similarities among the attackers. Threat-related information sharing between local, state, and federal partners is often difficult, but could have prevented some of these events from occurring at the outset, according to experts (Chermak et al., 2013).

The benefits are more obvious when terror attacks are thwarted, such as the unsuccessful 2015 Joshua Ryne Goldberg attack on a 9/11 Memorial event in Kansas City, Missouri (Ellis & Botelho, 2015). But more terror attacks can be prevented if all agencies cooperate and coordinate their efforts. Loss of life may be prevented if challenges to threat-related information sharing between local public safety organizations

are identified and eliminated (Chermak et al., 2013). The steady increase in violent attacks and other threat-related public safety issues is the reason this research is so important.

The gap in the literature is that researchers do not know how public safety organizations communicate threat-related information at the local level. Therefore, it is unknown whether there are challenges or benefits to sharing threat-related information between local public safety agencies in the United States. The findings of this study may help to fill this gap in the literature by providing insight on the perceived benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii.

Purpose of the Study

The purpose of this qualitative exploratory case study was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii. I focused on Honolulu for several reasons. Honolulu is a moderate sized city and faces many of the same challenges as other cities in the continental United States, including the need to share information across agencies in order to manage emerging threat-related issues. However, Honolulu is unique because unlike other cities it is remote and isolated, being approximately 2,500 miles from the mainland. Assistance from other states may not be available for several days due to shipping transit time (“Pasha Hawaii,” 2019). As a result, there is an increased need to ensure interagency information sharing is occurring to facilitate the region’s ability to manage an attack.

The gap in the current literature is that researchers do not know how public safety organizations communicate threat-related information at the local level. It is essential that agencies communicate threat-related information effectively, according to Chermak et al., 2013. Due to their unique situation, Honolulu public safety agencies provide an excellent opportunity for this research. The participants for this study were individuals who had at least 15 years' experience sharing threat-related information between public safety organizations in Honolulu. The findings should provide a unique understanding of how public safety organizations currently share threat-related information encounter challenges, and how these challenges differ between organizations.

Research Questions

I sought to answer three research questions (RQs) for this qualitative exploratory case study. The questions were aimed at exploring the benefits and challenges that exist in sharing threat-related information between public safety organizations in Honolulu, Hawaii.

RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?

RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

Conceptual Framework

This research was a phenomenological study. I used general systems theory as the conceptual framework because it effectively describes how information is exchanged between public safety organizations to protect the population from attacks. The theory also provided a conceptual platform to explore the specific research questions of this study. The goal of the research was to explore how agencies within the Honolulu public safety system are communicating with one another. I explored how public safety systems are interacting to create a cohesive response when needed.

Systems are essentially a set of objects, or variables "that affect one another within an environment and form a larger pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). In 1936 Ludwig von Bertalanffy first proposed general systems theory and the theory was expanded upon in the 1960s by Ross Ashby ("General Systems Theory," 2014). Von Bertalanffy (1968) stated that systems were comprised of a series of components that are in constant interaction with their environment.

General system theory can be defined as "the transdisciplinary study of the abstract organization of phenomena, independent of their substance, type, or spatial or temporal scale of existence" ("Communication Theories," 2019, p. 32). A system is often described as consisting of four things. The first are objects, the second attributes, the third is a relationship between those attributes, and the fourth is that the systems exist within a setting, or environment ("Communication Theories," 2019). Systems are essentially a set of objects, or variables "that affect one another within an environment and form a larger

pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). Because elements in systems are constantly interacting with one another, when one part of a system changes it results in a change somewhere else within the system ("Communication Theories," 2019).

General systems theory will best guide the research to answer this study's research questions. The theory has been used for several decades to study federal, state, and local government organizations. General systems theory is useful when studying the organizational changes and development of a community's public safety system because it allows the researcher to explore the interconnection between individual agencies, or subsystems. When public safety organizations within the same region share relevant threat information with one another, it prompts other agencies within that region to prepare for, or possibly counter the threat. Government public safety agencies work together as a system to protect the public. Therefore, if miscommunication of threat-related information occurs in one agency within a system, it can lead to poor operational decisions being made in another agency within the system, and potentially lead to a failure of the system to protect the public.

Because public safety systems are constantly interacting with one another, when one part of a system changes, it will result in a change somewhere else within the structure ("Communication Theories," 2019). As public safety analysts monitor the Internet and social media for terms, phrases, and threat-related indicators, they identify risks and then notify other public safety organizations within their regional network to effectively address the threat ("Public Safety," 2011).

The sharing of threat-related information between public safety organizations is vital to improving law enforcement's ability to uncover and stop violent attacks before they occur. Analysts at public safety organizations throughout the U.S. have the capability to research and analyze multiple forms of information from all regions of the nation, fusing local, regional, and national threat information together to uncover possible threats ("Public Safety," 2011).

State and local fusion centers are helping to integrate public safety organizations into an information-sharing environment. As public safety analysts collect and analyze information from multiple sources, they pass threat-related information to state fusion centers and then up to the federal government. Federal agencies share the information with their intelligence apparatus, add additional analysis, pass it back to state fusion centers and then finally back to the local public safety agencies. This circular information sharing, and collaboration process helps to protect the public from potential attacks.

As geopolitical situations evolve and develop, organizations with the responsibility for guarding the public's safety must adapt to a new asymmetrical threat environment through improved domestic intelligence (Rosenbach & Peritz, 2009). Fusion centers, which are strategically located throughout all 50 states, are currently in a position to take on an expanding role in our nation's domestic security by helping to protect the public. A more thorough explanation of the conceptual framework will be presented in Chapter 2.

Nature of the Study

A qualitative design was determined the best method to analyze this study's research information. Data was collected through interviews with SMEs, either current or recently retired, from four fields of public safety in Honolulu, Hawaii. The primary source of data was derived from in-depth interviews through conversational style discussions with the participants utilizing open-ended questions.

To ensure the interview questions were suitable to explore the research questions for this study, I performed a field test of the questions prior to the actual interviews. I went into the field and interviewed three individuals who had "expert knowledge about the population and research topic to provide feedback on the appropriateness of the questions being asked and how the questions are being asked in relation to the study focus" ("Field Testing," 2016). These experts helped me refine the interview questions and develop appropriate follow up questions, inviting more conversation along a similar line of thought ("Field Testing," 2016). The interview questions are closely linked to this study's research questions.

Purposeful sampling was utilized for this study. Individuals that had the depth of knowledge necessary to clearly articulate how threat-related information is analyzed and shared between public safety agencies in Honolulu, Hawaii, were selected. All of the participants had at least 15 years of experience sharing information between public safety organizations. Individuals who had recently retired were also included in the study, if they met the selection criteria. There were three primary reasons to include this group in the sampling criterion. First, all of the participants had extensive experience in their

respective fields of public safety. Second, because they were no longer associated with the organizations there was no political pressure on them to answer the questions in a politically sensitive manor. Third, this research was an opportunity to capture extensive institutional knowledge from retired public safety SMEs before the knowledge was lost forever.

The primary purpose was to explore communication across agencies and examine the benefits and challenges of sharing threat related information between public safety agencies in Hawaii. The individuals selected were a part of the culture of these organizations and knew the social dynamics of each agency. Patton (2002) points out, "qualitative inquiry typically focuses in depth on relatively small samples, even single cases (N=1), selected purposely" (p.230). It was important to select participants that had a rich knowledge of their environment in order to build a quality research data set. Patton explained, "The logic and power of purposeful sampling lie in selecting information-rich cases for study in depth" (p.230). This process allows a thorough understanding of the information in context.

The sample for this study was a subset of SMEs from the larger population within four fields of public safety that had extensive experience analyzing and sharing threat-related information between agencies. One gap that we see in sharing of threat-related information is who is included and how do we involve public health (Hospitals, CDC, etc.) in the process. I included agencies that had representatives assigned to the Hawaii State Fusion Center, because these are the organizations that are active during an event. The larger population currently consists of less than 50 SME's, who work within the

local public safety organizations and actively share threat-related information between agencies. For purposes of anonymity, three SMEs were selected from each of four fields. All individuals had at least 15 years' experience. It would not have been feasible to interview every member of the entire population for this study.

Purposeful sampling was utilized for this study. I identified SMEs in each of the four fields of public safety in Honolulu. Participants for the study were determined based on whether or not they met the inclusion criteria. Approximately three individuals from each field of public safety were interviewed, resulting in 13 cases, which was adequate for the study. This number of case interviews provided a clear understanding of the benefits and challenges associated with sharing threat-related information.

Each SME was contacted one month prior to the interview and the purpose of the study was explained. An email inviting them to participate in the study was mailed along with a consent form which was completed and returned to the researcher via email. The participants were contacted again by email prior to the interview to confirm a mutually agreed upon interview date and time. Each participant was given the choice to be interviewed via teleconference, the participants private residence, or a private meeting room at the Hawaii Public Library. The interviews were conducted outside of regular work hours. The researcher was the only person who knew the identity of the participants and did not disclose their names. Demographic details and site descriptions that might permit a reader to deduce the identity of a participant were withheld. Participants names and/or contact info was not recorded in the research records. During the interview phase of data collection, a review of the consent form was offered to ensure that the participants

were aware of the entire interview procedure. Consent forms did not require signatures if the participant indicated consent by returning a completed form via email with an identifying number.

In order to capture accurate information for a qualitative data set, I utilized voice recordings along with field notes. The answers were transcribed into written text and NVivo qualitative analysis software was used for data coding. The purpose of coding was to allow themes to emerge from the data that made sense to the researcher. I used a coding strategy that consisted of reading through all of the transcripts to gain a deep understanding of what took place during the interviews, while simultaneously reviewing my written notes. I then classified the data by "aggregating text into small categories of information" and then assigning an appropriate label (Creswell, 2013, p.184). Lastly, I separated all of the codes into four or five overarching themes that I referenced while writing my discussion of the data. A more thorough explanation of the methodology is presented in Chapter 3.

Operational Definitions

Centers of Excellence: "A team, a shared facility or an entity that provides leadership, evangelization, best practices, research, support and/or training for a focus area" ("Inquvent," 2013, para. 1).

Counterintelligence: An "organized activity of an intelligence service designed to block an enemy's sources of information, to deceive the enemy, to prevent sabotage, and to gather political and military information" ("Counterintelligence," n.d., para. 1).

Fusion center: Units that are located in every state in the nation and that "serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners" ("Homeland Security," 2014, para. 1).

General systems theory: "Systems theory was proposed in the 1936 by the biologist Ludwig von Bertalanffy, and further developed by Ross Ashby. Von Bertalanffy emphasized that real systems are open to, and interact with, their environments, and that they can acquire qualitatively new properties through emergence, resulting in continual evolution" ("General Systems Theory," 2014, para. 5).

Intelligence analyst: An analyst whose primary role is "intelligence collecting, evaluating and processing personnel" ("Federal Bureau of Investigation," 2015, para. 1). These positions "may involve gathering information from a variety of channels, including human intelligence, other intelligence agencies, electronic and Internet surveillance, interrogations, and criminal investigations" ("Federal Bureau of Investigation," 2015, para. 1).

Intelligence Community: "A group of government agencies and organizations that carry out intelligence activities for the United States government; headed by the Director of Central Intelligence" ("United States Intelligence," 2015, para. 1).

Open source intelligence (OSINT): Information utilized by the military, public safety, or the nation's intelligence community that is publicly available to anyone. This important data source "plays an essential role in giving the national security community

as a whole insight and context at a relatively low cost" ("Intelligence: Open Source," 2013, para.1).

Open Source Center: A government unit, operated by the Office of the Director of National Intelligence (ODNI), that is the "focal point for the intelligence community's exploitation of open source material. It also aims to promote the acquisition, procurement, analysis, and dissemination of open source information, products and services throughout the U.S. Government" ("Aftergood," 2014, para. 1).

Public safety: The primary responsibility is to protect the public from harm. It is often used in the context of a government organization that has a mission to provide protection to the general public from dangerous natural and/or manmade events. Organizations such as law enforcement, fire services, EMS, and public health agencies fall into this category ("Public Safety," 2016, para. 1).

Situational awareness: As defined by the United States Coast Guard, "the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission. More simply, it is the practice of knowing what is going on around you" ("United States Coast Guard," 1998, para. 1).

Threat-related information: Information that indicates a potential risk related to "an approaching or imminent menace; [a] negative event that can cause a risk to become a loss; … [or] a natural phenomenon such as an earthquake, flood, storm, or a man-made incident such as fire, power failure, sabotage, etc." ("Threat," 2017, para. 1).

Assumptions

For this academic research study, the following assumptions were made. It was assumed that the individuals from four fields of public safety in Honolulu had been appropriately trained in analyzing and sharing threat-related information. It was also assumed that each respondent would answer the questions to the best of their ability. It is important that the participants relay their personal experience working with threat-related information within the standard operating procedures established by their organization. It was assumed that the interviews followed the guidelines of Walden University and that the recordings made during the interview accurately represented the interview session.

Scope and Delimitations

The sample selection for this study focused on four fields of public safety in Honolulu, Hawaii. This study purposely did not collect information from across the entire nation, as the enormous dataset would be unmanageable. Fugard & Potts, (2015), point out that qualitative research sample size should be "small enough to manage the material and large enough" to allow a thorough understanding of the participants experience (p.670; Sandelowski, 1995).

The intent and design were to capture the experiences of SMEs in public safety within a particular region. Individuals who had at least 15 years' experience sharing threat-related information between public safety organizations in Honolulu were the participants. Individuals recently retired were selected if they met the research study selection criteria. Because these individuals were no longer associated with their organizations there was no political pressure on them to answer the questions in a

politically sensitive manor. This research was also an opportunity to capture extensive institutional knowledge from retired public safety SMEs before the knowledge was lost. This study will help fill a gap in the literature by determining the perceived benefits and challenges of sharing of threat-related information between public safety organizations in Honolulu, Hawaii.

Limitations

Limitations were present during the data collection process. Because the SMEs often worked with sensitive information, they were asked to keep the content of their conversations at the non-sensitive level. They were asked to speak openly and candidly, while at the same time not disclosing confidential material. During the interviews, the participants were very cautious when discussing internal agency issues and did not to disclose sensitive or otherwise confidential information.

Significance

The significance of this study was to determine the benefits and challenges of sharing threat-related information between public safety organizations in order to better protect the population. The research will advance the knowledge of prior published literature on information sharing between public safety organizations.

Some of the most successful defense organizations utilize information sharing as a key tactical component. Modern security practices “are built around the concept of fusion,” or sharing of information (Kalu, 2009, p.34). A continuous learning strategy combined with effective information flow between security agencies can significantly reduce the odds of an attack (Kalu, 2009).

It is inevitable that public safety officials will increasingly become more involved in open source and social media data analysis processes. This study will shed light on how effective information exchange can assist public safety agencies with future terrorism challenges.

Implications for Social Change

Sharing the results of this study will create positive social change by identifying the benefits and challenges of sharing threat-related information between local public safety agencies. As public safety organizations throughout the nation develop their ability to share threat-related information, they should review lessons learned from organizations examined in this study that have faced this important and complex undertaking. Horrific events such as the Boston marathon bombing (Hu et al., 2014), the Paris attacks ("BBC News," 2105), and the assault on an Orlando, Florida nightclub (Ellis, Fantz, Karimi, & McLaughlin, 2016), are a stark reminder that individuals with aspirations of domestic terrorism can be readily recruited and trained to carryout violent acts. Organizations with the responsibility for public safety must adapt to a new asymmetrical threat environment through improved domestic intelligence. With violent extremist organizations now able to communicate and recruit followers via the Internet, it is even more critical to monitor all available communication sources and share threat-related information between public safety organizations.

Summary

Public safety organizations are forming relationships and working in a collaborative manor to address the social phenomenon of terrorism and violent

extremism. However, more work needs to be done to ensure that threat-related information is shared seamlessly between all organizations that have a responsibility to keep the public safe.

The findings of this study will help to fill a gap in literature by determining the benefits and challenges of information sharing between public safety organizations. The purpose of this research was to explore the benefits and challenges of sharing threat-related information between public safety organizations (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii. The proliferation of the Internet and global communication along with the rise of violent extremism has brought together a new and dangerous phenomenon. This research will help to identify benefits and challenges of sharing threat-related information between public safety agencies in a mid-sized metropolitan city and what can be done to improve this information exchange.

Qualitative design was determined appropriate to explore the responses to the unique set of research questions for this study. General systems theory was utilized as the conceptual framework for the study. The findings of this research may assist other agencies across the nation share threat-related information in a more effective manner. Chapter 2 will review the pertinent literature related to the topic.

Chapter 2: Literature Review

Public safety organizations across the United States are engaged in the process of enhancing their open source information collection capabilities. At the same time the information revolution is growing at a rapid pace. It is crucial that public safety organizations keep up with the current pace of technology. Local public safety agencies often face challenges in using technology to share threat-related information that are specific to their individual organizations. Information sharing in today's environment is complex and dynamic and public safety organizations must employ individuals who understand the latest communication technology (Kozuch & Sienkiewicz-Malyjurek, 2015). The primary purpose of this research was to examine the benefits and challenges of sharing threat-related information between public safety organizations in Honolulu, Hawaii.

Individuals throughout the world now have the ability to communicate on multiple platforms in real-time. Complex media such as high-resolution video and images can be sent instantly around the globe. Communication techniques that were once expensive and complex are now available to anyone with a smart phone. According to Boczkowski, Matassi, and Mitchelstein (2018), a recent survey indicated that "98% of those between 18- and 29-years-old used social media and accessed 3.5 platforms on average" (p. 250) Terrorist organizations exploit these technology innovations to expand their global footprint (Cohn, 2013).

Pivotal information relating to situational awareness and threat identification resides in open source information and social media. Recent geopolitical events across the

world have been shaped in part through social media. In the recent political unrest exhibited during the 2010-2011 Arab spring, for instance, major protests in the streets were often proceeded by heated conversations of political unrest online (Howard et al., 2011, p. 3). In Egypt and Tunisia, protest organizers used social media extensively to connect with activists. Frequently, these online political conversations were picked up by news media outlets which spread the information regionally (Howard et al., 2011, p.3).

In the 21st century, not only are digital technologies evolving at an accelerated rate, but historical evidence also illustrates "a larger trend of ever-more-rapid adoption of new technologies" (Desilver, 2014, p. 2). These global events illustrate why it is important that domestic public safety organizations monitor and share open source information. A thorough review of the literature on the topic helps to better define the problem and the purpose of this research. By carefully reviewing the available information, I was able to determine the current relevance of the research problem. Reviewing the literature also helped to bring into context the importance of monitoring and sharing threat-related information between public safety organizations. The first major theme in the literature was benefits of sharing threat-related information, the second was fusion center facilitation of information sharing between public safety agencies, the third was challenges of sharing threat-related information, and the fourth was social media use between public safety agencies. I also discuss the Literature Search Strategy and Conceptual Framework in this chapter.

Literature Search Strategy

Library databases and search engines used in this research study included Homeland Security Digital Library, Sage Journals, EBSCOhost, Taylor Francis Online, PubMed, ProQuest Central. Database searches were conducted in the Walden University online library. Key information sharing websites were also used in this study including the Justice Information Sharing, and International Relations and Security Networks. Key search terms used in the research process included *policy*, *open source*, *open source center*, *social media, fusion centers*, *national security*, *network fusion*, *counterterrorism*, *interoperability*, *intelligence*, *counterintelligence*, *intelligence community*, *national intelligence*, *homeland security*, *information sharing*, *law enforcement*, *public safety*, and *public health.* I placed date restrictions on the database searches to ensure that the majority of the information had been published within the past 5 years. I also restricted the language to documents published in English.

The reference lists of the articles I selected were reviewed in order to locate other sources of data pertaining to my topic. I reviewed over 200 documents during the literature review process including books, peer reviewed journal articles, official government publications and websites, trade publications, and media sources that I deemed credible. I found over 80 documents that were relevant for this research. The major themes in the literature were benefits of sharing threat-related information, fusion centers facilitation of information sharing between public safety agencies, challenges of sharing threat-related

information, and social media use between public safety agencies. The results of the literature review are discussed in more detail in the "Literature Review" section later in this chapter.

Conceptual Framework

I used general systems theory ("General Systems Theory," 2014) as the conceptual framework for this research. I selected this theory because it offered the best description of how public safety organizations share threat-related information to protect the population from terrorist attacks. General systems theory also provided the best framework for responding to the research questions for this study. Researchers have used general systems theory for several decades to study both domestic and international politics (Tierney, 1972). General systems theory is useful when studying the organizational changes and development of a community's public safety system by analyzing the interconnection between individual agencies or subsystems. Elements in systems are consistently interacting with one another. A change in one area of a system results in changes in another area of the system ("Communication Theories," 2019).

In the article entitled, "Surveillance and Resilience in Theory and Practice," Raab, Jones, and SzJones (2015), pointed out that "a system may not only react to environmental effects by changing its internal properties or organization, but also act on and change its environment, bringing about a new relationship or a new equilibrium" (p. 26). General systems framework is effective in illuminating complex collaborative relationships between public safety organizations in dynamic, rapidly changing environments. Systems are essentially a set of objects, or variables "that affect one

another within an environment and form a larger pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). William et al., (2006) pointed out that within the U.S. public health industry there is growing awareness and acceptance of systems thinking.

In conducting this research, I sought to build upon the knowledge base of research regarding how general systems theory is currently utilized within modern government organizations. Von Bertalanffy first proposed general systems theory in the 1930s and the theory was furthered by Ross Ashby in the mid 1960s ("General Systems Theory," 2014). Von Bertalanffy stated that systems are "a set of things that affect one another within an environment and form a larger pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). Because elements in systems are constantly interacting with one another, when one area of a system undergoes change it subsequently results in change somewhere else in the system ("Communication Theories," 2019). Thus, as public safety organizations within the same region share relevant threat-related information with one another, other agencies within that region are prompted to prepare for or counter the possible threat. When public safety analysts are able to monitor the Internet and social media for terms, phrases, and threat-related situations, they are able better identify and prevent threats to the community (Chermak et al., 2013).

The sharing of threat-related information between public safety organizations is vital to improving law enforcement's ability to uncover and stop violent attacks before they occur. Analysts at public safety organizations throughout the U.S. have the

capability to research and analyze multiple forms of information from all regions of the nation, fusing local and national threat information together to uncover possible threats. As public safety analysts collect and analyze information from multiple sources, they pass threat-related information to local fusion centers. The information is then passed up to the federal government which in turn shares it at the top level of the nation's intelligence structure, adds additional threat data from federal sources, and then passes the information to local fusion centers and then finally back to local public safety organizations. This circular information sharing, and collaboration process helps to make the nation safer overall.

Systems are essentially a set of objects, or variables "that affect one another within an environment and form a larger pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). When public safety organizations within the same region share relevant threat information with one another, it prompts other agencies within that region to prepare for, or possibly counter the threat. As geopolitical situations evolve and develop, organizations with the responsibility for public safety must adapt to a new asymmetrical threat environment through improved domestic intelligence. State and local fusion centers are currently in a position to take on an expanding role in the nation's domestic security by helping to protect the public from violent attacks.

Literature Review

Threat-related open source information is a key resource for public safety organizations. Therefore, it is important that SMEs from multiple fields, including law enforcement, public health, EMS, and fire services work together toward the common

goal of sharing threat-related information between agencies. Lenart, Albanese, Halstead, Schlegelmilch, and Paturas (2012) explain, “fusion centers must employ people with the necessary competencies to understand the nature of the threat facing a community, discriminate between important information and irrelevant or merely interesting facts and apply domain knowledge to interpret the results to obviate or reduce the existing danger” (p. 174). The overarching goal of fusion centers is to share information between local public safety organizations, as well as ensure that vital threat-related information uncovered at the local level is passed up to federal government officials (Stone, 2015).

The studies and articles chosen for this literature review are within the scope of the research study. They represent the knowledge currently available on how public safety organizations across the nation analyze and share threat-related information. The literature was reviewed and then synthesized to bring to light observable trends in threat-related information sharing across multiple public safety organizations. The phenomena were described from the unique viewpoints of the individual organizations. This approach to the literature review process related back to the research questions posed for this study. The major themes in the literature were benefits of sharing threat-related information, fusion centers facilitation of information sharing between public safety agencies, challenges of sharing threat-related information, and social media use between public safety agencies.

Benefits of Sharing Threat-Related Information

Public safety systems are large and complex, involving large numbers of highly trained professionals interacting with members of multiple organizations and the general

public on a continual basis. Kozuch and Sienkiewicz-Malyjurek (2015) pointed out, “The process of information sharing in complex systems is multi-dimensional, asymmetrical and dynamic” (p.727). It involves numerous organizations within local public safety systems communicating effectively on multiple levels to deliver accurate information to first responders when needed. Currently, law enforcement, fire services, and emergency medical organizations communicate with one another effectively via 911 emergency dispatch centers to route needed resources where they are needed during emergencies.

Many public safety organizations across the nation also share information through fusion centers, emergency management agencies, and other associations developed specifically to improve coordination and information exchange. This information exchange occurs in various forms depending on the organizations involved and the interagency communication structure of the local municipalities. Coordination must be facilitated from the leadership level of the organization down through the chain of command to generate an ongoing exchange of useful information.

Health and medical integration into an information sharing environment. Health and medical issues are extremely important to the safety of the public, and many public safety organizations integrate medical analysts into their analytical staff (Carter & Rip, 2013). A primary responsibility of health analysts is to build relationships among medical partners to quickly identify dangerous substances such as chemical or biological agents. This capability relies not only on highly trained technicians in the field with the proper equipment, but also the reach-back capability to certified health laboratories within the region. These unique health laboratories can make an affirmative identification

of dangerous biological or chemical substances. Whether the threats are natural or man-made this important aspect of surveillance must not be overlooked.

Highly trained medical professionals can quickly determine which important health information should be disseminated to the public in an emergency (Carter & Rip, 2013). Utilizing medical analysts is an effective way of validating and correctly determining true medical threats in an emergency. Lenart et al., (2012) pointed out the "ability to respond effectively to threats or events that place the country at risk is greatly enhanced when collection, analysis, synthesis and dissemination of public health and medical information and intelligence are included in the national network of anti-terrorism fusion centers" (p. 175).

Information sharing between the health community and law enforcement organizations is a complex undertaking. As public safety information sharing evolves through the utilization of state fusion centers, public health and medical support is becoming a necessity. Lenart et al., (2012) explained, the process of "conferring appropriate security clearances to public health and medical personnel, as well as policies for ensuring patient confidentiality" are extremely important issues that must be addressed as information sharing between public safety organizations increases (p. 175).

Carter and Rip (2012) pointed out that the U.S. Department of Health and Human Services (HHS) and the U.S. Department of Homeland Security (DHS) work collaboratively facilitating important public health information into fusion center operations. Multiple grants have been awarded through the National Institute of Justice to ensure that public health analysts work side-by-side first responders to protect the

nation's population. As fusion centers find their footing as an important addition to the nation's intelligence community, public health may be the next logical edition to this public safety effort.

The U.S. Centers for Disease Control and Prevention (CDC) and the DHS are currently developing policy to work more closely together. Sharing of information throughout law-enforcement, public safety, and public health are a primary reason for the facilitation of fusion centers nationwide. Carter and Rip (2012) explained, "Since September 11, 2011, a significant amount of progress has been made to improve information collection and sharing in both the public health and homeland security sectors in their own rights" (p.574).

Carter and Rip (2012) argued that although significant efforts have been initiated, federal, state, and local environments still do not effectively share information nationally. One problem, which has been highlighted nationally is that public health has not typically been a part of law enforcement activities. Carter and Rip contend, with the development of threat-related information sharing on a national scale, public health should be integrated into the collaborative. Fusion centers were developed to share information between all levels of public safety sectors, so integrating public health into the public safety matrix is an important national agenda item.

National security and public health integration have had a long history. Since the creation of chemical weapons in World War I, there has been a need for medical personnel trained and capable of effectively detecting these dangerous weapons, both in military and civilian operating environments. After the attacks of 9/11, there was

considerable concern that terrorist organizations around the globe could launch a chemical or biological attack on an American city. Therefore, public health SMEs were recruited into the security apparatus of the nation, as equal partners in the fight against terrorism. As more research has been completed on exotic weapons that could affect our nation's bio surveillance of both human and animal disease, threat identification has become extremely valuable. A terrorist attack on the nation's agriculture or livestock could be devastating to the U.S. economy.

In order to keep a robust situational awareness, intelligence personnel have consistently welcomed the participation of highly trained medical staff. After the attacks of 9/11, a significant national security priority was placed upon identifying chemical and biological attacks. Within Homeland Security, the Office of Health Affairs (OHA) holds the principal responsibility for health issues, while the National Biosurveillance Integration Center (NBIC) has the primary responsibility to monitor heath related threats to the population (Carter & Rip, 2012).

Carter and Rip (2012) pointed out that the DHS is responsible for responding to chemical, biological, radiological, nuclear, and explosive (CBRNE) events. However, HHS coordinates all health emergency response activities. Carter and Rip explained, "the CDC within USDHHS created a surveillance mechanism known as BioSense 2.0, which is currently the only nation-wide all-hazards emergency public health surveillance system" (p. 577). With these efforts, first responders must responsible for isolating and identifying not only man-made bioterrorism, but also natural disease epidemics that occur throughout the world which have the capability to threaten the U.S. population.

Involvement of private organizations in an information sharing environment. Taylor and Russell (2011) argued since the attacks of 911 there are now hundreds of government and private organizations involved in homeland security and intelligence collection activities. They pointed out, before the attacks sharing of intelligence between police departments and public safety agencies was severely lacking (Taylor & Russell, 2011, p. 184). Currently however, public safety agencies throughout the nation are beginning to participate in the nationwide network of fusion centers in an effort to better protect the public.

The DHS has invested millions of dollars toward improving the coordination of police departments to share criminal and threat related information (Jackson & Brown, 2007). A mix of crime analysis, intelligence, and open source information may finally be a formula for fusion centers success. Taylor and Russell (2011) explained, "The strategic integration of intelligence, with an emphasis on predictive analysis derived from the discovery of hard facts, information, patterns, and good crime analysis defines intelligence led policing (ILP)" (p. 185). Relying solidly on information technology, intelligence led policing may help combat crime by significantly increasing intelligence decision making (Bharosa, Lee, & Janssen, 2010).

Taylor and Russell (2011) explained that sophisticated computer programs and competent analysis align hand-in-hand with grassroots relationships with the public. As this wealth of information is derived from on-going police operations it is compiled into fusion databases, which "serve as hubs for information on crime and terrorist operations in a specific region focusing on the recognition of patterns, indications and warnings,

source development, interdiction, and coordination of critical criminal justice resources" (Taylor & Russell, 2011, p. 185). All of this collective analysis and processing of important data focuses on the ability of analysts to help uncover terrorist plots in the early stages of development before they become deadly terrorist attacks.

Vital information that is collected and processed on the streets of the nation's cities is now passed up to the "National Counter Terrorism Center in Washington, DC for a coordinated response to potential threats" (Taylor & Russell, 2011, p.85). However, problems inherent in local police departments and other public safety agencies may plague the effectiveness of this fusion process. Taylor and Russell (2011) argued, "The structure and mission of law enforcement agencies undermines the very essence of fusion centers as well as what they are intended to do and who they are intended to protect" (p.185).

Shepherd (2011) explained that although our world is inundated with communication platforms that the public uses every day, there continues to be a disconnect between public and private sharing of information when it pertains to terrorism surveillance. Shortly after the attacks of September 11th, the 9/11 Commission pointed to a series of suggestions that if implemented would better protect the nation. Shepherd indicated that incentives should be cultivated to bring about a fundamental public and private cooperation toward national security issues. He explained that fusion centers can be the conduit that effectively moves information simultaneously between public and private organizations.

The federal government has long maintained that the private sector owns or operates most of the key resources within the nation; therefore, it is crucial that government security organizations actively engage the private sector in security operations. Shepherd (2011) pointed out "The U.S. Department of Homeland Security (DHS) maintains the Commercial Facilities Sector Coordinating Council (CFSCC)," which represents "more than 100 different associations across an open access market" (p. 36). Because all of these organizations come from different backgrounds and have different business models, the information provided by the CFSCC can be used differently by each organization.

Shepherd (2011) explained that the benefits of fusion centers extend far beyond law-enforcement and security concerns into public safety, public health, and emergency management. A few of the benefits of this information sharing include terrorism and public safety training in a modern technologically advanced fusion center facility. An increased situational awareness during any type of hazard, whether it be man-made or natural, as well as an increased partnership with private organizations better protects the population from a wide spectrum of threats.

One area of the nation that has succeeded in expanding the fusion center's role within the public sector is the Southern Nevada Counterterrorism Center (SNCTC) located within the greater Las Vegas area. Sheppard (2011) explained, "blending data from different sources, including law enforcement, public safety, and the private sector, with analysis, can result in meaningful and actionable intelligence and information that goes a long way in protecting a community against acts of terrorism" (p. 36). The

SNCTC management understands that the "private sector is a valuable asset to the fusion center and is a legitimate recipient of law enforcement intelligence due to their national and international operations, and the preponderance of private sector ownership of critical infrastructure and key resources of the United States" (Sheppard, 2011, p.37).

Centers such as the SNCTC can possibly fill a gap in the nation's security and emergency preparedness. They have the ability to augment law enforcement, private security, and public safety all from a within one consolidated facility. Innovative fusion center directors can also expand their information exchange value by creating public safety training facilities. Additionally, integrating public/private cooperation into fusion center operations will create one facility that can provide multiple layers of protection for large urban areas.

Integration of public safety organizations into an information sharing environment. The DHS works with local public safety organizations to establish fusion liaison officer (FLO) programs, which allow fusion centers to recruit and train individuals from various public safety organizations to act as extensions of the fusion program. FLOs work with police departments, fire departments, and EMS organizations to report important threat information back to fusion center analysts as needed. They are not assigned full-time to fusion centers but work as a supportive counterpart of the fusion center process.

According to the DHS, fusion center initiatives include three interrelated critical focus areas, "better understand the phenomenon of violent extremism, and assess the threat it poses to the nation as a whole and within specific communities; Bolster efforts to

address the dynamics of violent extremism, and strengthen relationships with communities as they play a vital role in countering violent extremism; Expand support for information-driven, community-oriented policing efforts that have proved effective in preventing violent crime across the nation" ("The Role of Fusion Centers," 2012, para. 10). Public safety officials rely on various types of public engagement. Primarily, analysts encourage an open discussion of violent extremism in communities and promptly address any questions concerning extremist actions ("The Role of Fusion Centers," 2012). Analysts also work closely with first responders to identify "behaviors that are potentially indicative of terrorist or other criminal activity, raise public awareness of indicators of terrorism and violent crime, and emphasize the importance of reporting suspicious activity to the proper law enforcement authorities" ("The Role of Fusion Centers," 2012, para. 10). This particular initiative builds a cooperative trust between the public safety responders and fusion center analysts. An important and unique component of the public safety community also includes various health and medical organizations.

Fusion Center Facilitation of Information Sharing

State and local fusion centers are staffed primarily with representatives from federal, state, local, tribal, and private partners ("State and Major Urban," 2014). According to the DHS, the government has invested significant federal funding to ensure that fusion centers are engaged in national security ("State and Major Urban," 2014). With international terrorism threatening our nation's security, public safety professionals will increasingly engage in the fight against terrorism. By integrating fusion centers into

the government's intelligence community, DHS hopes to identify terrorist threats at the earliest opportunity rather than waiting until terrorist cells become operational.

The focus of this process relies on collaboration with local public safety organizations. It is a slow process of building relationships so that terrorist activity information can begin flowing from the field operations level up. DHS officials believe that this direct contribution of information from local communities throughout the country will lead to a series of successes in the future. The current U.S. National Security Strategy states, "the federal government must continue to integrate and leverage fusion centers to enlist all of our intelligence, law enforcement, and homeland security capabilities to prevent acts of terrorism on American soil" ("State and Major Urban," 2014, para. 5).

The federal government published guidance in 2003 that was designed to help fusion centers develop their capabilities to a baseline functional level across the nation. These baseline proficiencies are designed to ensure that all fusion centers nationwide can operate in an effective information sharing environment. The capabilities are built upon tested methodologies, such as the intelligence cycle used in the nation's IC. The FBI points out, "the intelligence cycle is the process of developing unrefined data into polished intelligence for the use of policymakers" ("Intelligence Cycle," 2010, para. 1). Using these standard methodologies allows state and local public safety analysts to communicate effectively with analysts within all levels of the federal government. This nationwide "strategic vision can be realized only when fusion centers demonstrate institutionalized levels of capability that enable efficient and effective information

sharing and analysis across the national network" ("State and Major Urban," 2014, para. 6).

Baseline of common information analysis competencies. The DHS believes that a baseline of information analysis competencies will improve the nation's ability to take on the threat of asymmetrical terrorist activity. In an effort to expedite this process, DHS has initiated an expansive set of technical training courses for local public safety analysts. DHS states, "through its long-standing partnership with the Department of Justice (DOJ), the Department has conducted more than 300 training and technical assistance deliveries, workshops, and exchanges on topics including risk analysis, security, and privacy, civil rights, and civil liberties since 2007" ("State and Major Urban," 2014, para. 7).

The DHS has also established a nationwide yearly assessment of fusion centers throughout the nation in an effort to ensure that public safety personnel are performing at excepted levels. Four critical operational capabilities (COCs) are tracked including the fusion centers ability to "receive, analyze, disseminate, and gather" information ("State and Major Urban," 2014, para. 11). Several capabilities including "privacy/civil rights and civil liberties protections, sustainment strategy, communications and outreach, and security" are tracked in the assessment ("State and Major Urban," 2014, para. 11). Through this ongoing evaluation process, gaps are identified and corrected in a timely manner. The overarching goal of the program is to develop analytical centers of excellence throughout the nation that are effective at sharing threat-related information.

Increasing analytical standards. State fusion centers that achieve a high level of analysis competence are proudly acknowledged as centers of analytic excellence. These organizations have made great strides towards analytical excellence. Abold, Guidetti, and Keyer (2012) pointed out, “This is a significant departure from the sense in which this term has been used previously and provides a next state for individual fusion centers that aspire to share their analytic competencies across a national network” (p.1).

Public safety analysts working in fusion centers across the nation are finally reaching their goal of becoming true analytical centers. Just as in the nation's intelligence community different agencies perform different functions, which helps to significantly strengthen the collective. Abold et al. (2012), explained that this push toward specialized expertise that will help to build a larger more reliable network. Over the last decade public safety analysts assigned to state fusion centers have worked diligently to increase collaboration, as well as a sense of comradely between centers.

In 2008, DHS in collaboration with the FBI developed a document entitled, *Baseline Capabilities for State and Major Urban Area Fusion Centers*. A portion of the document highlighted “capabilities determined necessary to achieve a national, integrated network of fusion centers and detailed the standards necessary for a fusion center to be considered capable of performing basic functions by the fusion center community” (“Information Sharing,” 2014, p.8). Since that time, many fusion centers across the nation have worked vehemently to not only meet those standards, but to surpass them. As noted earlier, “With the best practices of the IC (Intelligence Community) as a model for

success, one could argue that the same attribute of specialization should be extended to the network of fusion centers" (Abold et al., 2012, p.2).

This focused development of fusion centers of analytical excellence would help to increase the nation's ability to counter domestic threats. These locally owned and operated multi-agency organizations' primary responsibility is to receive, analyze, and disseminate information from multiple sources. Regardless of where the information originates, the primary function should be to assist in the coordinated situational awareness of public safety response agencies.

The idea of this information-sharing network originated from the horrific events of 9/11. Soon after the infamous disaster, it was determined that information sharing between state and local public safety organizations was severely lacking ("National Commission," 2004). Consequently, fusion centers were tasked to develop vital communication links between public safety organizations throughout the nation. The 9/11 tragedies rallied a "diverse group of centers not only around a common cause of securing the homeland but also around a common framework for communicating and doing business" (Abold et al., 2012, p.2). The development of fusion centers of excellence is an effort by the government to better protect the nation from both domestic and international threats. Abold et al., stress that it is imperative that individual fusion centers continue to develop their unique set of analytical expertise as this rigor and precision will "greatly benefit the overall capability of the national network" (p.15).

Protecting the public from terrorism. An atmosphere of effective information exchange is essential in the current asymmetrical threat environment. The DHS emphasizes that "fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities" ("State and Major," 2014, para. 2). Effective information sharing can provide situational awareness to decision makers at the state level through collaboration with their federal partners. Although federal agencies support the centers, they are operated solely by the states in which they reside. Federal entities primary focus is to support operations and assist when needed. Federal funding is also available to support infrastructure and personnel costs ("Federal Emergency Management Agency," 2015). Security clearances and a full range of security issues have been initiated to train local public safety analysts to operate in an information sharing environment. The DHS clearly states that threats to our nation have changed dramatically since enemies abroad transitioned to asymmetrical tactics. Therefore, the nation's defensive capabilities must change to meet the threat.

It is highly anticipated that threat-related information sharing will assist both local and federal law enforcement by uncovering terrorist plots across the nation ("State and Major," 2014). The DHS projects, through federal, state, local and private partner collaboration that public safety analysts will have the capability to "gather and share the information necessary to pursue and disrupt activities that may be indicators of, or potential precursors to, terrorist activity" ("State and Major," 2014, para. 4). The attacks

of 9/11 marked a turning point in national security and many policy makers began stressing the importance of sharing threat-related information between all government agencies to protect the nation abroad and at home. As terrorism grows globally it also initiates incidents of homegrown violent extremism.

Countering domestic violent extremism. In a government publication entitled *The Role of Fusion Centers in Countering Violent Extremism* DHS states, "as analytic hubs, fusion centers are uniquely situated to empower frontline personnel to understand the local implications of national intelligence by tailoring national threat information into a local context and helping frontline personnel understand terrorist and criminal threats they could encounter in the field, while also protecting the privacy, civil rights, and civil liberties of individuals in their communities" ("The Role of Fusion Centers," 2012, para.1).

Public safety analysts across the nation work with federal agencies in a collaborative information-sharing environment to ensure that local public officials are aware of any terrorist activities, violent extremism, or organized crime in the area. The DHS has invested a significant amount of funding to ensure that public safety analysts are trained to meet predetermined analytic guidelines. This assists in "building grassroots intelligence and analytic capabilities within the state and local environment so state and local partners can understand the local implications of national intelligence by tailoring national threat information into a local context" ("The Role of Fusion Centers," 2012, para. 2). In order to achieve effective situational awareness, all components of the public safety community must be involved in the information sharing process. The sharing of threat-

related information between public safety organizations also involves many challenges. The following chapters will highlight many of these challenges, as well as touch upon lessons learned from sharing information throughout the intelligence community.

Challenges of Sharing Threat-Related Information

Throughout history great military leaders, including Civil War commander Ulysses S. Grant, realized that publicly available open source information was extremely valuable and should be collected and analyzed order to better understand the enemy (Steele, 2008). During the Cold War, the Union of Soviet Socialist Republics (USSR) was America's primary adversary. As a result, the U.S. military relied on classified intelligence collection methods to monitor the soviets. It is now evident that classified collection capabilities may not be the most effective means to gather information on the nation's enemies. Many government reviews of our nation's intelligence community (IC) have experienced "America's deficiencies in foreign languages and, to one extent or another, the open sources they represent; and every single President, Secretary, and Director of Central Intelligence has seen fit to ignore these concerns, persisting with the understandable but necessarily erroneous view that the U.S. Intelligence Community is in the business of finding and delivering secrets for the President" (Steele, 2008, p. 610).

Open source information. Steele (2008) explained that CIA officials believe that open source intelligence (OSINT) provides approximately 80 percent of the useful information utilized by the IC. The U.S. spends a significant amount of resources on classified information and only a small percentage of that on OSINT. Steele argued, "the return on investment (RoI) implications—of spending next to nothing on that 80 percent, while

spending tens of billions of dollars on secret collection, most of it technological, yet not having any single place where both secrets and non-secrets could be processed coherently and with all available automated tools" (Steele, 2008, p. 610). During the 1990s, there were several instances where proponents for OSINT lobbied Congress to approve funding for a robust OSINT program. However, in all instances funding for open source information never became a priority. Steele declared the consequences for the lack of funding for OSINT "including our lack of awareness of the open spread of virulent Islam, in radicalized schoolhouses funded by Saudi Arabia from 1988 to 2001, continue to cost the United States blood, treasure, and spirit" (p.612).

Steele (2008) went on to explain that open source information is not something that can be controlled by the intelligence community. It is something that flows freely from the Internet and social communication. He indicated that no one source can control its dissemination; therefore, because of its distributive nature, it must be shared between government and private organizations. In 2005 the federal government developed a national center devoted predominantly to processing open source information.

United States national intelligence. This U.S. government's primary source of open source information is the Open Source Center (OSC) located just outside of Washington, DC. This modern facility, established in 2005 by the Office of the Director of National Intelligence (ODNI), helped to transform the nation's IC toward accepting open source information as a legitimate intelligence resource. The acceptance of OSINT was accelerated by the rapid rise of radical Islamist attacks throughout the world. These

emerging new paramilitary organizations had become adept at using the Internet and social media to rally followers and plan attacks. With a single act of Congress entitled the "*Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), which President Bush signed into law on December 17," the 16 agencies that made up the nation's IC became 17 ("Office of the Director of National Intelligence," 2004).

For decades, the IC struggled with how to effectively utilize open source information. This distinctive information did not quite fit within the well-structured boundaries of classified information. Even though OSINT made up a large portion of the nation's intelligence, it had long been neglected as an integral source of intelligence data. Bean (2007) pointed out, "The professional literature typically points to the benefits and limitations of OSINT in meeting intelligence requirements, but larger investigations of how the concept of OSINT functions as an organizational symbol and site of contestation in the intelligence reform debate are absent" (p. 241).

Some analysts in the nation's IC do not consider OSINT a true form of intelligence. For decades it was considered unreliable, as most intelligence analyst's preferred classified information gathered through covert or technological methods. It was not until the events of 9/11 that OSINT was elevated to a prominent status. Asymmetrical terrorist attacks throughout the Middle East and the world have added to the popularity of OSINT as a valuable source of intelligence. Bean (2007) explained, "Discrepancies about OSINT's status as an intelligence discipline signify differences among stakeholders that lead to problems for OSINT's status as a special type of knowledge" (p. 241). Nevertheless, the reliance on OSINT by the IC over the last decade has been surprising; it

is now considered vital in the ongoing struggle against global terrorism. The Defense Intelligence Agency (DIA) 2012-2017 Strategic Plan states, "given the expansive, open-source environment—combined with social media, rapidly developing new technologies, and growing mission partnerships in an era of diminishing resources—DIA will become increasingly dependent on outside sources of knowledge to succeed in its mission" ("Defense Intelligence Agency," p. 10).

One important fact about open source information is that the government and private industry access its value from different perspectives (Bean, 2007). Open source information is a huge revenue generator for the private sector. Large corporations throughout the world pull in substantial amounts of open source information, process and analyze it, and then sell it to multiple customers around the world. This generates large sums of revenue for their customers. The government collects large amounts of open source information and distills it down into actionable intelligence in order to better secure the nation. Therefore, some officials within the government believe that the private sector is actually much better at collecting, collating, and analyzing huge amounts of open source data than the government (Bean, 2007).

The government and private industry interpret open source information in significantly different ways. The government states that it should pay for open source information once and only once, yet the open source community proposes that they should collect information once and then sell it multiple times (Bean, 2007). The utilization of OSINT by the United States government is currently on the rise. Many

OSINT reports are making their way to the president's daily briefing, which is one of the most important intelligence products in the nation (Bean, 2007).

The OSC is consistently producing a large volume of open source material for government use. Bean (2007) explained, "The OSC houses and builds upon the work of the Foreign Broadcast Information Service (FBIS), which was established in 1941 to monitor and translate foreign media" (p.250). The FBIS has been around for decades providing "translation, monitoring, and analysis of foreign Internet, print, radio, television, and other sources" (Bean, 2007, p.250). This consolidation of the FBIS into the OSC is a signal that the government is taking open source information very seriously. Bean explained "Transforming FBIS into the DNI Open Source Center implies a significant change; in order to prevent bureaucratic disruption, however, no consolidation of resources or operational authority under the DNI seems to have occurred" (p.250).

Hulnick (2002) explained, OSINT makes up a large portion of the ICs actionable data. It is the mix of classified information and OSINT, which work in concert to build a better intelligence product. In the competitive private business environment "the use of anything other than OSINT, such as industrial espionage or electronic intercepts, has become a federal crime" (Hulnick, 2002, p. 566). Hulnick explained that some organizations, "have actually settled potential lawsuits at great cost because their intelligence professionals strayed beyond the use of OSINT into such classic illegal activities as dumpster-diving and trying to trick sources into revealing trade secrets" (p.566).

Most analysts, public and private agree that open source information contains a vast amount of valuable information on a myriad of topics. The biggest problem with this key source of information is that there is so much of it that it is difficult to distill down into useable data. The sheer volume of open source information available has literally become overwhelming. The accuracy of the information collected is also a significant issue. The raw information "needs to be constantly checked and validated which is very difficult given the amount of data" available (Yates & Paquette, 2011, p. 12). The National Security Agency (NSA) "resorted to sampling and keyword techniques to sort the information, but some raw material allegedly remains untapped because there aren't enough people to deal with all of it" (Hulnick, 2002, p.567). One dynamic solution to this problem involves initiatives that "are designed for 'data mining' and 'knowledge management' to detect patterns or anomalies in vast streams of raw data" (Hulnick, 2002, p. 567).

Hulnick (2002) explained, the CIA has developed solutions to deal with the overwhelming amount of open source data. Recently, they have "turned to the private sector to develop techniques to sort, order, and deliver raw intelligence so that analysts are not overwhelmed" (p.567). Hulnick also pointed to the fact that open source information is riddled with reliability issues. There is so much information on the web that it is challenging to sort out which information is reliable, and which is not. Hulnick argued, "The world wide web has led to the proliferation of individual sites that produce propaganda, misinformation, or disinformation. But professional intelligence analysts should have no trouble sorting wheat from chaff in web databases" (p.568).

Language is an extremely important component of OSINT, and it is critical that analysts to be fluent in the language of the countries in which they study. Because we now live in a true global society, OSINT is intertwined into every language on the planet. Significant U.S. interests now focus on countries such as China and Iran where it is vital that analysts understand the culture intimately and speak the language fluently. Hulnick (2002) explained, "In the aftermath of the September 2001 events, the language problem has again led the CIA to turn to the private sector for technological help" (p. 572).

Another form of OSINT that is often overlooked is referred to as grey intelligence. Hulnick (2002) explained, "Grey intelligence, a category coined by Jon Sigurdson, who teaches business intelligence, refers to materials that are not classified but have to be obtained by digging" (p.573). Financial transactions generate a huge amount of data that can be exploited by intelligence analysts. Hulnick stated, "Real estate transactions, environmental impact statements, uniform commercial code, for example, fit this category and are particularly useful for the private sector intelligence operative" (p.573).

Several important successes have come from the OSC over the last decade. Much of the information that is gathered through the OSC is now filtered into intelligence reports giving analysts a better idea of how terrorist organizations operate and communicate throughout the world. Bean (2013) pointed out that the U. S. President's daily intelligence briefing regularly includes information provided by the OSC. Most analysts understand that although open source information contains a wealth of valuable knowledge; it is often buried in volumes of data. Finding those golden nuggets of

valuable intelligence is truly a challenge. After the attacks of 9/11 the nation's IC was forced to undergo an extensive organizational change. The looming threat to the nation is now from organizations that communicate, organize, and plan their attacks through social media and the Internet. However, Congressional funding for open source information collection is still deficient. The lack of significant financial support is truly a roadblock to the OSCs ability to fully engage the problem (Bean, 2013).

Bean (2013) explained "the nature of bureaucratic organizations, the ability of bureaucrats to protect their turf, and the fragmented structure of the U.S. federal government tend to stymie significant IC reform" (p. 43). Because officials within the IC are reluctant to fully embrace OSINT's elevation to a primary intelligence source, the discipline continues to suffer from that neglect (Bean, 2013). However, things are beginning to change, the sheer existence of the OSC "represents the institutionalization of open source in the IC" (Bean, 2013, p. 43). There are several major tensions that inhibit the OSCs ability to dominate the nation's IC. Bean explained, "tensions between and among materiality/symbolism, structure/agency, message processing/human context, exceptionalism/integration, and internal/external production characterize the post-9/11 open source debate" (p. 43). As the IC continues to adapt to global terrorism, analysts reflect on lessons learned.

Lessons learned from the intelligence community. Stephen Marrin (2004) explained that the primary focus of intelligence is its ability to prevent future terrorist attacks (p.656). He acknowledged that there are many imperfections in the nation's IC.

Some of those imperfections led to the IC's inability to identify Osama bin Laden's terrorist organization planning of the September 11th attacks. However, even with these imperfections the IC can learn from their mistakes and refocus their energy towards two basic principles. These include "the use of rigor and tradecraft in the production of intelligence analysis, and the integration of analysis into the policymaking process" (Marrin, 2004, p.656). One of the primary reasons for having an intelligence apparatus is to prevent surprise attacks like the one that occurred on 9/11. Years of intelligence production can ultimately lead to failure if the "information is not collected or integrated effectively, and policy failure can lead to surprise if actions were not taken despite intelligence warnings" (Marrin, 2004, p.656).

One of the biggest takeaways from intelligence failure is to learn from mistakes and reshape the IC to combat new and unique threats. Marin (2004) explained that evolving international relations and the rise of a global society create conditions where surprise is ever present. It is important to remember that "intelligence agencies may be responsible for the prevention of surprise, but not all surprises can be prevented by uncovering secrets" (Marrin, 2004, p.656). Even though some failures are inevitable, it is important to continually refine and improve our analytical standards. Marrin goes on to explain that many failures in intelligence throughout the last century, including the attack on Pearl Harbor, the 1950 North Korean invasion and other catastrophic failures of both intelligence and foreign policy, had a significant impact on geopolitics (p.659). As demonstrated in these examples, it is important to review the strategic failures of foreign policy, so that they will not be repeated in the future. Marrin explained, "Failure, though

perhaps inevitable, can be made less frequent through the implementation of a number of reforms that improve the quality of intelligence analysis" (p.662). The focus in the future will be learning from past mistakes and attempting to limit the amount of intelligence failures moving forward. Marrin pointed out, "this will require a two-pronged approach: more rigorous tradecraft to minimize faulty or incomplete analysis, combined with better customer service" (p.662).

Many experts in the IC believe that the free flow of information has been significantly restricted by a series of classification barriers ("New Information and Intelligence," 2008). This lack of organization prevents the analyst from viewing all of the information necessary to take effective action. Marrin (2004) argued, the "removal of organizational controls on certain types of information, and the relaxation of the need-to-know principle and other security devices responsible for informational 'stovepipes,' would allow for more horizontal distribution of information throughout the intelligence and policy communities" (p.662). It is actions such as these that reduce the chances of surprise to the intelligence community. Intelligence failures, which often lead to devastating circumstances, can be "related to flaws in the delivery of the more conceptual rather than merely the informational product" (Marrin, 2004, p.663).

Inevitably, there is a significant amount of political pressure on the IC to develop intelligence analysis products that support policy maker agendas. It is this conforming posture that significantly threatens clear and unbiased intelligence analysis. Therefore, there a strong focus in the IC to develop methods that increase the accuracy of the overall intelligence product. Marrin (2004) explained, "an additional method for increasing the

accuracy of a conceptual model is to ensure that the analyst possesses in-depth knowledge of the account to include, as necessary, context, history, or language" (p. 665). As the IC continues its adaptation to current threats, situational awareness of real-time events in remote locations around the world is a high priority. Social media monitoring is proving to be a useful activity to establish situational awareness of emergent events around the globe. Public safety organizations are beginning to embrace the use of social media during large public events to enhance situational awareness.

Social Media Use Between Public Safety Agencies

Currently, the ardent use of social media enables information to be rapidly shared between individuals throughout the world. Whether emails, photos, videos, or text messages, these digital information sources are commonly utilized in both personal and private endeavors. Government organizations are also utilizing social media sites to disseminate important information on everything from public events to public safety. However, law enforcement officials have been warning for some time that these digital tools are being utilized for unlawful purposes. Tech savvy criminal use the internet to "coordinate a criminal-related flash mob, or plan a robbery, or terrorist groups may use social media sites to recruit new members and espouse their criminal intentions" ("Developing a Policy," 2013, p.1).

To combat these illegal activities law enforcement agencies have been developing their ability to monitor open source information on the Internet. One of the most effective ways to monitor social media within legal boundaries is to develop an effective social media policy ("Developing a Policy," 2013). These policies allow intelligence and law

enforcement analysts' gradient levels of authority when monitoring social media outlets. Activities may range from "viewing information that is publicly available on social media sites to the creation of an undercover profile to directly interacting with an identified criminal subject online" ("Developing a Policy," 2013, p.2)

As analysts move along the continuum from least invasive to most invasive monitoring activities, they must secure multiple layers of authorization from supervisory personnel. Just as other covert actions are authorized in police investigations, social media monitoring should be well within legal authority. Fusion center "personnel must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information" ("Developing a Policy," 2013, p.2). As in most law enforcement activities, fusion center analysts should not maintain "political, religious, or social views, associations, or activities of any individual or group, association, corporation, business, partnership, or organization unless there is a legitimate public safety purpose" ("Developing a Policy," 2013, p.2).

The Bureau of Justice Assistance (BJA), working with law-enforcement agencies nationwide has developed policies regarding social media. These policies not only protect the public's civil rights, but also help to protect law enforcement agencies from civil litigation. All policies should be developed in close cooperation with local legal counsel to ensure that local, state, and federal laws are followed in the development of these important guidelines ("Developing a Policy," 2013). It is also important than law enforcement agencies update their privacy policies to include public notice of how they plan to monitor social media related data. Just as a police officer is compelled to search a home

or vehicle, criminal investigative regulations must be followed, and the public's civil rights must always be held in the highest regard. As public safety agencies develop internal policies for social media, they must also incorporate social media connectivity between organizations.

Social media as an information sharing platform. Pfeifer (2012) explained that information fusion between public safety agencies is not only a process of communicating between different disciplines, but also leveraging technology to connect databases between different agencies. In order to give first responders, the ability to anticipate threats, they must have an effective situational awareness of an event as it unfolds (Carter & Rip, 2013). Pfeifer explained, it is the process of actual network fusion, tying together not only intelligence community officials with local law-enforcement officials, but also reaching out to fire departments, emergency medical service organizations, and public health officials to collaborate before an emergency occurs. In fact, "finding new approaches for collaboration may be less a matter of innovation and more a matter of discovering what is already done by organizations" (Pfeifer, 2012, p.2). In the current digital environment, public safety organizations throughout the nation are increasingly becoming integrated into larger and larger digital networks. Therefore, it is likely that computer connectivity between these organizations is more achievable than ever before. Pfeifer pointed out, "Network fusion is an information sharing system that fuses information and intelligence from multiple sources to allow decision makers to better adapt to a changing threat environment" (p.2).

Linking public safety data systems can enhance the actual preparedness capabilities of public safety organizations to share information. Pfeifer (2012) explained that to truly have an integrated system, public safety organizations must do more than simply place individuals in a fusion center facility where they can share information face-to-face. Pfeifer argued that the "future of fusion centers will depend on their ability to collaborate with other organizations for prevention and response as well as their capacity for information to be pushed and pulled in real time through networking" (p.2). The process of network fusion has several advantages over building brick and mortar fusion centers. In a true virtual network, representatives of different organizations can communicate with colleagues faster online than they can in person. It is much cheaper to collaborate with public safety officials in a virtual meeting, than it is to co-locate them together over a period of time in a brick and mortar facility (Pfeifer, 2012). Pfeifer stated, "Network fusion exploits technology to quickly connect various organizations that participate in homeland security to exchange critical information, insights into potential attacks, and real-time situational awareness reports" (p.3).

Utilizing this process, decision-makers can also be drawn into the conversation when the need arises through security video conferencing. Virtual conferences can be organized within moments, much faster than physical meetings can be called together. Pfeifer (2012) argued that the nation's refusal to include collaboration technology in counterterrorism activities will severely reduce the ability to disrupt or respond to terrorist attacks. It is this data linking innovation that will provide public safety agencies the image of a terrorist suspect that may be progressing toward an imminent attack. Terrorist

organizations are already quickly adapting to new technology at a much faster rate than law enforcement organizations.

As fusion centers increase in size and scope throughout the nation in-person communication and collaboration will be a significant prohibitive factor. Collocating individuals from every organization that should be present within these centers will become more and more difficult to achieve. Using data networking as a leveraging factor will help government organizations achieve needed results without incurring prohibitive costs. Pfeifer (2012) explained, "The development of network fusion for faster, smarter, and cheaper information sharing and collaboration will require a socio technical approach that makes use of hard and soft systems" (p.3). In various areas of the nation public safety organizations are beginning to utilize social media in tactical operations during public safety emergencies.

Social media use during public safety emergencies. In the last several years, social media has been taking on a new role in threat related emergencies. Nearly every facet of modern society now utilizes social media. Government agencies are increasingly using this communications platform to relay vital information to the public during crisis situations. Emergency responders as well as public and private organizations can deliver and receive important information instantly during an event. When major hazardous events occur, public safety organizations are beginning to depend upon social media tools. During the 2013 attack on the Westgate Mall in Kenya, Africa, authorities assisting with emergency management activities used Twitter. This simple form of communication

allowed government agencies to deliver public information from multiple locations simultaneously, which proved to be a valuable source of situational awareness.

Simon, Goldberg, Aharonson-Daniel, Leykin, and Adini (2014) explained that during the mall attack, “all emergency responders used and leveraged social media networks for communicating both with the public and among themselves” (p.1). However, although extremely useful during emergency events, social media public postings also risk misinformation as well as vast amounts of irrelevant information. Simon et al., pointed out, “emergency managers should utilize filtering and pattern recognition algorithms on the data streams, in order to access important and meaningful information in real-time” (p.1). Utilization of this software can be invaluable to public safety and law enforcement organizations. Social media communication during emergency events has steadily risen over the last several years. However, because social media is a relatively new form of communication “there is not enough evidence for best practice when incorporating social media in emergency response” (Simon et al., 2014, p.2).

In a case study of the Westgate Mall attack Simon et al., (2014) utilized specialized computer software to collect the posts from Twitter and analyze various attributes of the data. The findings demonstrated that social media “served as an integral tool for emergency management in Kenya” particularly during this event (p.7). The information ranged from the location and number of injured individuals to actual photos of the attackers as they entered the mall. Much of the information was instrumental in public safety and law enforcement activities. During these types of rapidly unfolding

events, public safety organizations across the globe are slowly beginning to utilize social media (Simon et al., 2014).

Use of social media by terrorist organizations. Advancing technology in mobile communications has unfortunately proven to be an asset to terrorist organizations throughout the world. Cohn (2013) pointed out that complex web-based communication applications allow extremist groups to communicate with their followers in real-time. He explained, “the ability to immediately notify all of one's collaborators, simultaneously, of sudden and spontaneous tactical changes is a tremendous leap in the terrorists' ability to evade law enforcement personnel” (Cohn, 2013, p.64). This incredible change in the communication capabilities inside terrorist organizations over the last decade has counterterrorism officials throughout the world scrambling to keep up. Cohen (2004) stated that the ability to carry out a successful terrorist attack is a very complex and dynamic task. It is extremely difficult to carry out military tactical operations in a rapidly changing asymmetrical environment. Cohen explained, the “insertion, actualization, evasion, and finally extraction of the terrorists are far more difficult to achieve than a fantastical Hollywood story would have us believe” (p.64).

The ability to effectively communicate in real-time through all of the phases of a combat operation is a strategic advantage. The attacks of 9/11 forced the FBI and CIA to expand security measures domestically and globally (“Federal Bureau of Investigations,” 2015). It also set into motion collaborative agreements between organizations that had never existed before. Public safety organizations throughout the nation were forced to operate in a much more collaborative environment.

In 2008 a “commando styled terrorist raid in Mumbai, India,” again shook the world’s consciousness (Cohn, 2013, p.64). In this instance, a terrorist organization modified their attack strategy to the increased security environment. This indicated that terrorist organizations learned and adapted in order to succeed in a unique type of brutal attack on a major city. In the attack they utilized “elusive communication techniques to outwit dated counterterrorism defensive techniques” (Cohn, 2013, p.64). Cohn went on to explain how a 10-man squad was able to make their way into the city of Mumbai and carry out the catastrophic attack. Real-time communications were a significant factor in the attack. He explained, “the deep and comprehensive mobile communicative coordination amongst both the terrorists on site and their controllers proved to be the cornerstone of the operation's triumph” (Cohn, 2013, p.64). The coordinator of the terrorist operation was able to use common mobile cellular devices to orchestrate several teams of highly trained commandos from a secure location outside of the country. The coordinator watched live news feeds of the attack and then readjusted his commandos as needed. Cohen (2013) explained, “while these terrorists relied primarily on walkie-talkies and not social media per se, we may consider this communicative tool a predecessor to the ubiquitous mobile social media applications, which mark 2012, and beyond” (p.64).

What is important to glean from this article is that there are terrorist organizations around the globe that study these attacks and others like them and concentrate on what worked, and what did not. It is plausible that social media communication, location, and mapping tools can be readily used to orchestrate future terrorist’s attacks. Law enforcement organizations around the world are now spending considerable time and

effort studying a number of social media applications, so that they may avoid being blindsided by the next innovative terrorist attack.

Summary and Conclusions

The major themes in the literature were benefits of sharing threat-related information, fusion centers facilitation of information sharing between public safety agencies, challenges of sharing threat-related information, and social media use between public safety agencies. The findings of this study will help to fill the gap in literature by determining the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii, and what can be done to improve information exchange between these agencies. The findings will extend knowledge in the discipline surrounding the ability of public safety organizations to effectively share threat-related information.

The first major theme in the literature review focused on the benefits of sharing threat-related information. Soon after the 9/11 terror attacks, it became clear to the nation's leaders that information sharing between federal, state, and local public safety organizations must be improved. Fusion centers were tasked with developing a vital information-sharing link between public safety organizations throughout the nation. Although the goal is slowly being achieved, fully integrated information sharing between public safety organizations has not yet become a reality. The federal government has been aggressively assisting the development analytic capabilities by assigning highly trained analysts to public safety organizations throughout the nation. This is done with the hope of increasing collaboration and intelligence sharing capabilities.

The second major theme in the literature was fusion centers facilitation of information sharing between public safety agencies. State and local fusion centers are staffed primarily with representatives from federal, state, local, tribal, and private partners ("State and Major Urban," 2014). By integrating public safety analysts into the government's intelligence community, the DHS hopes to identify terrorist threats early and intervene before violent extremists become operational. The focus of this process relies on collaboration with local public safety organizations. It also depends on building interagency relationships, so that terrorist activity information can begin flowing from the field operations level up to the federal government.

The third major theme in the literature review was challenges of sharing threat-related information. Until the rise of global terrorism in the 21st century, freely available open source information had long been one of the least valued forms of information collected by the IC. It had been considered unreliable and very difficult to validate. During the Cold War, classified information gathered through covert or technical methods was the preferred intelligence asset. The attacks of 9/11 and the rise of asymmetrical terrorist warfare across the globe have proven otherwise. Currently, the nation's IC estimates that OSINT provides approximately 80% of the useful information utilized by the IC (Steele, 2008).

As a result, the nation's IC invested millions of dollars in the development of the OSC in McLean, Virginia. The establishment of this modern research facility will help to counter terrorist activity throughout the world. The fusion of information collected from the OSC and analytic reports from intelligence agencies from around the world allow

members of the IC an enhanced perspective on terrorist organizations that threaten the United States. Many components of the IC are becoming increasingly dependent on open source of information to fulfill their mission, both domestically and abroad.

The fourth major theme in the literature review was social media and the information sharing process. Because terrorist groups develop and plan attacks via the Internet, social media has become a valuable tool for threat analysis. Public safety organizations also use social media communication capabilities to collaborate between law enforcement, EMS, and public health officials during large-scale emergency events. The use of social media by public safety agencies will continue to develop and evolve into the foreseeable future.

Local public safety agencies throughout the nation are working to improve their threat-related information sharing capabilities. At the same time digital technologies are evolving at a rapidly escalating pace. Therefore, it is crucial that local public safety organizations keep up with the rapid pace of technology. After a thorough review of the literature, it was apparent that a gap exists in clearly identifying the benefits and challenges of sharing threat-related information between local public safety agencies in Honolulu, Hawaii. Chapter 3 will describe the methodology utilized to conduct the research for this study.

Chapter 3: Research Method

This chapter consists of an overview of the research design, rationale, and methodology of the study. It also includes a discussion of the role of the researcher and issues of trustworthiness. The findings of this study may help to fill a gap in literature on the perceived benefits and challenges of sharing threat-related information between public safety agencies. The purpose of the research was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii, a midsized metropolitan city. I sought to identify how these organizations can improve interagency information exchange. I determined that qualitative design was appropriate to explore the responses to the research questions for this exploratory case study. General systems theory ("General Systems Theory," 2014) was the conceptual framework.

Research Design and Rationale

I developed the following RQs for this qualitative exploratory case study:

RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?

RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

To ensure that an appropriate design was selected for this study, I considered various quantitative, qualitative, and mixed methods approaches. A qualitative

exploratory case study was selected to effectively answer the specific research questions. In a case study, "the researcher explores in depth a program, event, activity, process, of one or more individuals" (Creswell, 2009, p. 13). I collected data from several individuals. The data were then thoroughly reviewed and analyzed to identify the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu.

Researchers typically use quantitative methods to "examine the relationships between and among variables" utilizing surveys and experiments to test hypotheses (Creswell, 2009, p. 145). The quantitative process includes "a parsimonious set of variables, tightly controlled through design or statistical analysis" to test a theory or assumption (Creswell, 2009, p. 145). I opted against using a quantitative design because the rigid methodology would not allow adequate investigation of the information sharing process between public safety agencies. The deductive manner of quantitative analysis was not well suited, I concluded, for this particular research.

I opted against using a mixed methods design, which involves use of both quantitative and qualitative methodology (Creswell & Clark, 2017), because the quantitative aspect was not adequately suited to answer the research questions. My research relied on inductive open-ended questions rather than deductive closed-ended questions. The primary focus was to interpret the meaning inductively, within a flexible environment. The inclusion of quantitative data at this phase of an exploratory case study would require a research process that was preplanned and structured (Creswell, 2009).

Qualitative research differs from quantitative in that researchers become fully involved in the process of collecting data. Patton (2002) argued qualitative researchers are "interested in investigating a phenomenon to get at the nature of reality with regard to that phenomenon" (p. 215). The researcher seeks to thoroughly understand a particular phenomenon or event and then explain it to others. Analysis of qualitative data "requires reflection on the part of researchers, both before and during the research process, as a way of providing context and understanding for readers" (Sutton, & Austin, 2015, p.226). Researchers go through painstaking measures to interview participants, examine documents related to the topic, and collect other important information that will be utilized in the analysis portion the project (Patton, 2002). Qualitative researchers rarely utilize prepared instruments to collect their data (Creswell, 2009) and in qualitative research "there is no attempt to generalize the findings to a wider population" (Sutton, & Austin, 2015, p. 226). Themes should be allowed to develop naturally from the data, without the restrictive control deductive inquiry often requires (Creswell, 2009). The process depends on the researcher's skill in analyzing multiple sources of information. Creswell (2009) pointed out that "qualitative research builds patterns, categories, and themes from the bottom up, by organizing the data into increasingly more abstract units of information" (p. 175).

The data collection method for qualitative research evolves and develops as information rich cases allow the researcher to uncover unique data for the study (Palinkas et al., 2015). Qualitative researchers ensure that they capture the data in the context of which was observed by working closely with the participants (Creswell, 2009). Unlike

quantitative research, the process is not preplanned or tightly scripted, but emerges as the researcher becomes more familiar with the participants and how they interact in the context of their environment (Creswell, 2009). Palinkas et al., (2015) point out, "qualitative methods are, for the most part, intended to achieve depth of understanding" (p.534). Creswell (2009) explained, "the key idea behind qualitative research is to learn about the problem or issue from participants and to address the research to obtain that information" (p. 176).

A sincere interpretation of what is observed is woven into the fabric of the qualitative process. The researcher attempts to determine why individuals behave in a particular manner and what are the thoughts and feelings associated with those behaviors (Sutton, & Austin, 2015). Regardless of the process of qualitative data collection, there will be some researcher clarification involved, as this is a key difference between qualitative and quantitative processes. Creswell (2009) explained that "qualitative research is a form of interpretive inquiry in which researchers make an interpretation of what they see, hear, and understand" (p. 176). Qualitative researchers often interpret a particular issue by utilizing multiple perspectives to present a complex image that has developed through consistent qualitative processes (Creswell, 2009). Research for this study was intentionally designed to allow me to thoroughly understand the phenomenon, interpret it after thoughtful reflection and then explain it to the reader in a clear and concise manner.

Mode of Qualitative Analysis

I explored several forms of qualitative analysis to determine which type would best answer the research question. These included grounded theory, ethnography, narrative, phenomenological research, and case studies. After considering these designs, I selected a case-study approach for the study. In Ethnography, the researcher focuses on specific groups acting within their natural settings over a period of time and attempts to describe the culture of the group (Hammersley & Atkinson, 2007). In grounded theory, the researcher "derives a general, abstract theory of a process, action, or interaction grounded in the views of participants" (Creswell, 2009, p. 13). Developing patterns and relationships of significance within a limited number of participants is the objective of phenomenological research (Moustakas, 1994). Narrative research involves having individuals provide detailed narratives about life experiences. The researcher goes through a process combining detailed narratives from both the participant and the researcher into a rich collaborative blend (Clandinin & Connelly, 2009; Creswell, 2009).

After reviewing multiple forms of qualitative analysis, I confirmed that an exploratory case study would best answer the research questions for this study. I thoroughly reviewed the influences that helped shape the current state of threat-related analysis and information exchange between local public safety organizations. After careful examination I determined qualitative analysis would best explore the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii.

Role of the Researcher

As a researcher, my role in this study was to ensure that I provided an accurate account of information I collected throughout the research process. The topic of investigation was selected through my exposure to threat-related information exchange between public safety agencies in Hawaii. I was employed as a health and medical analyst at the Hawaii State Fusion Center for approximately five years. It was only natural that I decided to focus my PhD dissertation on an information sharing related topic, as I was immersed in this intriguing field of work for several years.

Academic researchers often select topics that are related to their personal or professional interests. Frankfort-Nachmias and Nachmias (2008) explained that research topics are often "related to the researcher's job, personal relationships, family history, social class, or ethnic background" (p.260). It is also important to select a topic of research that the researcher finds interesting and engaging at a personal level. Frankfort-Nachmias and Nachmias pointed out that researchers "emotional involvement in their work provides a meaningful link between the personal and emotional lives of the researchers and the rigorous requirement of the social scientific endeavor" (p. 261).

Some of the study participants were individuals that I worked alongside in public safety organizations. Others were analysts and administrators from various public safety organizations in Hawaii. An advantage to the selection of this topic was that I was familiar with the inner workings of public safety organizations in Hawaii. I understood the social dynamics of the work environment as well as the professional terminology used in the profession.

Methodology

Participant Selection Logic

Patton (2002) pointed out, “Sample size depends on what you want to know, the purpose of the inquiry, what is at stake, what will be useful, what will have credibility, and what can be done with available time and resources” (p. 244). A qualitative design was utilized for this research. This project included data collection from interviews with SMEs from four different fields of public safety in Honolulu, Hawaii (law enforcement, fire services, EMS, and public health). In-depth interviews were the primary source of data collected and was gathered from conversational style discussions with the participants utilizing open-ended questions.

The organizational culture of each agency was an important topic during the conversation. The interviews lasted 60 to 90 minutes and were recorded for reference. I took notes during the conversations. All interviews took place via a teleconference or in-person meetings. Approval to conduct the study was confirmed through Walden’s institutional review board. Each SME was contacted one month prior to the interviews and the purpose of the study was described. An email inviting them to participate in the study was mailed along with an informed consent form. The participants were also contacted by email prior to the interview to confirm a mutually agreed upon interview date and time. The interviews took place via teleconference, in person at the participants private residence, or a private meeting room at the Hawaii Public Library. The interviews were conducted outside of regular work hours and were kept confidential. I was the only person

who knew the identity of the participants and did not disclose their identities to anyone. Participants names and/or contact info was not recorded in the research records.

Approximately three individuals from four different public safety organizations were interviewed, resulting in 13 cases. This number of case interviews provided a clear understanding of the benefits and challenges within public safety organizations of sharing threat-related information. Individuals who had at least 15 years' experience sharing threat-related information between public safety organizations in Honolulu were participants. Individuals recently retired were selected if they met the research study selection criteria. Because these individuals were no longer associated with their organizations there was no pressure on them to answer the questions in a politically sensitive manor. This research was also an opportunity to capture extensive institutional knowledge from retired public safety SMEs before the knowledge was lost forever.

During the interview phase of data collection, a review of the consent form was offered to ensure that the participants were aware of the entire interview procedure. The participants received a detailed description of the purpose of the research and an invitation to participate. The participants were asked to read and sign an Informed Consent form with a nameless identifying number in order to keep their identity confidential. Consent Forms did not require signatures if the participant could indicate consent by returning a completed form with an identifying number. While conducting the interviews, I followed all of the steps outlined in the research Interview Protocol (Appendix B). I explained that their contribution would provide valuable information to the study. The interviews were structured in a manner allowing a smooth transition

through the various steps of the interview. Open-ended questions also permitted the participant to expand upon any of their answers, as time allowed.

Instrumentation

When a researcher collects qualitative data using open-ended questions, "the searcher cannot statistically test the validity and reliability of questions" ("Field Testing," 2016). To ensure the interview questions were suitable to explore the research questions for this study, I performed a field test of the interview questions prior to the actual interviews. To accomplish this, I went into the field and interviewed three individuals which had "expert knowledge about the population and research topic to provide feedback on the appropriateness of the questions being asked and how the questions are being asked in relation to the study focus" ("Field Testing," para. 4, 2016). These experts helped me to refine the interview questions and develop appropriate follow up prompts, inviting more conversation along a similar line of thought ("Field Testing," 2016). The interview questions were closely linked to the research topic. A detailed chart showing the linkage between the research questions and the interview questions is available in Appendix C.

An interview guide was utilized. Patton (2002) explained, "An interview guide is prepared to ensure that the same basic lines of inquiry are pursued with each person interviewed" (p. 343). The interview guide also ensured that the interview followed a relaxed agenda in order to utilize the time allotted for each interview effectively (Patton, 2002). A loose framework of the interview was predetermined ensuring questions were presented to each participant in roughly the same sequence and style. The data was recorded by

hand in a field notebook and simultaneously electronically recorded using a portable voice recorder.

Procedures for Recruitment, Participation, and Data Collection

Purposeful sampling was utilized. Subject matter experts that had extensive knowledge of sharing threat-related information between public safety agencies in Honolulu, Hawaii, were be selected for this study. These individuals had the depth of knowledge necessary to clearly articulate how threat-related information is analyzed and shared between organizations. The primary purpose was to explore communication across agencies and examine the benefits and challenges of sharing threat-related information between public safety organizations in Honolulu. Individuals selected were a part of the culture of these organizations and knew the social dynamics of each agency. Patton (2002) pointed out, "qualitative inquiry typically focuses in depth on relatively small samples, even single cases (N=1), selected purposely" (p.230). It is important to select participants that have a rich knowledge of their environment in order to build a quality research data set. Patton explained, "The logic and power of purposeful sampling lie in selecting information-rich cases for study in depth" (p.230). This process allows a thorough understanding of the information in context.

The sample for this study was a subset of SME's from the larger population within four fields of public safety that had extensive experience analyzing and sharing threat-related information between agencies. One gap that we often see in sharing of threat-related information is who is included, and how do we include public health (Hospitals, CDC, etc.). The study participants mirrored the population of the state fusion

center. Agencies that currently have representatives at the state fusion center were included because these are the organizations that will be active during an event. The larger population currently consists of less than 50 SME's, who work within four fields of public safety in Honolulu. For this research, approximately three SME's were selected from each field, which resulted in 13 participants. All individuals had at least 15 years of experience in public safety. It would not have been feasible to interview every member of the entire population for this study.

Purposeful sampling was utilized for this study. I identified subject matter experts from each of the four fields of public safety. Participants for the study were determined based on whether or not they met the inclusion criteria. Research study inclusion criteria included: Individuals who worked for a public safety organization in Honolulu, Hawaii; They had 15 or more years of experience in information sharing between public safety organizations in Honolulu; If retired, within the last 10 years. For this research, the data collected from 13 interviews provided a clear understanding of the benefits and challenges of sharing threat-related information between public safety agencies.

Qualitative analysis is different than quantitative in the fact that there is no optimal number for sample size. It is important to recognize while performing qualitative analysis, it is the richness of the cases that are of primary importance. Many highly regarded qualitative studies have been accomplished using very small sample sizes. Patton (2002) explained, "the validity, meaningfulness, and insights generated from qualitative inquiry have more to do with the information richness of the cases selected

and the observational/analytical capabilities of the researcher than with the sample size" (p.245).

Interviews were arranged with the participants and conducted once, via teleconference, the participant's private residence, or a private meeting room at the Hawaii Public Library. The interviews took place outside of regular work hours. Questions were asked in a semi-structured, open-ended format. It was anticipated that each participant would provide a substantial quantity of information. Patton (2002) explained, "the conversational interview offers maximum flexibility to pursue information in whatever direction appears to be appropriate, depending on what ever emerges from observing a particular setting or from talking with one or more individuals in that setting" (p. 342).

An interview of this type is often described as ethnographic in nature (Patton, 2002). Because the conversation was allowed to flow in any direction the participant preferred, it was not appropriate to offer prepared follow-up questions before hand. Therefore, the answers from each individual were unique in nature (Patton, 2002). It was extremely important that the participants were allowed to answer in their own distinct manner, as this is where significant knowledge was derived from the data. The interviews were scheduled several weeks in advance and I personally performed the interviews and collected the data for the study. The interview sessions lasted 60 to 90 minutes.

Data Analysis Plan

In order to capture accurate information for a qualitative data set, the voice recordings along with the field notes were transferred to a laptop computer. The

participant responses were then transcribed into written text. Once a draft transcript was transposed it was e-mailed to each participant to review to ensure that their responses were captured accurately. After the draft transcripts were returned with revisions they were entered into NVivo qualitative analysis software for data coding. All of the data collected from the participants was considered highly confidential and maintained in an encrypted format on a password protected laptop computer that will be held for one year and then permanently deleted. The process consisted of identifying key themes in the data, while continually reviewing my field notes to ensure that I was capturing the participants responses accurately. Maxwell (2013) explained, the key to data analysis is ensuring that all transcripts from the participant interviews are reviewed thoroughly and accurately. All of the information was organized, scanned, and prepared so that it could be analyzed and coded at a later date**.**

A process of coding was utilized to assist with the process of analyzing the data. The key to coding is to allow themes to emerge from the data that makes sense to the researcher. Creswell (2013) stated that researchers should develop a codebook for each research study. To ensure that I captured the essence of the of the interviews I used a coding strategy that consisted of reading through all of the transcripts several times to get a deep understanding of what took place during the interviews. I also reviewed my written notes, making memos of important facts and details. The next step involved classifying the data. Creswell (2013) pointed out "coding involves aggregating text into small categories of information" and then assigning an appropriate label (p.184). I then developed a short list of codes, or a codebook, which was expanded upon as I continued

processing the data (Creswell, 2013). Lastly, I separated all the codes into four or five overarching themes that assisted me while writing my discussion and narrative of the data. I utilized NVivo computer software throughout the coding process.

Issues of Trustworthiness

Credibility

Validity and reliability of quantitative data were established for this study through credibility, transferability, dependability, and conformability. Creswell (2009) pointed out that the trustworthiness and validity of qualitative analysis is extremely important in academic research. In order to ensure the credibility of the study several strategies were utilized. Creswell explained, "They should answer the reader's ability to assess the accuracy of findings as well as convince readers of that accuracy" (p.191). Multiple data sources were analyzed in this research to triangulate the information and better develop the themes (Silverman, 2014).

Transferability

The process of data gathering was described in detail, utilizing a rich and thick descriptive technique, so that the reader will receive a full and detailed account of each participant's experiences (Creswell, 2009). I attempted to bring insights to the topic and enrich the understanding of the phenomenon that was being investigated (Maxwell, 2013). The process of member checking was utilized in the analysis of the data. This allowed the participants the opportunity to comment on, add to, and even change any portion of the data they provided during the interviews.

Dependability

To ensure the validity of the study, I also included information uncovered that did not support the developed themes. This ensured that different perspectives were captured when they were presented in the research data. Most themes were built upon evidence found in the data collected for the study. Creswell (2009) pointed out that researchers "can also present information that contradicts the general perspective of the theme" (p.192). This process allows any counter perspectives encountered to also be considered by the reader (Creswell, 2009). Peer debriefing was utilized as another validity check for the study. Creswell (2009) explained, "This process involves locating a person (a peer debriefer) who reviews and asks questions about the qualitative study so that the account will resonate with people other than the researcher" (p.192).

Confirmability

Confirmability was established by practicing reflexivity throughout the project. Hsiung (2010) defined reflexivity as the ability of the researcher to reflect on him or herself and examine the relationship between the researcher and the individual being interviewed. An integral part of reflexivity is devoted to "examining one's 'conceptual baggage,' one's assumptions and preconceptions, and how these affect research decisions, particularly, the selection and wording of questions" (Hsiung, 2010, para. 1). I also utilized my experiential knowledge, consisting of "technical knowledge, research background, and personal experiences" to help uncover rich information revealed through a thoughtful in-depth interview process (Strauss, 1987; Maxwell, 2013, p. 45).

Ethical Procedures

In developing a research project there are many ethical issues that must be anticipated to protect the integrity of the project. Professional conduct was observed at all stages of the research. This included following rigorous guidelines that have been put into place by Walden University. Creswell (2009) stated that researchers must go beyond what is expected of them ethically. He explained, "Ethical practices involve much more than merely following a set of standard guidelines such as those provided by professional associations" (p.88). The researcher should be aware of the possibility of ethical issues occurring during the research process. Significant problems can occur if ethical procedures are not followed from the beginning. Creswell explained, "Deception occurs when participants understand one purpose, but the researcher has a different purpose in mind" (p.89). This is why researchers should thoroughly explain to the participants how the research will be accomplished and what the research will be used for.

An air of credibility and trust must be established early on to ensure that the information is gathered freely and openly in a safe environment. Walden Internal Review Board (IRB) monitors research conducted at the university to ensure that studies do not infringe upon the participants civil rights or civil liberties. Confidentiality must be discussed, if statements made by the participants are confidential in nature. Creswell (2009) explained that federal regulations have been established to ensure IRB committees oversee academic research studies and protect the research participants. I ensured that Walden IRB approval had been granted before any research was conducted for this study.

The study data will be kept in an encrypted password-protected data file on my computer for one year, and then it will be permanently deleted. During the study I was careful to anticipate any situation that could bring harm to the participant. Patton (2002) explained that this process should be well thought out from the beginning, because attempts to reduce the impact or damage after the study is completed often leads to disaster. During the study I ensured that no language was used that could be considered biased or discriminative against anyone.

Summary

In summary, this chapter described a process in which I used in a qualitative exploratory case study involving SMEs from four fields of public safety in Honolulu, Hawaii. It outlined an effective research design, as well as explained why a qualitative approach would best serve this particular topic. It explained that the data was collected utilizing in depth interviews of several SMEs who had experience sharing threat-related information between public safety organizations in Honolulu. It explained the role of the researcher and how the topic of investigation was selected for this project. It also reviewed the methodology of the process, ensuring that all guidelines established through Walden's institutional review board were followed. The process for recruitment of participants, data collection, and data analysis was explained. Trustworthiness concerns were integrated into the process to ensure that the study was ethically sound. Chapter 4 will describe the results of my research.

Chapter 4: Results

The purpose of this qualitative exploratory case study was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii. I focused on Honolulu for several reasons. Honolulu is a moderate-sized city and faces many of the same challenges as other cities in the continental United States, including the need to share information across agencies to manage emerging threat-related issues. However, Honolulu is unique because unlike other cities it is remotely isolated, being approximately 2,500 miles from the mainland. As a result, there is an increased need to ensure interagency communication occurs to facilitate the region's ability to manage an attack (Carter & Rip, 2013).

The gap in the literature was that there is a lack of knowledge about how public safety organizations communicate threat-related information at the local level. Because it is essential that these agencies communicate threat-related information effectively, due to their unique situation, an exploratory case study of Honolulu public safety agencies served as an excellent opportunity for this research. Individuals who had at least 15 years of experience sharing threat-related information between public safety organizations in Honolulu participated in this study. The findings provided a unique understanding of how public safety organizations that currently share threat-related information have encountered challenges and how these challenges differ between organizations.

I developed three RQs for this qualitative exploratory case study. The questions were aimed at exploring the benefits and challenges that exist in sharing threat-related information between public safety organizations in Honolulu.

RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?

RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

Field Test

To ensure the interview questions were suitable to explore the research questions for this study, I performed a field test of the interview questions prior to the actual interviews. To accomplish this, I went into the field and interviewed three individuals who had "expert knowledge about the population and research topic to provide feedback on the appropriateness of the questions being asked and how the questions are being asked in relation to the study focus" ("Field Testing," 2016, para. 4). These experts helped me to refine the interview questions and develop appropriate follow-up prompts. Conducting a field test also aided in establishing validity and reliability of the research questions. By using this process, I was able to develop interview questions that were closely linked to the research topic.

I e-mailed the Field Test to three SMEs in early January 2018. I received responses from all three individuals within 30 days. All three SMEs agreed that the

interview questions were appropriate in relation to the study focus and aligned well with the research questions. Two of the SMEs submitted suggestions on how to expand on the interview questions and continue the conversation on the topic. Field Test Participant 1 stated:

> Many individual systems comprise the larger system. Threat actors may cross through multiple systems in a given period of time. Each organization may function as its own system. Problems within one system could be manifesting within other systems as well. The sharing of threat information between systems is needed to make others aware a threat may exist. Threat identification and mitigation strategies identified by one system can be shared to assist neighboring systems.

This observation helped me visualize the individual organizations as separate systems within a larger public safety system. It also helped me understand how a violent individual could interact with different agencies within the larger public safety system and how, if that information was not shared, it could put other first responders at risk. For example, an individual may have a hostile or violent interaction with local law enforcement agencies on one occasion and several days later have an interaction with paramedics. The paramedics may be drawn into a dangerous encounter with a known violent individual with no prior warning from police. Therefore, it is vitally important that the emergency medical services are aware of individuals who may pose a threat to their responders so that they can take the appreciate precautions.

Field Test Participant 3, who had many years of experience working in a federal law enforcement agency informed me that ongoing law enforcement investigations would be a significant factor in an organization's ability to share information related to the case. Field Test Participant 3 noted the tension between how "public safety agencies manage public safety, while ensuring no compromises of ongoing open law enforcement cases." This concern was an important factor in my research and was addressed often by study participants who were from the field of law enforcement. Although the responses from the SMEs did not necessitate a change in the interview questions, they provided valuable context on the complexities of sharing information between public safety agencies. Their responses helped me to prepare for the interviews with the actual research study participants a few months later. A detailed chart showing the linkage between the research questions and the interview questions is available in Appendix C.

Demographics

I used purposeful sampling to select the participants. Individuals who had extensive knowledge of sharing threat-related information between public safety agencies in Honolulu were selected. These individuals had the depth of knowledge necessary to clearly articulate how threat-related information is analyzed and shared between organizations. It was important to include participants who had a deep knowledge of the public safety environment in order to build "information-rich cases for study" (Patton, 2002, p. 230). Patton (2002) explained, "Studying information-rich cases yields insights and in-depth understanding rather than empirical generalizations" (p. 230).

Table 1

Participant Demographics

Participant	Gender	Ethnicity	Years in public safety
350	Male	Hawaiian/Filipino/Portuguese	20 years
351	Male	Caucasian	37 years
352	Female	Asian	22 years
353	Male	Asian	34 years
354	Male	Caucasian	28 years
356	Male	Caucasian	33 years
357	Male	Caucasian	39 years
358	Female	Asian	17 years
362	Male	Caucasian	17 years
363	Male	Caucasian	46 years
364	Female	Asian	25 years
365	Male	Part Hawaiian	35 years
366	Female	Caucasian	46 years

The study participants mirrored the population of the Hawaii State Fusion Center. At the time of the study, officials at the Hawaii State Fusion Center stated the larger population consisted of fewer than 50 SMEs who work within the local public safety organizations, including law enforcement, fire services, EMS, and public health. It would not have been feasible to interview every member of the entire population for this study. For this research, I selected approximately three SMEs from each field of public safety, which resulted in a total of 13 participants (Table 1). Two of the participants were SMEs in more than one field of public safety, which enhanced their distinctive knowledge of public safety in Hawaii.

Eleven participants chose to conduct the interview via teleconference, one participant preferred to submit the responses to the interview questions via a written document rather than take part in an interview, and one chose to conduct the interview at the individual's private residence. The interview process took place over a 5-month

period. Each interview lasted approximately one hour or less, resulting in 92 pages of transcribed data (Table 2).

Table 2

Interview Descriptive Statistics

Participant	Interview date	Interview time	Sessions	Pages transcribed
350	8/9/2018	44 minutes	1	9
351	8/30/2018	54 minutes	1	7
352	10/3/2018	58 minutes	1	11
353	9/18/2018	50 minutes	1	9
354	10/25/2018	25 minutes	1	4
356	9/14/2018	59 minutes	1	12
357	9/18/2018	31 minutes	1	6
358	10/3/2018	34 minutes	1	6
362	9/17/2018	68 minutes	1	13
363	10/4/2018	26 minutes	1	6
364	12/3/2018	30 minutes	1	3
365	1/21/2019	Submitted transcript	1	2
366	1/11/2019	27 minutes	1	4

All interviews took place outside of the participants' work schedule. All participants in the study had at least 15 years of experience sharing threat-related information between public safety organizations in Honolulu. Several participants who met the research study selection criteria were recently retired. This research proved to be an excellent opportunity to capture extensive institutional knowledge from these retired public safety SMEs before the knowledge was lost forever.

Data Collection

Approval to conduct this study was granted by Walden University's Institutional Review Board assigning the study number 06-14-18-0334016. Purposeful sampling was used to identify SMEs within four fields of public safety in Honolulu, including

individuals from law enforcement, fire services, EMS and public health. Individuals which had a least 15 years of experience sharing information between organizations were selected. The purpose of this qualitative exploratory case study was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii. Each participant had a rich knowledge of their field of public safety and provided insight into what how their organization perceived the benefits and challenges of sharing information with other organizations.

Patton (2002) pointed out, "what would be 'bias' in statistical sampling, and therefore a weakness, becomes intended focus in qualitative sampling, and therefore a strength" (p.230). The strength of purposeful sampling in qualitative research focuses on cases that are rich with information about the topic (Patton, 2002). This process allows a thorough understanding of the information in the context of the participant's environment. Participants for the study were determined based on whether or not they met the inclusion criteria. For this research, the data was collected from 13 in-depth interviews and provided a clear understanding of the benefits and challenges of sharing threat-related information. I reached saturation at the 11th participant, as no new data was being discovered. However, I continued the interviews to include two more participants to ensure that I did not find new and unique data in the coding process. Faulkner and Trotter (2017) explained, "Data saturation refers to the point in the research process when no new information is discovered in data analysis, and this redundancy signals to researchers that data collection may cease" (para. 1).

The sample was a subset of SMEs from the larger population within four fields of public safety in Honolulu, including law enforcement, EMS, fire services, and public health. In many large cities, fire services and EMS are housed within the same organization. In Honolulu they are separate organizations, thus they were acknowledged as separate fields of public safety. Agencies with representatives who coordinate with the state fusion center were included, because these are the organizations that are active during large public safety events. The larger population currently consists of less than 50 SMEs who work within local public safety organizations. Approximately three SMEs were selected from each field, which resulted in a total of 13 participants. It would not have been practical to interview every member of the larger population for this study.

I began recruiting participants and scheduling interviews in August 2018. Due to their busy schedules, it took approximately 5-months to schedule and complete the interviews for 13 participants. Each participant was asked if they would like to conduct the interview via teleconference, at their residence, or at a private meeting room at a Hawaii public library. Eleven participants chose to conduct the interview via teleconference, one participant preferred to submit the responses to the interview questions via a written document rather than take part in an interview, and one chose to conduct the interview at their private residence. All of the interviews took place outside of the participants' work schedule. Four of the interviews took place during the participants' lunch break. Questions were asked in a semi-structured, open-ended format and each participant provided a substantial quantity of rich information. All of the

interviews were recorded except the one participant who preferred to submit the responses to the question via a written text document.

After each interview I transcribed the recorded information to text. I then e-mailed the transcription of the interview to each participant so that they could review it to ensure that my understanding of their responses was in line with their thought process. This process of member checking gave the participant the opportunity to comment on, add to, and even change any portion of the data they provided during the interview. I felt it was extremely important that the participants were allowed to answer in their own distinct manner during the interview and then make changes, if needed, to ensure I was capturing their thoughts accurately. Four of the participants made changes and additions to their interview data during this process. These individuals reviewed the transcripts carefully and added information, such as additional descriptions of an event, or clarifying statements that helped to explain their point of view on a topic. This additional information richly enhanced the data set. The data collection process took longer than I originally anticipated and therefore pushed the timeline of the data collection and analysis well into December of 2018.

Data Analysis

Data analysis for this study began by selecting 13 participants and interviewing them individually. After each interview, I listened to the recorded conversations and transcribed them into text and then uploaded all 13 files into NVivo qualitative analysis software. All research data was securely stored on a password-protected laptop computer. I carefully read through each transcript multiple times looking for common words that I

thought had meaning. I began aggregating the words into separate categories and assigned descriptive labels in the form of codes (Creswell, 2013). I also reviewed my written notes to ensure that I was documenting exactly what the participant expressed to me during the interview. I closely followed the coding process outlined by Creswell (2014), which includes assembling "raw data (transcripts, fieldnotes), organizing and preparing data for analysis, reading through all data, coding the data, interrelating themes/description," and finally "interpreting the meaning of themes/descriptions" (p. 197). I worked through all of the interview data and then coded each interview question separately to ensure that the codes I found during the first process surfaced again during a second pass. I sorted the data in NVivo by key words, looking for new and unique codes that I had not discovered during my initial attempt. My intent was to develop a thorough understanding of what the participants expressed during the interviews. The coding protocol is described in Appendix D.

The coding process resulted in 92 first level codes and 31 second level codes (Appendix E). Using a process of inductive analysis, I continued aggregating the emerging phrases into categories. Creswell (2014) explained, "in the analysis of the data, researchers need to 'winnow' the data (Guest, MacQueen, & Namey, 2012), a process of focusing in on some of the data and disregarding other parts of it" (p. 195). I identified 12 primary categories: (a) information flow, (b) collaboration, (c) fusion center, (d) confidential information, (e) agency culture, (f) different abilities, (g) policy, (h) responder safety, (i) secure websites, (j) politics, (k) training and (l) electronic communication.

Once I felt confident that the patterns were consistent throughout, I began identifying the links in the data by gathering similar codes into categories and similar categories into themes. Patton (2002) explained that "inductive analysis involves discovering patterns, themes, and categories in one's data. Findings emerge out of the data, through the analyst's interactions with the data" (p.453). By inductively analyzing the codes, categories, and themes, I developed four overarching themes: (a) Information flow within and between public safety organizations, (b) A lack of on-going collaboration between public safety organizations, (c) Agency participation with the state fusion center, and (d) The complexity of sharing confidential information between public safety organizations (Table 3). Creswell (2014), pointed out that the intent of qualitative analysis is to interpret the meaning of the patterns in the data, "It involves segmenting and taking apart the data (like peeling back the layers of an onion) as well as putting it back together" (p.195).

Table 3

Table of Themes

Overarching themes	Definitions	Categories (emerging themes)	Codes	Aggregate references
Information flow within and between public safety organizations	Participants stated that information did not flow smoothly within their departments and consequently out to other organizations. Several of the problems stemmed from information being shared only during intermittent urgent situations, rather than establishing an ongoing	Effective information flow, Withholding information	Information sharing between state and county, Co-locate dispatch, Communication, Include decision makers, Information sharing in real-time, Less information than before, Right information to the right people, Sharing information internally,	97

	information sharing environment.		Threat information not acted upon, Withholding information	
A lack of ongoing collaboration between public safety organizations	Participants felt that an ongoing collaborative environment allows multiple agencies with different perspectives to view the threat information and analyze it from different points of view.	Collaboration, Everyone on the same page	After action report, Agencies are equally invested, Coordinated response, Coordination of resources, Engagement with the visitor industry, Everyone on the same page, Common operating picture, Interoperability	70
Agency participation with the state fusion center	Participants stated that it is important that their agency participate with the fusion center so that threat-related information was disseminated across all public safety agencies simultaneously.	Fusion center, Identifying gaps and threats	Identifying gaps, Threat Team Oahu, Validating threats	56
The complexity of sharing confidential information between public safety organizations	Participants stated that it is often difficult to share information due to its sensitive nature, or its relation to an ongoing law enforcement investigation.	Confidential information, Information goes to the wrong people	Clearances, Leaks to the news media, Information goes to the wrong people, Law enforcement confidential informants, Need to know, People must be vetted, Understand when to share confidential information	48

Information flow within and between public safety organizations was the most prominent overarching theme in the data. Many of the participants felt that information did not flow smoothly within their departments and consequently out to other organizations. Several of the problems stemmed from information being shared only

during intermittent urgent situations, rather than establishing an ongoing information sharing environment. Participant 364 explained:

> I think that it is sometimes difficult to determine how much information to share, or what is pertinent. Also, transparency is important. You may have the top people in the organization that know what is going on, but it doesn't filter down to the workforce. The leadership may not feel that it is important to pass information down the chain, or even across to other agencies. Even if they do pass information down, they may not pass all of the information, or leave out important details. They may filter what they want to pass down, which could be dangerous. (Participant 364, personal communication, December 3, 2018).

Participant 352 pointed out:

> I think if it's not done on a regular basis, it may not be properly received, or there may not be a mechanism to receive and act on the information. So, we've got to have something in place so that when the information is pushed, or shared, or whatever, now I can receive it and I can deal with it, as opposed to what is this about, why are you calling me, what am I supposed to do with this. (Participant 352, personal communication, October 3, 2018)?

Several of the participants stated that information sharing between public safety organizations is a relatively new concept. Participant 353 explained:

> Sharing of information between public safety organizations, or for that matter within units within an organization is a newer phenomenon. I will tell you 30 years ago, people didn't tell anyone about their investigation, they would not to

> tell other people within the police department, for example, or they wouldn't tell federal law-enforcement, or other state agencies. They just didn't tell anyone because it was a need to know situation. (Participant 353, personal communication, September 18, 2018).

A lack of ongoing collaboration between public safety organizations was the second overarching theme. An ongoing collaborative environment allows multiple agencies with different perspectives to view the threat information and analyze it from different points of view. Participant 358 explained, "The benefits are awareness. I just had a meeting with an FBI colleague discussing some of these things. I believe that we have different perspectives on the same information, so there could be some helpful sort of awareness, so that we can address the issues that we tend to address. For them it is law enforcement issues, for us it may be disease issues, disease threats. It's how that information is shared, and what particular information is shared" (personal communication, October 3, 2018). Many of the participants stated it is vital that public safety organizations collaborate with one another on a daily basis rather than just when an emergency event brings them together. Participant 352 pointed out, "It's a really bad day if you're meeting your fellow responder for the first time, as you enter a life-and-death situation" (personal communication, October 3, 2018).

Agency participation with the state fusion center was the third overarching theme. Many of the participants stated that it is important that their agency participate with the fusion center so that threat-related information was disseminated across all public safety agencies simultaneously. Participant 366 explained, "If we are sharing information, then

everyone has the same information and it provides better protection for the public. If we don't share, then we just open ourselves up and any type of situation could happen. Only a few agencies may have that information and if we want to be responsive, it is going to take all of us to be responsive, not just one agency. Security is not one agency's responsibility, it is all of our responsibility" (personal communication, January 11, 2019).

The complexity of sharing confidential information between public safety organizations was the fourth overarching theme in the data. Many participants stated that it is often difficult to share information due to its sensitive nature, or its relation to an ongoing law enforcement investigation. Participant 366 explained, "I think the challenges are, number one, the interpretation of the information. Number two, how timely that information is. If you are sharing information via Homeland Security Information Network (HSIN), or the computer, or email, is everyone looking at the same information? Also, the sensitivity of that information. While you may have a disclaimer on that material and have a need to know, others may be sharing with people who do not have a need to know" (personal communication, January 11, 2019).

By inductively analyzing the participants responses to the interview questions, I linked the overarching themes to the study's research questions (Table 4). RQ1 asks, how are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii? The most prominent overarching theme in the data, information flow within and between public safety organizations, linked to RQ1. Agencies in Honolulu are communicating via information flow within and between organizations; however, in some cases this flow of information was intermittent. Several problems

stemmed from information being shared only during urgent situations. Establishing an ongoing information sharing environment between organizations is necessary to ensure that information is effectively shared in an all situations.

RQ2 asks, what are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii? The second overarching theme in the data linked to RQ2, indicating that there was a lack of an ongoing collaborative environment between public safety agencies that allows multiple agencies with different perspectives to view threat-related information and analyze it from different points of view. Because agencies have different skills and expertise, it is important that they collaborate on the analysis of threat-related information. The fourth overarching theme in the data, the complexity of sharing confidential information between public safety organizations, also linked to RQ2. Some threat-related information contains highly protected, or law enforcement sensitive information and is difficult to share between agencies. It is important that agencies develop a process, through ongoing collaboration to share this sensitive information.

RQ3 asks, what can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii? RQ3 linked to the third overarching theme in the data, agency participation with the state fusion center. Ongoing agency participation with the state fusion center is vitally important to allow threat-related information to be analyzed by multiple agencies with different skills and expertise, and then disseminated across all public safety agencies simultaneously.

Table 4

Table Linking Research Questions to Overarching Themes

Research questions	Overarching themes
RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?	Information flow within and between public safety organizations.
RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?	A lack of ongoing collaboration between public safety organizations. The complexity of sharing confidential information between public safety organizations.
RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?	Agency participation with the State Fusion Center.

Discrepant cases were also included in the analysis. In the Study Results section, I included contradictory perspectives on several topics. Different perspectives are important to understand the complexities of sharing threat-related information in a real world environment. Creswell (2009) explained, "researchers can also present information that contradicts the general perspective of the theme. By presenting this contradictory evidence, the account becomes more realistic and hence valid" (p.192).

Evidence of Trustworthiness

Credibility

Creswell (2009) pointed out that researchers using qualitative analysis should carefully document their procedures, describing the multiple steps of the research to demonstrate the reliability of the study. Throughout the data collection and analysis process I carefully described every step involved in order to assure the reader that the

information was accurately collected and examined. I triangulated multiple sources of data including participant interviews, field notes and supporting publicly available documents to develop the themes in the data.

In order to enhance the validity of the research, the participants were selected from various professions within four fields of public safety to allow for multiple perspectives. Creswell (2009) explained, "if themes are established based on converging several sources of data or perspectives from participants, then this process can be claimed as adding to the validity of the study" (p.191).

Transferability

I attempted to describe the collection and analysis of the data for the study in a rich descriptive manner to enhance the explanation of the process to the reader (Creswell, 2009). I first collected the research data through in-depth interviews, which were recorded, and then transcribed the data to written text exactly as it was communicated to me. I then e-mailed the transcription of the interview to each participant so that they could review it to ensure that my understanding of their responses was in line with their thought process, intentions, and understanding. This process of member checking gave the participant the opportunity to comment on, add to, and even change any portion of the data they provided during the interview. Several of the participants made changes and valuable additions to their interview data during this process which richly enhanced the data set.

Dependability

In an effort to strengthen the validity of the study, I coded all of the data that I received from the interview transcripts. I worked diligently to include all the viewpoints of the participants throughout the study, including information that contradicted the majority perspective (Creswell, 2009). This process allows counter perspectives to be uncovered and considered as the reader moves through my description of the data (Creswell, 2009). I utilized peer debriefing as another validity check in the study by asking a public safety SME at the PhD level to review my analysis of the data and ask questions about any aspect of the process (Creswell, 2009). This helped me to uncover errors and/or weaknesses in the process that might catch the attention of the reader.

Confirmability

I established confirmability by applying reflexivity throughout the data collection and analysis process. Reflexivity is described as the ability of the researcher to reflect on themselves to examine the relationship between the researcher and the individual being interviewed (Hsiung, 2010). Hsiung (2010) pointed out, "reflexivity is the process of examining both oneself as researcher, and the research relationship" (para. 1)." The researcher must examine their own preconceptions, and how this may affect the wording of the interview questions (Hsiung, 2010). Before I finalized the research questions for this study, I performed a field test to ensure the interview questions were as free from bias as possible and suitable to explore the research questions (Appendix F). The field test consisted of interviewing three individuals who had "expert knowledge about the population and research topic to provide feedback on the appropriateness of the questions

being asked and how the questions are being asked in relation to the study focus" ("Field Testing," 2016). I also utilized my first-hand knowledge, consisting of "technical knowledge, research background, and personal experiences" in the field of public safety to help uncover rich information revealed through the in-depth interview process (Strauss, 1987; Maxwell, 2013, p. 45).

Study Results

In the following section I present each research study question along with responses from the participants. In the Interpretation of Findings, I discuss the three most prominent themes that emerged from the data for each specific question.

Interview Question 1

The question was, what are the benefits of sharing threat-related information between public safety agencies in Honolulu, Hawaii? The following responses were provided by the interview participants.

Participant 350 stated, "being able to communicate and then kind of validating if something is really a threat" (personal communication, August 9, 2018).

Participant 351 stated, "why would we need to know what kind of chemical? Well, a lot of reasons, one for the medical people to treat it, if it happens" (personal communication, August 30, 2018).

Participant 352 stated, "I think a third thing that it will do is that it will broaden the perspective of the group. Because in a way you're enhancing the collective wisdom and different entities have different perspectives" (personal communication, October 3, 2018).

Participant 353 stated, “the benefits are obviously keeping our community safe and preventing terrorist attacks, whether domestic or foreign, or self-radicalized” (personal communication, September 18, 2018).

Participant 354 stated, “I think with the sharing you get a bigger picture. Some agencies may have a piece of the puzzle another agency doesn’t have, and then put it altogether” (personal communication, October 25, 2018).

Participant 356 stated, “one agency doesn't have expertise in every single potential threat to our community, there's no way we could understand or learn about this information without threat sharing between the agencies and having an organized manner to disseminate that information” (personal communication, September 14, 2018).

Participant 357 stated, “for the sharing of information in real time during responses, and to maximize coordination and minimize the impact on the community during those responses” (personal communication, September 18, 2018).

Participant 358 stated, “the benefits are awareness. I just had a meeting with an FBI colleague discussing some of these things. I believe that we have different perspectives on the same information, so there could be some helpful sort of awareness” (personal communication, October 3, 2018).

Participant 362 stated, “the benefits are it keeps everyone on the same page. I mean if one agency knows something criminal related, or law enforcement, or public safety related and it's important that the other agencies ought to know also” (personal communication, September 17, 2018).

Participant 363 stated, “that's pretty easy, the benefits are everybody knows the same information at the same time. The trouble is getting the trust and rapport good enough that people at the higher-ups will actually share the threat information” (personal communication, October 4, 2018).

Participant 364 stated, “I think that some of the benefits are it makes for a better coordinated effort between agencies. I think that it also keeps everybody informed and on the same page” (personal communication, December 3, 2018).

Participant 365 stated, “agencies will commit to more focused assessments and risk analysis in their daily operations and at emergency incidents” (personal communication, January 11, 2019).

Participant 366 stated, “first of all, we are too small for every agency to have their own information network. It has got to be shared, so that we collectively are collaborating on what needs to be done” (personal communication, January 11, 2019).

Interpretation of findings for Interview 1. Participant responses were analyzed according to their perception of the benefits of sharing threat-related information between public safety agencies in Honolulu. All 13 participants stated that collaboration was a benefit of sharing information. The different abilities of each public safety agency and information flow within and between agencies also ranked high in the responses to the question. The chart in Figure 1 highlights the number of participants who mentioned certain topics in their responses to Interview Question 1.

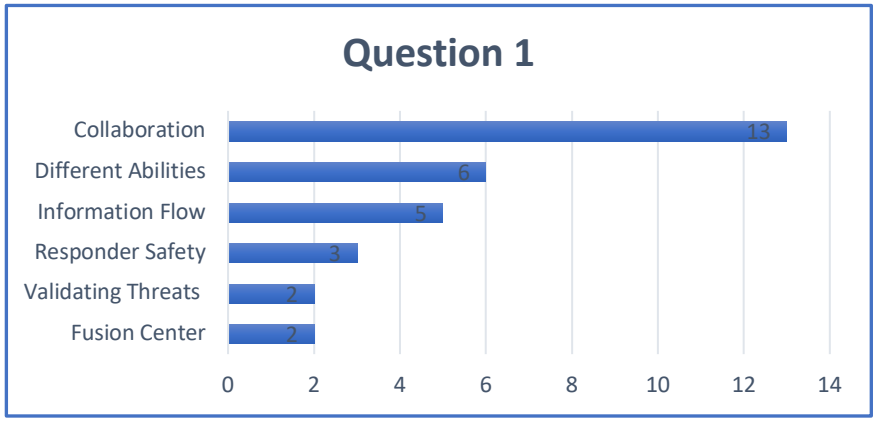

Figure 1. Comparison of topic frequency in participants' responses to Interview Question 1.

The most prominent theme in the responses to Interview Question 1 focused on collaboration. The participants stated that having all of the public safety agencies on the same page was very important. It is also essential that these agencies establish an ongoing collaborative relationship with one another before they arrived at the scene of a major incident and must work together. Participant 366 touched on the theme collaboration by explaining, "First of all, we are too small for every agency to have their own information network. It has got to be shared so that we collectively are collaborating on what needs to be done" (personal communication, January 11, 2019).

The second theme in the responses to this question was different abilities of each public safety organization. Many participants offered the opinion that one agency cannot know all of the threat-related information, and each agency views threat-related information from a different perspective. Law enforcement perceives threat-related data much differently than public health; however, each organization can provide valuable feedback toward better protecting the public and their fellow responders. If all of the

public safety agencies have access to the same information, it leads to a much more coordinated response.

The third theme in the responses to this question was information flow. Several participants stated that information flow is essential within organizations and also between organizations. Often information may flow effectively within an organization but is then blocked internally before it is shared with other organizations. Participant 350 explained, "some of the benefits right off the top is validating. Being able to actually validate what are really actual threats" (personal communication, August 9, 2018).

Interview Question 2

The question was, how does sharing threat-related information between public safety organizations help identify and prevent threats to the public? The following responses were provided by the interview participants.

Participant 350 stated, "the agencies can identify gaps and aid each other by bringing resources to bear in those gaps, in those areas that help deter, help detect, and help respond to specific threats" (personal communication, August 9, 2018).

Participant 351 stated, "one thing is the awareness for the staff, and way back when, and the cleaning staff, you know that make up the rooms. There were products for law enforcement only, and it says what to look for, identifiers" (personal communication, August 30, 2018). Participant 351 continued, "who's in hotel rooms. You've got to make it where we can share it with the hotel cleaning staff" (personal communication, August 30, 2018).

Participant 352 stated, “it's a really bad day if you're meeting your fellow responder for the first time, as you enter a life-and-death situation” (personal communication, October 3, 2018).

Participant 353 stated, “it is important to share information because they may have different pieces of the puzzle, the same puzzle” (personal communication, September 18, 2018).

Participant 354 stated, “the Customs and Border Patrol intelligence officer realized that in California they were getting ship containers that were coming from Vietnam or Thailand that were filled with the wrong refrigerant that could possibly explode” (personal communication, October 25, 2018). Participant 354 continued, “I notified my department to see if we had any other containers coming into Honolulu, and we were able to establish a big response and standby with police and fire at the docks while they carefully unloaded these things” (personal communication, October 25, 2018).

Participant 356 stated, “I think it goes back to the old saying, you don't know what you don't know. In our agency for instance, the drugs of abuse, the narcotics with contamination of first responders and the need for mega doses of Naloxone” (personal communication, September 14, 2018).

Participant 357 stated, “information being gathered by the law enforcement community is critical to the safety of the responders, not only to the responders to that particular incident, but also to developing the response protocol to protect the responders from secondary events” (personal communication, September 18, 2018).

Participant 358 stated, “obviously we deal with a lot of sensitive information so we want to be aware of potential cyber threat concerns, because we don’t want any compromise of our data which could impact public health” (personal communication, October 3, 2018).

Participant 362 stated, “say, whoever gets the information, the organic information does put it out to the news or something, do all of the law enforcement agencies see that at the same time, no, because they are busy” (personal communication, September 17, 2018).

Participant 363 stated, “so, it's important again, more eyes on the on the precursors, more eyes on anybody that is being crazy out there. Talking crazy, acting crazy, buying guns and other bad stuff” (personal communication, October 4, 2018). Participant 363 also stated, “the people who can actually do something are those folks who are out there like cops. Get the information back through HSIN through LEEP (FBI Law Enforcement Enterprise Portal), get it back to the JTTF (FBI Joint Terrorism Task Force)” (personal communication, October 4, 2018).

Participant 364 stated, “say that law enforcement is watching a certain person because they believe that they are a threat and they have information from an employer that this person is a loose cannon” (personal communication, December 3, 2018). Participant continued, “then EMS responds to the house and sees weapons. If EMS had known that beforehand, they could have informed law enforcement earlier and possibly avoided a dangerous situation” (personal communication, December 3, 2018).

Participant 365 stated, “emergency medical personnel are the first indicators of the health of the community and can detect sharp increases in medical emergencies stemming from possible chemical/biological threats” (personal communication, January 11, 2019).

Participant 366 stated, “if we are sharing information, then everyone has the same information and it provides better protection for the public. If we don’t share, then we just open ourselves up, and any type of situation could happen” (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 2. Participant responses were analyzed according to their perception of how sharing of threat-related information between public safety organizations helps to identify and prevent threats to the public. Seven of the participants stated that collaboration and responder safety was an important factor. Safety of the public also ranked high in the number of the responses to this question. The chart in Figure 2 highlights the number of participants who mentioned certain topics in their responses to Interview Question 2.

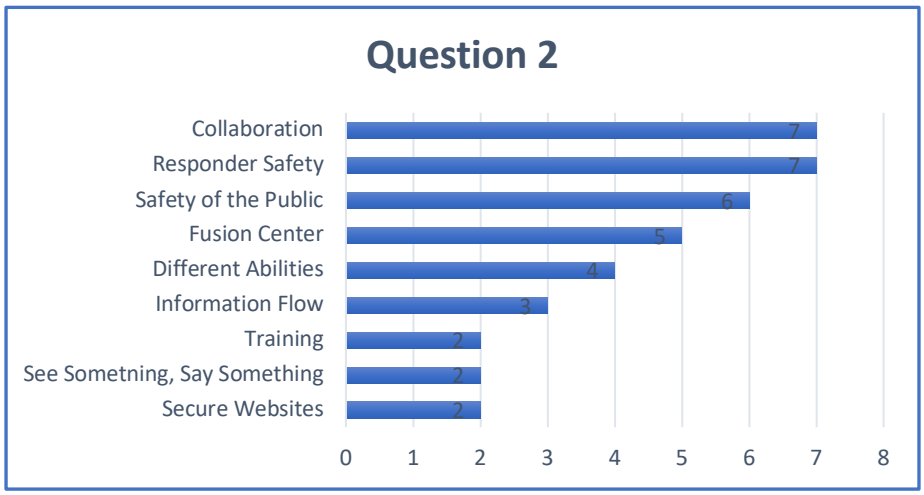

Figure 2. Comparison of topic frequency in participants' responses to Interview Question 2.

The most prominent theme in the responses to Interview Question 2 focused on collaboration between public safety agencies. By sharing information, the agencies can identify gaps and provide collaborative resources to protect the safety of the public. Participant 351 indicated that the information must be pushed, not only to public safety professionals, but also to individuals in the private sector such as hotel security and cleaning staff who might have access to important threat-related information within the hotels. Participant 352 stated that responders should work together collaboratively before they are forced to meet during an actual incident.

The second theme in the responses to this question centered around responder safety. One agency may have information that can add a piece of the puzzle held primarily by another organization. Threat-related information not shared by one agency may put other responders' safety at risk, such as EMS when they enter a domestic violence scene to render medical care. Participant 357 touched on this theme by pointing out, "information being gathered by the law enforcement community is critical to the safety of the responders, not only to the responders to that particular incident but also to developing the response protocol to protect the responders from secondary events" (personal communication, September 18, 2018).

The third theme in the responses to this question focused on safety of the public. Participants were acutely aware that their actions, or inactions, affect the safety of the public. As an example, cyber-attack information that results in breached data should be

shared between agencies so that they can better protect their networks from unauthorized intrusion. Participant 358 explained, “we deal with a lot of sensitive information, so we want to be aware of potential cyber threat concerns, because we don’t want any compromise of our data which could impact public health” (Personal communication, October 3, 2018).

Interview Question 3

The question was, how does communication software play a role in the sharing of threat-related information? The following responses were provided by the interview participants.

Participant 350 stated, “in this day and age, the technological advances in communication software, really what it does is it allows us to communicate in real-time, overtly, covertly, across multiple agencies” (personal communication, August 9, 2018).

Participant 351 stated, “the office of homeland security finances HHVISA (Hawaii Hotel Visitor Industry Security Association), HIORCA (Hawaii Organized Crime Alliance) and Safe Keiki websites, so important, the buy-in” (personal communication, August 30, 2018).

Participant 352 stated, “I think it helps to build a network and a mechanism, for sharing that will remove that that margin for individual error” (personal communication, October 3, 2018).

Participant 353 stated, “besides the Homeland Security Information Network (HSIN), and FBI’s Law Enforcement Enterprise Portal (LEEP), I could also to a certain respect include the Hawaii High Intensity Drug Trafficking Area (HIDTA) and the

Western States Information Network (WSIN)" (personal communication, September 18, 2018). Participant 353 added. "I think they all play a major role in collecting information, categorizing information, sharing information and then add to that notifying an agency if there is a conflict. That's typically the way deconfliction works" (personal communication, September 18, 2018).

Participant 354: "I think one it allows all first responders in Honolulu to access the HSIN stuff. Not only to see what is going on here in Hawaii, but in the bigger picture, to get information from across the entire nation" (personal communication, October 25, 2018).

Participant 356 stated, "personal health care information, response capabilities, response patterns. Not to the level of classified or top-secret or anything like that, but it definitely is for official use only type of information where you just don't want that widely disseminated" (personal communication, September 14, 2018).

Participant 357 stated, "right now, we are looking at implementing software applications for an immediate notification of key city department heads. That was a missing piece in our response protocols" (personal communication, September 18, 2018).

Participant 358 stated, "in terms of disease management, we have our own disease management software for monitoring trends from our surveillance data, but in terms of broadly, no" (personal communication, October 3, 2018).

Participant 362 stated, "there are several ways that communication software plays a role. We currently use our intranet system exclusively for passing information up and

down within the organization, but you are not always logged on" (personal communication, September 17, 2018).

Participant 363 stated, "I think it is getting better because of community access to HSIN. That's a really big deal, that's huge. Non-law enforcement people get in there and we know who they are, and they become a trusted partner" (personal communication, October 4, 2018).

Participant 364 stated, "if you put it in writing it can be a good reference. We can avoid misinterpretation or a situation where we send out the wrong message. So, I think that it is very important" (personal communication, December 3, 2018).

Participant 365 stated, "most public safety agencies using social media, websites, and wireless emergency alerts are effective in providing information rapidly to the public" (personal communication, January 11, 2019).

Participant 366 stated, "everyone has the same platform of information to work from. Versus, if we picked up the telephone and we called someone, how did you hear it, and how I hear it and how the next person hears it may be different" (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 3. Participant responses were analyzed according to their perception of the role communication software plays in the sharing of threat-related information. Eight of the participants stated that secure websites played a significant role in the sharing of threat-related information. Information flow and electronic communication also ranked high in the number of the responses to this

question. The chart in Figure 3 highlights the number of participants who mentioned certain topics in their responses to Interview Question 3.

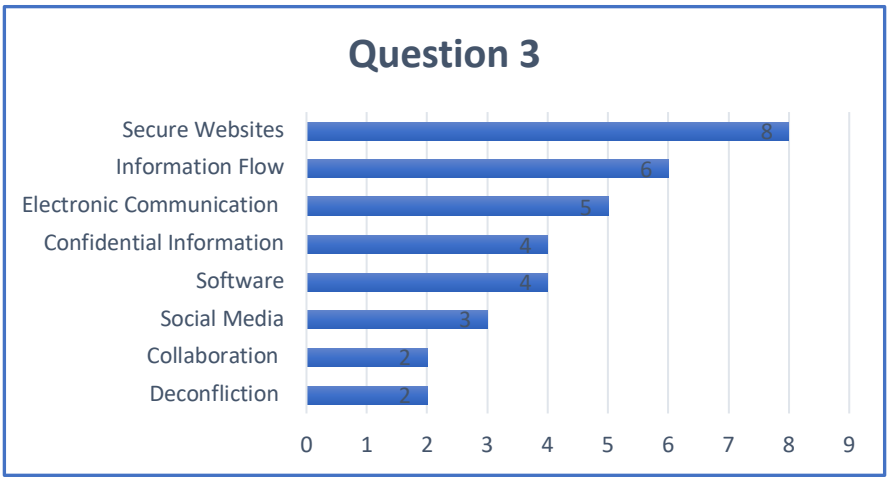

Figure 3. Comparison of topic frequency in participants' responses to Interview Question 3.

The most prominent theme in the responses to Interview Question 3 pertained to storing data on secure websites. Various online portals are utilized by public safety organizations in Honolulu including, HSIN, LEEP, and WSIN, which allow law enforcement and other public safety officials to share sensitive threat-related information in a secure portal. Only vetted individuals who have completed background checks are allowed to access these portals. One of the challenges is encouraging people to utilize these assets and login to the portals to check for new and updated information. Participant 354 explains, "it allows all first responders in Honolulu to access the Homeland Security Information Network (HSIN) stuff. Not only to see what is going on here in Hawaii, but in the bigger picture, to get information from across the entire nation" (personal communication, October 25, 2018).

The second theme in the responses to this question pertained to utilizing communication software within their own organizations and then passing pertinent threat-related information out to other organizations so that all of the public safety organizations have a common operating picture of the potential threats in their region. Participant 366 explained, “everyone has the same platform of information to work from. Versus, if we picked up the telephone and we called someone, how did you hear it, and how I hear it and how the next person hears it may be different” (personal communication, January 11, 2019).

The third theme in the responses to this question focused on disseminating threat-related information to other organizations in real-time, utilizing electronic communications software during critical events. Participant 364 commented on this concept stating, “if you put it in writing it can be a good reference. We can avoid misinterpretation or a situation where we send out the wrong message. Effective communication can reach a larger number of people” (personal communication, December 3, 2018).

Interview Question 4

The question was, what are the challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii? The following responses were provided by the interview participants.

Participant 350 stated, “I believe the classification of information is a challenge. How we classify what information we have really depends on who's going to see it, or how it's going to get shared” (personal communication, August 9, 2018)?

Participant 351 stated, “for instance when CIU (Criminal Intelligence Unit) comes to a partner's meeting, almost invariably, they never say a word, zero. I'm constantly told by administrators of the police they are there just to absorb” (personal communication, August 30, 2018). Participant 351 continued, “if they can't give us techniques and procedures, there's something to look out for, then we don't need them in the partners meeting because we are there to share information” (personal communication, August 30, 2018).

Participant 352 stated, “I think if it's not done on a regular basis, it may not be properly received, or there may not be a mechanism to receive and act on the info” (personal communication, October 3, 2018). Participant 352 continued, “I think it is a challenge right now, because I think if you were to call EMS today, or even Fire, with some sort of active threat info, would they know what to do with that information” (personal communication, October 3, 2018)?

Participant 353 stated, “sometimes the providing agency of the information, the investigators work hard, they work extensively, and maybe months of arduous work on this investigation then when it is given to another agency” (personal communication, September 18, 2018). Participant 353 went on to say, “the agency that provided information would like to be acknowledged or receive some credit for it. Sometimes that does not happen” (personal communication, September 18, 2018).

Participant 354 stated, “I think one of the challenges is if you share too much, or someone leaks it out to the public or to the media, it could possibly ruin an ongoing investigation” (personal communication, October 25, 2018).

Participant 356 stated, “the biggest challenge is trust and making sure the information is secure. Because in any agency, federal, state, or local governments, there's always a few people who want to share things with the media and share things with their friends” (personal communication, September 14, 2018).

Participant 357 stated, “I don’t see any major barriers at this point of time in Honolulu. I think we have an excellent sharing of information amongst our public safety agencies” (personal communication, September 18, 2018).

Participant 358 stated, “I think it’s knowing what it is they might, or might not, be interested in” (personal communication, October 3, 2018). Participant 358 added, “let me know if they [FBI] felt there was something that they needed to know, because I wouldn’t necessarily know if there was something nefarious about a particular bunch of cases we are investigating, or outbreak or whatever” (personal communication, October 3, 2018).

Participant 362 stated, “do they have a system set up to be able to share between public safety agencies other than just a phone call between people that know each other” (personal communication, September 17, 2018). Participant 362 added, “is there a software system set up, is there a bridge built to be able to share threat information, other than the news” (personal communication, September 17, 2018)?

Participant 363 stated, “the senior level guys, they get bonuses for having these meetings and showing that they're sharing. They get out of the meeting and then they bad mouth, oh I had to share, I had to, had to share” (personal communication, October 4, 2018). Participant 363 added, “it's a reluctance that they're losing their power, they're

losing. They think, I don't have complete control over my information anymore. My information. I've heard it at many meetings" (personal communication, October 4, 2018).

Participant 364 stated, "it may make it more of a competition between certain agencies. Say, for example law enforcement wants to be the one to track down the bad guy, or be a hero, so they may not share the information as necessary" (personal communication, December 3, 2018).

Participant 365 stated, "Agencies need to evaluate and react appropriately to threat-related information" (personal communication, January 11, 2019).

Participant 366 stated, "I think the challenges are, number one, the interpretation of the information. Number two, how timely that information is. If you are sharing information via HSIN, or the computer, or email, is everyone looking at the same information" (personal communication, January 11, 2019). Participant 366 added, "while you may have a disclaimer on that material and have a need to know, others may be sharing with people who do not have a need to know" (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 4. Participant responses were analyzed according to their perception of the challenges of sharing threat-related information between public safety agencies in Honolulu. Nine of the participants stated that confidential information was a challenge of sharing of threat-related information. Information flow and agency culture were other themes which ranked high in the responses to this question. The chart in Figure 4 highlights the number of participants who mentioned certain topics in their responses to Interview Question 4.

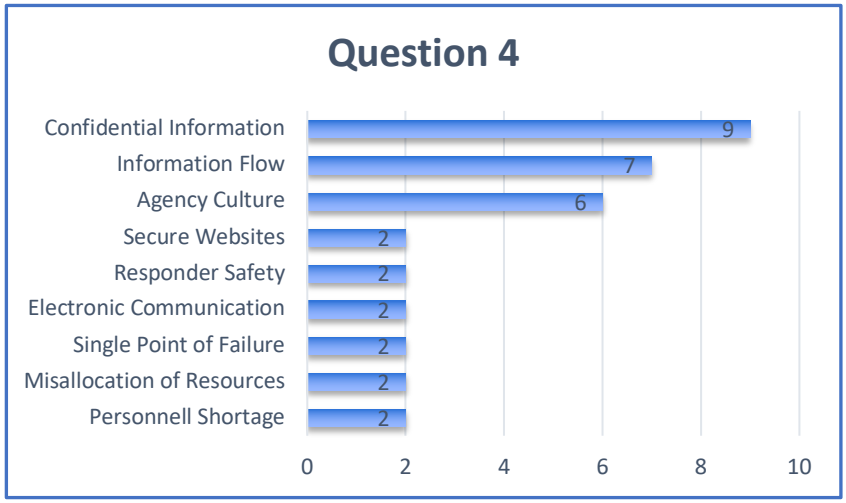

Figure 4. Comparison of topic frequency in participants' responses to Interview Question 4.

The most prominent theme in the responses to Interview Question 4 centered around the complexity of sharing confidential and protected information between public safety organizations. When information contains details that are confidential or sensitive it can only be shared with people that have a legitimate need to know that information (e.g. active police investigations). Also, classified national security information can only be shared if the receiver has a national security clearance and is authorized to receive the information. Therefore, sharing this type of information with all public safety organizations is not possible. Confidentiality of information inherently inhibits the ability to share information. Participant 356 stated, "the biggest challenge is trust and making sure the information is secure. Because in any agency, federal, state, or local governments, there's always a few people who want to share things with the media and share things with their friends" (personal communication, September 14, 2018).

The second theme in the responses to this question pertained to information flow within and between organizations. It is important to build paths for information to flow within agencies so that when it is received, it can be disseminated to the right people within the organization. Participant 352 pointed out that information must be shared on a regular basis for agencies to develop the processes to utilize it, or eventually the flow of information will stop. Participant 352 explained, “I think if it's not done on a regular basis, it may not be properly received, or there may not be a mechanism to receive and act on the info” (personal communication, October 3, 2018).

The third theme in the responses to this question focused on agency culture. When threat-related information is shared between agencies there is always a concern that the information may be inadvertently shared to the wrong people or to the media. Participant 364 explained, “In some situations we may not know who the good guy is, and who the bad guy is. If information is shared carelessly, someone may tip off the bad guys” (personal communication, December 3, 2018).

Interview Question 5

The question was, please describe the top three barriers, at your organization, to sharing threat-related information between public safety organizations. The following responses were provided by the interview participants.

Participant 350 stated that national security clearances create a barrier. He explained, “we kind of touched on it, but I think you know again it is the clearance” (personal communication, August 9, 2018). Participant 350 added, “here in Honolulu we have multiple military installations from every branch of service you know from the basic

military unit level all the way up to the combatant command level and so, there's a lot of information flowing about threats" (personal communication, August 9, 2018)

Participant 351 stated, "HPD has a Crime Analysis Unit. We wanted to hook up with them and share information. The last administration said no. So, it's that lack of data that we're getting, well that we're not getting" (personal communication, August 30, 2018).

Participant 352 stated, "law enforcement does a great job dealing with the information coming in and sifting through it and deciding what's relevant and what's not. There's no medical perspective or no healthcare perspective that is viewing that intelligence or that data" (personal communication, October 3, 2018).

Participant 353 stated, "sharing of information between public safety organizations or for that matter within units within an organization is a newer phenomenon. I will tell you 30 years ago people didn't tell anyone about their investigation" (personal communication, September 18, 2018).

Participant 354 stated, "the only real barrier that I can think of was that the HIDTA wanted to do drug raids on suspected houses that were producing illegal drugs. They wanted a way to warn us [Firefighters/EMS] if we responded to that house" (personal communication, October 25, 2018). Participant 354 added, "they had to be very careful about not sharing the information so that it would not get back to the criminals" (personal communication, October 25, 2018).

Participant 356 stated, "the second barrier is I think, that just not everyone understands the importance of information sharing" (personal communication, September

14, 2018). Participant 356 added, “people who've been in one lane for many years in their agency and they are kind of in this tunnel and don't realize what's going on in the world around them, actually affects your agency” (personal communication, September 14, 2018).

Participant 357 stated, “we [Honolulu county government] do have the public safety response functions, we are much more attuned to planning and preplanning for these events, but it does become very important to include functions of state government in this as well” (personal communication, September 18, 2018). Participant 357 added, “that is going to be a bigger challenge because they are not focused towards a public safety function. At least in the state of Hawaii” (personal communication, September 18, 2018).

Participant 358 stated, “if we are going to be sharing data with entities who don’t normally deal with protecting health information, personal information on a day-to-day basis, how do we get assurance that they have appropriate training” (personal communication, October 3, 2018).

Participant 362 stated, “lack of education or knowledge of the benefits of sharing information. Another one would be lack of manpower or at least not allocating resources that should be. The third one would be the political will” (personal communication, September 17, 2018).

Participant 363 stated, “so that's all we're supposed to do is filter that stuff and you have to be judicious on how you filter it, because what you filter out might be what somebody else needs” (personal communication, October 4, 2018).

Participant 364 stated, “you may have the top people in the organization that know what is going on but it doesn’t filter down to the workforce” (personal communication, December 3, 2018). Participant 364 added, “even if they do pass information down, they may not pass all of the information or leave out important details. They may filter what they want to pass down, which could be dangerous” (personal communication, December 3, 2018).

Participant 365 stated, “one perceived barrier could be that dedicated resources within a department specifically focused on the intelligence function. With personnel staffing functions so difficult to procure, the intelligence function would be assigned as an additional duty” (personal communication, January 11, 2019).

Participant 366 stated, “the different levels in which the DPS (Department of Public Safety), the DLNR (Department of Land and Natural Resources), the AG (Attorney General) and the HPD all relate to one another. They are not all on the same level.” (personal communication, January 11, 2019). Participant 366 also added, “I think that hurts us because I don’t think that we communicate enough together. How do we bring everyone together? I don’t think we do that very well” (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 5. Participant responses were analyzed according to their perception of the top three barriers at their respective organizations to sharing threat-related information between public safety organizations. Seven of the participants stated that information flow was a barrier when sharing threat-related information. Different abilities and employee training were themes which also

ranked in the top three responses to this question. The chart in Figure 5 highlights the number of participants who mentioned certain topics in their responses to Interview Question 5.

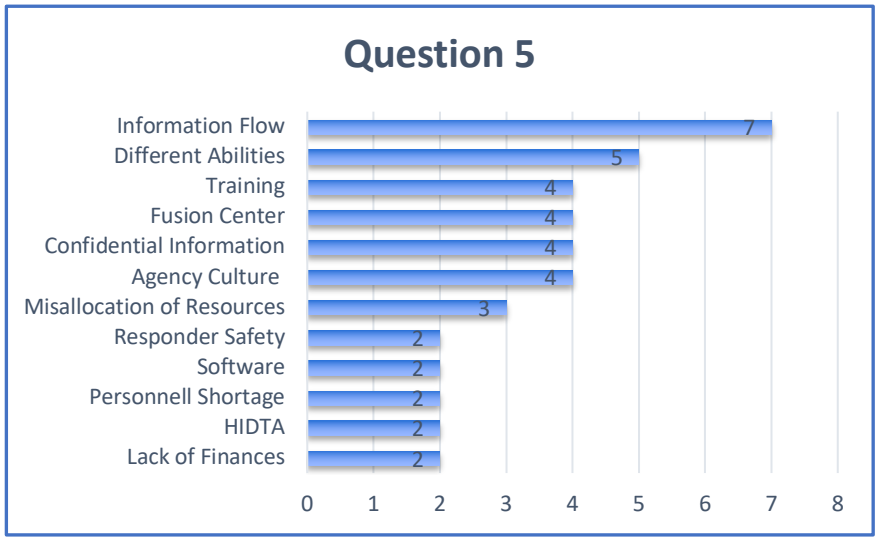

Figure 5. Comparison of topic frequency in participants' responses to Interview Question 5.

The most prominent theme in the responses to Interview Question 5 focused on information flow within and between organizations. Often, the leadership of an organization may be receiving information but does not chose to pass all of the information down to the rest of the organization. Participant 364 pointed out:

> It is often difficult for leadership to determine what information to share and how much information to share. Because leadership is not continually working at the operations level, they may not pass down information that is important to the responders on the street, or they may only pass down a portion of the information that was received. Whether they realize it or not, if all of the information received

> is not passed down, they are filtering it in one form or another. (Participant 364, personal communication, December 3, 2018).

The second theme in the responses to this question focused on the different abilities of each public safety organization. Each agency is proficient at what they do on a daily basis; however, each excels at different skills. Law enforcement may be very good at determining threats related to an active shooter situation, but not skilled at detecting threats from a health or medical related emergency. Participant 352 pointed out, “If the threat-related information is not viewed by subject matter experts in various fields of public safety, such as medical or public health, critical information may be missed which may pose an unintentional risk to the public” (personal communication, October 3, 2018).

The third theme in the responses to this question focused on employee training. In order to share information effectively, organizations must invest in the appropriate training for staff members who are designated to receive and transmit confidential or sensitive data. Participant 358 explained, “If we are going to be sharing data with entities who don’t normally deal with protecting health information, personal information on a day-to-day basis, how do we get assurance that they have appropriate training” (personal communication, October 3, 2018).

A discrepant response to this question focused on financial resources. A lack of financial recourses could restrict an organizations ability to assign staff to participate in information sharing environments. Participant (356) pointed out, “if we were unable to fund someone's participation in something like the fusion center and we were also unable

to fund someone to generate our own research, to disseminate our own information, that's a barrier" (personal communication, September 14, 2018).

Interview Question 6

The question was, how does politics play a role in the sharing of threat-related information between public safety organizations? The following responses were provided by the interview participants.

Participant 350 stated, "I guess it's really dependent upon if we are nearing an election season for politics; depending on who is running and gunning for positions. I would say that sometimes the politics are from even within their own unions" (personal communication, August 9, 2018).

Participant 351 stated: "So HPD's culture you know well, not to share, not to release but to work things internally. That is the culture of HPD" (personal communication, August 30, 2018).

Participant 352 stated, "one is that the director overseeing the department that contains EMS is appointed by the mayor. So, every time you change the mayor you probably are going to change that director and so you have a lack of continuity" (personal communication, October 3, 2018). Participant 352 also added, "that director may have little or no medical background and yet they're seen as being in a position that should be the medical lead for the city. So, I think that's usually problematic and that's entirely political" (personal communication, October 3, 2018).

Participant 353 stated, "the importance of the fusion center. Whether they are firefighters or police officers, through the wish of the chief, if the chief wants those

personnel back and staffed somewhere else then there is no one at the fusion center" (personal communication, September 18, 2018). Participant 353 also added, "that's a big impact and that is a big policy decision that could play a role" (personal communication, September 18, 2018).

Participant 354 stated, "one of the big ones would be funding" (personal communication, October 25, 2018).

Participant 356 stated, "We were appointed and when you're appointed you have to follow the orders of your elected official or you get fired. So, what I noticed in the Health Department is they were very nervous about upsetting tourists" (personal communication, September 14, 2018). Participant added, "I appreciated that and understood that, but that was a political reality as a barrier. Not so much of the information we released internally as information sharing, but what we released to the public" (personal communication, September 14, 2018).

Participant 357 stated, "within state government, many of the state government functions culturally do not see types of responses as being part of their mission or even part of their responsibility and that is going to take a cultural shift" (personal communication, September 18, 2018).

Participant 358 stated, "starting with the real politics. There are state legislators and even congressional members who seem to think that they should be privy to everything, no matter what. They get very irate when we politely decline and tell them no" (personal communication, October 3, 2018).

Participant 362 stated, “The people making decisions are not the people on the ground, they are not getting the information from people on the ground to help them guide their decisions at the top. That is the biggest problem. This is information sharing” (personal communication, September 17, 2018).

Participant 363 stated, “that really affects the intelligence community the police, fire, EMS, their budgets. I get more votes because I help the homeless or I do something with the urban stuff. I don’t get more votes by having more cops on the street” (personal communication, October 4, 2018).

Participant 364 stated, “people may have alternative motives such as, if we make our organization look better, we will get more funding next year, purchase more equipment and improve the organization” (personal communication, December 3, 2018).

Participant 365 stated, “In my experience amongst numerous administrations, politics will enhance or diminish the importance of sharing threat-related information. Politics can impact the procurement of vital equipment in information sharing and the staffing of new positions” (personal communication, January 11, 2019).

Participant 366 stated, “Because of the geography and the political climate here I think people feel they are protected. They do not feel that there is a great threat against the state of Hawaii” (personal communication, January 11, 2019). Participant 366 added, “it would be nice if everything could remain open as it did many years ago. But I think we still put many people at risk by not implementing security measures” (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 6. Participant responses were analyzed according to their perception of how politics plays a role in the sharing of threat-related information between public safety organizations. Nine of the participants stated that politics played a significant role in the sharing of threat-related information. Agency culture and information flow were themes which also ranked in the top three responses to this question. The chart in Figure 6 highlights the number of participants who mentioned certain topics in their responses to Interview Question 6.

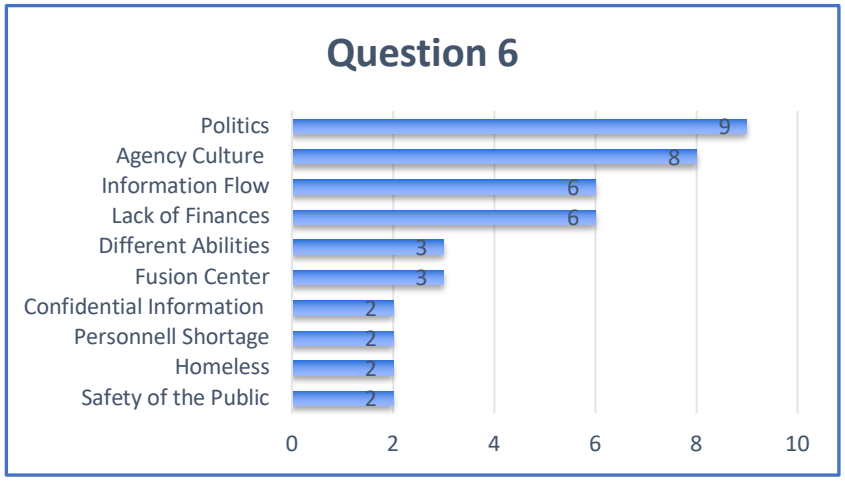

Figure 6. Comparison of topic frequency in participants' responses to Interview Question 6.

The most prominent theme in the responses to Interview Question 6 focused on politics. The participants indicated that the political environment at any given time could affect the sharing of threat-related information. State or county political leadership may request information that is sensitive, such as personally identifiable data or law enforcement sensitive information that cannot be shared outside of individuals with a legitimate need to know. Participant 358 explained, "starting with the real politics. There

are state legislators and even congressional members who seem to think that they should be privy to everything, no matter what. They get very irate when we politely decline and tell them no" (personal communication, October 3, 2018).

Within each agency politics at the leadership level also plays a role in the sharing of information. Participant 353 explained, "the importance of the fusion center. Whether they are firefighters or police officers, through the wish of the chief, if the chief wants those personnel back and staffed somewhere else then there is no one at the fusion center" (personal communication, September 18, 2018). Participant 353 added, "that's a big impact and that is a big policy decision that could play a role" (personal communication, September 18, 2018).

The second theme in the responses to this question was agency culture within an organization. According to the participants, some public safety organizations are very protective of their programs which leads to less sharing of information between agencies. A perceived competition between agencies or even between agency sponsored public safety campaigns can affect information sharing. Participant 354 stated:

> Like what we are doing here with the see something say something [campaign]. I remember going to the meetings and crime stoppers representatives were there, and they were totally against it because they had a similar program and they thought that it would interfere with their operation. They did not want us to push the agenda of the see something say something and take away from their program. So, I know that that was kind of a huge political. I guess the politics between the organizations. (Participant 354, personal communication, October 25, 2018).

Participants also described a reluctance to share due to entrenched agency culture. Participant 351 stated:

> So HPD's culture you know well, not to share, not to release but to work things internally. That is the culture of HPD. I'll tell you exactly, so when we asked the last administration for the highlights and for working with CIU (Criminal Intelligence Unit). The assistant chief who oversaw that area said yes, this makes sense of course. This person goes to the chief and it's blocked. I don't think it was politics but a culture of close hold. (Participant 351, personal communication, August 30, 2018).

The third theme in the responses to this question was information flow within and between organizations. Several participants stated that information flow within their agencies did not flow effectively from the administrative level down to operations level and from the operations level back to the administrators. It is important that the leadership of public safety organizations designate internal information flow as a priority and take the steps necessary to make it an effective part of daily operations. Participant 362 explained, “The people making decisions are not the people on the ground, they are not getting the information from people on the ground to help them guide their decisions at the top. That is the biggest problem.” (personal communication, September 17, 2018).

Interview Question 7

The question was, what can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii? The following responses were provided by the interview participants.

Participant 350 stated, “having technology to help us keep each other on the same page and communicate, you know, that's always key. Communication is key” (personal communication, August 9, 2018).

Participant 351 stated, “I'll tell you what the problem with HPD is. The problem for getting somebody assigned to the fusion center like it used to be” (personal communication, August 30, 2018).

Participant 352 stated, “involve non-law enforcement agencies in kind of lower-level more day-to-day threats. Sort of begin information sharing on some level and I would start ramping it up from there and getting it a little more sophisticated. I think that would help” (personal communication, October 3, 2018).

Participant 353 stated, “first it is what I mentioned earlier, maybe considered overlap here is that the chief of police has to buy in on the importance of participating in WSIN, HIDTA, participating in deconfliction requirements” (personal communication, September 18, 2018).

Participant 354 stated, “I think we need to get more of the organizations buy in. You saw what happened when we got our new fire chief. He pulled us out of the fusion center and did not want to have anything to do with it” (personal communication, October 25, 2018). Participant 354 also added, “to prove that it will be beneficial to everyone. That is one way to include organizations like the fire department and EMS. I think that it would be important to have a fire representative at the fusion center” (personal communication, October 25, 2018).

Participant 356 stated, “whether that be police, fire, EMS, or military, you have to have someone who reports to the highest levels assigned to disseminate and receive information” (personal communication, September 14, 2018).

Participant 357 stated, “between the federal and state levels and in particularly between the joint chiefs of staff and the military and the military command and the sharing of information with the state. I think that is an area that can be improved” (personal communication, September 18, 2018).

Participant 358 stated, “agencies that are again not used to dealing with health information or other private information it would be good if they had regular training in place for key personnel and had protocol in place on how to handle sensitive information” (personal communication, October 3, 2018).

Participant 362 stated, “better communication not only between agencies, but the agencies should share the information that they are getting from within their organizations by better communications from the boots on the ground to the administrators” (personal communication, September 17, 2018).

Participant 363 stated, “unfortunately, until we get another big 9/11 event people are not going to be freely sharing information” (personal communication, October 4, 2018). Participant 363 also added, “like I say until we get another big bang everybody is withdrawing back into their stove pipes” (personal communication, October 4, 2018).

Participant 364 stated, “create a website that everyone in the department can go to and access the same information. A shared drive or folder on the intranet for internal use,

so that everyone has the same information. It can serve as a reference" (personal communication, December 3, 2018).

Participant 365 stated, "for county fire departments, the State Fire Council provides cooperation amongst the counties by state statutes. Funding each county with one intelligence officer responsible for coordination, research, and monitoring of current and emerging threats" (personal communication, January 11, 2019).

Participant 366 stated, "understanding that the state agencies don't have the same responsibilities as the Honolulu Police Department. But respecting what they do and the training that they have and the responsibilities that they have I think would go a long way" (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 7. Participant responses were analyzed according to their opinion of what could be done to improve the sharing of threat-related information between public safety agencies in Honolulu. Five of the participants stated that agency culture, information flow, and the state fusion center were factors that may improve threat-related information sharing. The chart in Figure 7 highlights the number of participants who mentioned certain topics in

their responses to Interview Question 7.

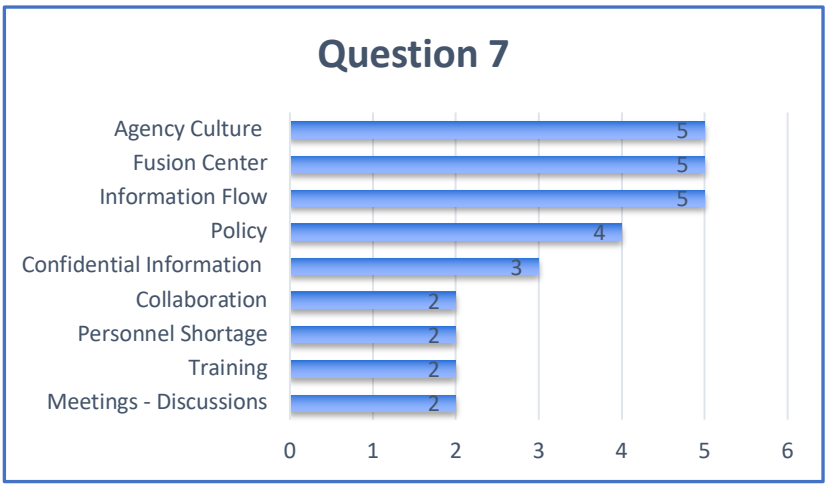

Figure 7. Comparison of topic frequency in participants' responses to Interview Question 7.

The most prominent theme in the responses to Interview Question 7 was agency culture within organizations. A topic that was mentioned several times in the responses was buy-in by the leadership of the organizations. If the chief of a department (e.g., police, fire, or EMS) does not buy-in to an initiative or program it simply will not move forward. Participant 356 explains, "I think first of all there has to be buy in from the highest levels of the agency" (personal communication, September 14, 2018).

The second theme in the responses to in this question focused on the state fusion center. Several participants stated the need to have representatives from all of the public safety organizations assigned to the fusion center. Staff shortage, lack of funding, and lack of buy-in were primary reasons why some organizations do not currently assign staff to the state fusion center. Participant 350 pointed out, "Communication is key. As you know the Hawaii State Fusion Center is really an entity that's kind of keeping this thing

together and really helping things evolve in the sharing of information" (personal communication, August 9, 2018).

The third theme in the responses to this question was information flow within and between agencies. There was a concern by several participants that information was not effectively flowing internally between the administration of the organizations and the operational staff, or boots on the ground, as one participant put it. This was a common theme throughout the study. Participant 362 explained, "better communication not only between agencies, but the agencies should share the information that they are getting from within their organizations by better communications from the boots on the ground to the administrators" (personal communication, September 17, 2018). Participant 362 added, "because right now the communication is pretty much straight down or sideways. Also, the communication that is coming down is not really needed you know, it is administrative" (personal communication, September 17, 2018).

Participant 363 stated:

> Unfortunately, until we get another big 9/11 event people are not going to be freely sharing information. Right after 9/11 if you wanted something you got it. At APEC (Asia Pacific Economic Cooperation) if we wanted to do something related to the event you got it. You want to share information, good, share that information. Like I say until we get another big bang everybody is withdrawing back into their stove pipes. (Participant 363, personal communication, October 4, 2018).

Interview Question 8

The question was, what role could agency policies, within your organization, play in improving the sharing of threat-related information? The following responses were provided by the interview participants.

Participant 350 stated, “now do I think there needs to be some level of guidance and direction, absolutely because how do you gain manpower and how do you gain funding” (personal communication, August 9, 2018)?

Participant 351 stated, “A fusion center can help coordinate that along with the FBI, that's in policy” (personal communication, August 30, 2018).

Participant 352 stated, “I don't think just making a policy is going to solve it. You really need to have the buy-in and the policy just is just a document for the steps that you take to do something” (personal communication, October 3, 2018).

Participant 353 stated, “I worked for the Honolulu Police Department. I believe the policies are critical. The reason I say that it is because it keeps our personnel safe” (personal communication, September 18, 2018).

Participant 354 stated, “I think that it would be important to have a policy so that if you saw certain things you would have to report it. Because we don’t have any policies like that currently” (personal communication, October 25, 2018).

Participant 356 stated, “having it in writing I think kind of guarantees it. I guess guarantees is to strong of a word, but it more enables a department to do the right thing” (personal communication, September 14, 2018).

Participant 357 stated, “I think where we could really make some significant gains if we began to utilize some of the available resources in terms of alerting the public more. So that they could be more prepared” (personal communication, September 18, 2018).

Participant 358 stated, “Within our organization based on our past experience, it would probably be good to have ongoing discussions within the agency or organization to determine how we might address these things in the future” (personal communication, October 3, 2018).

Participant 362 stated, “They [HPD] can make it a policy that they are going to be a part of the fusion center and share information” (personal communication, September 17, 2018). Participant 362 added, “they have different policies for SSD (Specialized Services Division) and MED (Major Events Division) they all have policies so they could assign someone to the fusion center or a group and make a policy that they will participate” (personal communication, September 17, 2018).

Participant 363 stated, “policy on the big government side is knock down those walls of information sharing between operations and intelligence. There is still that division” (personal communication, October 4, 2018).

Participant 364 stated, “I think policies keep people accountable. Accountability is a big one. No one can say I didn’t know, or I didn’t have access, or no one can point the finger at anyone else” (personal communication, December 3, 2018).

Participant 365 stated, “Fire departments with organized top-down hierarchy are reinforced to up-channel any threat-related information as soon as possible. Those

subject matter experts work with leadership to provide a uniform/unified posture or response" (personal communication, January 11, 2019).

Participant 366 stated, "to codify the SLEC (State Law Enforcement Council). I think that is one thing. I think the other thing would be to have representation of all of these agencies in the fusion center" (personal communication, January 11, 2019).

Interpretation of findings for Interview Question 8. Participant responses were analyzed according to what role agency policies played in improving the sharing of threat-related information between public safety organizations. Nine of the participants stated that specific agency policies may improve threat-related information sharing. The fusion center and information flow were themes which also ranked in the top three responses to this question. The chart in Figure 8 highlights the number of participants who mentioned certain topics in their responses to Interview Question 8.

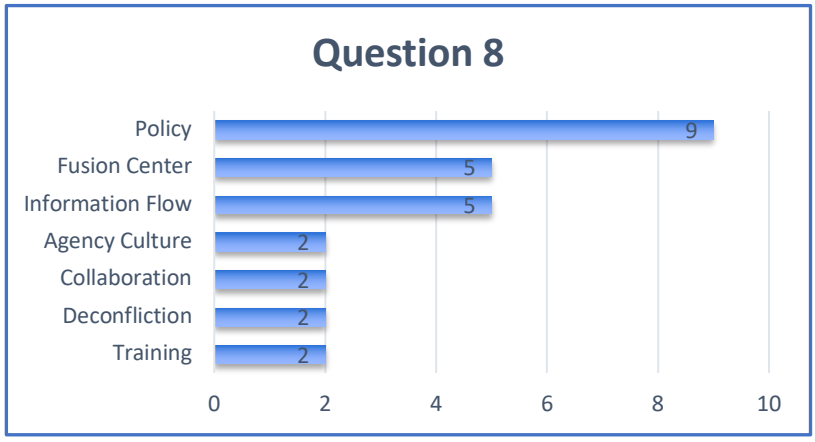

Figure 8. Comparison of topic frequency in participants' responses to Interview Question 8.

The most prominent theme in the responses to Interview Question 8 centered around agency policies. A majority of the participants agreed that agency policies were

needed to enhance the sharing of threat-related information. Policies help keep responders safe and ensure that individuals stay involved in the information sharing process and are not allowed to regress to a pre 9/11 culture of holding information within each organization. Participant 353 stated, "I worked for the Honolulu Police Department. I believe the policies are critical. The reason I say that it is because it keeps our personnel safe" (personal communication, September 18, 2018). Participant 353 also added, "there are many things that we have no control of but there are things that we do have control of and deconfliction and case activation procedures are critical to keeping our people safe" (personal communication, September 18, 2018).

Participant 364 explained, "I think policies keep people accountable. Accountability is a big one. No one can say I didn't know, or I didn't have access, or no one can point the finger at anyone else" (personal communication, December 3, 2018).

The second most prominent theme in the responses to this question was public safety participation in the state fusion center. Several of the participants stated that it is vitally important for public safety organizations to assign a liaison to the fusion center. The U.S. Department of Homeland Security (2018) defines state and major urban area fusion centers as organizations that "operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial; and private sector partners" (para.1). Participant 366 explained:

> I think the other thing would be to have representation of all of these agencies in the Fusion Center, so that we could actually gain their confidence and they would

> feel like they are part of what's going on when it comes to the security and the protection of our community. Because right now I do not feel that outside of the fusion center, even my own office, I do not feel that they understand all of the threats that are out there. All of the areas that we need to be watching. You have got to have that influence that brings it together, but right now I think everyone is operating in their own little world and when they have to, then they support each other. (Participant 366, personal communication, January 11, 2019).

The third most prominent theme in the responses to this question was information flow within and between organizations. This was a theme highlighted multiple times in this study. There was a concern by several participants that information was not effectively flowing between segments within the organizations. Participant 363 stated, "policy on the big government side is knock down those walls of information sharing between operations and intelligence. There is still that division" (personal communication, October 4, 2018). Participant 363 also added, "the agents find out the information and say I don't want to share that with the intelligence side because then it doesn't become my case, my information" (personal communication, October 4, 2018).

Interview Question 9

The question was, please describe any past lessons learned at your organization that could improve the exchange of threat-related information between public safety organizations. The following responses were provided by the interview participants.

Participant 350 stated, “they're asking for help and their giving us information and how we can help and how we did help. That's what's got to be encouraged” (personal communication, August 9, 2018).

Participant 351 stated, “set your objectives, set your goals, set your objectives and make your strategies” (personal communication, August 30, 2018).

Participant 352 stated, “I am for some cross training of medical people and maybe even just simple cross training of some of the law-enforcement guys” (personal communication, October 3, 2018). Participant 352 added, “they call it tactical EMS, and they have tactical physicians or physicians that are on their EMS staff. Like through the partnerships with the university or whatever and so they have a high degree of medical expertise” (personal communication, October 3, 2018).

Participant 353 stated, “I was a commander of a narcotics vice division at one time and I had a drug unit report to me that they conducted an undercover investigation and they followed the procedures required for a critical event deconfliction” (personal communication, September 18, 2018). Participant 353 added, “when they went to the scene that they identified, they ran across their brother officers from HPD at the same location also in plain clothes, which was a conflict” (personal communication, September 18, 2018).

Participant 354 stated:

> I think the improvement on sharing information of stuff that you don’t really want to get out to the public. The confidential information that may have to do with law enforcement. Our agency just dropped all of that stuff. I think that it was a huge

help when we were actually using it. Everyone had an opportunity to log into HSIN and check out the information. The last two years before I retired and no one was using it, so I think a lot of the information sharing has stopped at least within my department. You know our department used to send out threat-related stuff as far as being exposed to something, like when we are responding to calls and stuff. But they stopped sending that kind of stuff out and put it into an area like a doc you share, so that you would have to go look it up. Guys stop going there because they had to actually look it up and it was more of a hassle. So, as far as the fire department is concerned, I think information sharing has gotten much worse since APEC in 2011. Information sharing has really gotten worse as far as dangers and things like that. (Participant 354, personal communication, October 25, 2018).

Participant 356 stated:

Again, I touched on some of these in the earlier discussions but number one, working with the health department. They did not have I thought an active role in the fusion center and so their information coming in was not good and their receiving information was not good. So, again this sensitivity to tourism and having to kind of clear everything with them before we put it into memos to the other city agencies was an issue. But again, I learned to kind of work with them and we learned a system to kind of keep them happy and to keep their executive branch happy. So, we could share biological threat information and again not necessarily biological terrorism, but just naturally occurring diseases such as flu

and other things to make our first responders aware. (Participant 356, personal communication, September 14, 2018).

Participant 357 stated:

The biggest lesson is the need for immediate sharing between the leadership of the organizations that are responding. I think a really good one was again that nuclear attack warning that we had. When that alert came out falsely within three minutes our police chief knew that it was a false alert. That was because HPD dispatch was extremely proactive in terms of reaching out to PACOM (U.S. Pacific Command) to try to validate whether we actually had an incoming missile. They found out that it was not true. So, that information flowed out to the police officers in the field who had begun to go through communities making PA announcements, but it did not flow to the leadership of the fire department or the emergency services department. So, as a consequence, because we were unaware that one of our key partners had validated that it was a false alert and because we had not heard anything from the governor, we shut down our EMS service for 16 minutes which was protocol in that circumstance. So that could have been avoided. So that was a big lesson learned. Thus, the effort to bring these key decision-makers to a single text platform to share that kind of information. (Participant 357, personal communication, September 18, 2018).

Participant 358 stated:

If the legislation actually gave me the staff that I needed it would help. Unfortunately, this unrealistic expectation that we can monitor for the diseases,

> investigate them, stamp them out and then also establish all the protocols and agreements and to deal with all the administrative stuff at the same time. That's the challenge for us. That would be the most ideal if we had staff that could work on those things. That would be helpful. It still doesn't obviate the need to reach out to partners and have ongoing discussions. (Participant 358, personal communication, October 3, 2018).

Participant 362 stated, "when my organization supported the fusion center by putting someone in it, we were doing great things. Information was getting shared, information from databases inside the police department was getting shared with other agencies" (personal communication, September 17, 2018).

Participant 363 stated:

> My first one was APEC. Everyone was sitting on that main floor. Everyone saw the same information on the LEO (FBI Law Enforcement Online) board at the same time. They were all sitting in a big room together. We had a little intelligence cell off to the side doing classified stuff. When we found information that we could share we popped it over onto the LEO board. Once we lost that facility, that cohesiveness then we lost the ability to share quickly with everybody. Everybody went back to their agency and said oh that was nice. We saved the world from unattended packages. But that was the best information sharing that I have ever seen. That was a good lesson learned. It was expensive but everyone was sleeping better at night because everyone on these islands knew

> the same information at the same time. (Participant 363, personal communication, October 4, 2018).

Participant 364 stated, "in 2011, I know that we worked with the 93rd CST a lot. I think that we had a really good relationship with them. We also had a good relationship with the fusion center. At that time information flowed very smoothly" (personal communication, December 3, 2018).

Participant 365 stated, "even with all of the lessons learned from 9/11 and the changes made, at many times there is no sense of urgency" (personal communication, January 11, 2019).

Participant 366 stated:

> I think that the last half of the year all the events that we have had in the state. I think has helped bring folks together, but we don't have enough resources to have it on a continual basis and I think we saw that in December. I don't know what we can do about that. Because we are not going to increase their resources, so how do we increase the support or how do we make sure that we have good support for everything versus just a few. (Participant 366, personal communication, January 11, 2019).

Interpretation of findings for Interview Question 9. Participant responses were analyzed according to past lessons learned at their organization that could improve the exchange of threat-related information between public safety organizations. Eight of the participants stated that improved information flow within and between organizations could improve information sharing. Collaboration between organizations and the

challenges involved in sharing confidential information also ranked in the top three responses to this question. The chart in Figure 9 highlights the number of participants who mentioned certain topics in their responses to Interview Question 9.

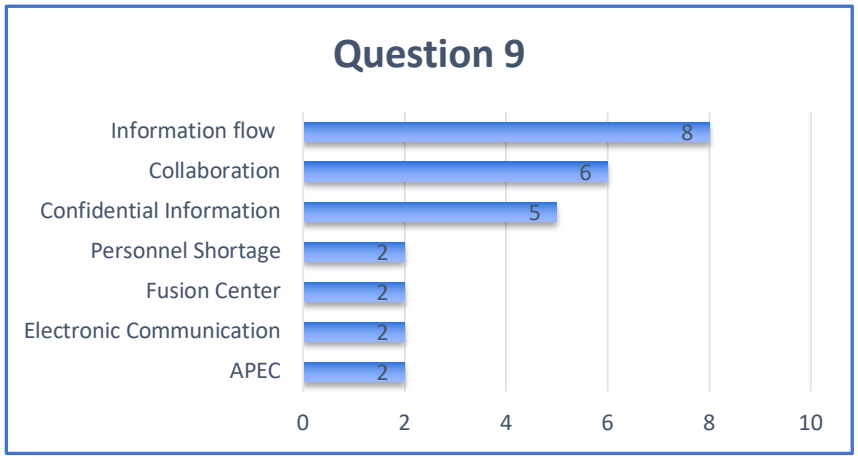

Figure 9. Comparison of topic frequency in participants' responses to Interview Question 9.

The most prominent theme in the responses to Interview Question 9 was information flow within and between organizations. Eight of the participants stated that information flow within organizations and between organizations is vital; however, many believe that information flow has declined since the attacks of 9/11. Participant 362 stated:

> Here is the biggest thing, when my organization supported the fusion center by putting someone in it, we were doing great things. Information was getting shared, information from databases inside the police department was getting shared with other agencies. Other agencies information was getting shared with the police department. This was nationwide and even worldwide. We caught

> people because we were sharing information. Now here's the lesson, our police department does not support the fusion center by putting someone there and that communication has been cut off. (Participant 362, personal communication, September 17, 2018).
>
> Participant 354 explained:
>
> I think the improvement on sharing information of stuff that you don't really want to get out to the public. The confidential information that may have to do with law enforcement. Our agency just dropped all of that stuff. I think that it was a huge help when we were actually using it. Everyone had an opportunity to log into HSIN and check out the information. The last two years before I retired and no one was using it, so I think a lot of the information sharing has stopped at least within my department. (Participant 354, personal communication, October 25, 2018).

The second theme in the responses to this question was collaboration. Six of the participants stated that collaboration was very important in the sharing of information. Not only collaboration when an event happens, but ongoing collaboration between organizations on a daily basis. The sharing of information between agencies builds a common operational picture of the current threat environment. Several participants believe some of the collaborative environment between agencies has declined since the attacks of 9/11. Participant 363 pointed out that while working at the APEC event in 2011, "Everyone was sitting on that main floor. Everyone saw the same information on

the LEO (FBI Law Enforcement Online) board at the same time. They were all sitting in a big room together" (personal communication, October 4, 2018).

The third theme in the responses to this question centered around the complexity of sharing confidential and protected information between public safety organizations. Several participants indicated that confidential information inherently slows information flow because only those individuals with a need to know can receive the information. Often, only the leadership of organizations received the highly confidential or sensitive information. It takes specially trained analysts additional time to filter out the confidential content before it can be shared between agencies, if it can be shared at all. Participant 357 pointed out, "The biggest lesson is the need for immediate sharing between the leadership of the organizations that are responding" (personal communication, September 18, 2018).

A discrepant case in the responses to this question focused on critical event deconfliction of law enforcement active operations to ensure the safety of responders. When undercover officers initiate field operations it is important that those operations are deconflicted to ensure that another law enforcement agency is not targeting the same suspect at the same time. Deconfliction is extremely important for police officer safety but would not typically be utilized by other public safety organizations. Participant 353 described deconfliction:

> I was a commander of a narcotics vice division at one time and I had a drug unit report to me that they conducted an undercover investigation and they followed the procedures required for a critical event deconfliction. However, when they went to the scene that they identified they ran across their brother officers from

> HPD at the same location also in plain clothes, which was a conflict. If I remember correctly, the plan to make a drug buy wasn't successful because they saw other police officers there. They recognized other police officers there in plain clothes, so the operation was called to a halt and the supervisor there put a hold on the investigation and pulled out. (Participant 353, personal communication, September 18, 2018).

Interview Question 10

The question was, what is your perception of the current state of threat-related information exchange between public safety agencies in Honolulu, Hawaii? The following responses were provided by the interview participants.

Participant 350 stated:

> I think it's really good. I really do think here in Honolulu we're doing a great job and I say that because I witnessed it. Like I was kind of using an example of the new techniques and tactics that we happen to use by getting police, fire, and EMS together. To go to these just horrific events, should they ever happen, and I hope they never happen, but to see them working together and training together for what we hope never happens is a sign of healthy relationships. I think if you talk about specifically sharing threat-related information and they've got to probably be. I'd say probably at a 9 (on a rating scale from 1 to 10, with 1 representing low and 10 representing a high level of information sharing) and the only reason it's a 9 and not a 10 is that 'threat' is sometimes defined or perceived differently across

those cultures you know, it's just different cultures as to what are threats. (Participant 350, personal communication, August 9, 2018).

Participant 351 stated:

So externally when we get external products, we're able to disseminate them. Exchange of internal information within the state then there's a gap. We're not getting data. Is it improving? Well yes, it is improving. We are going to join with WSIN. That is good. I would rate the current state of information exchange at a 3, because if there is criminality involved it's going to get to whoever's got to investigate the case. That's going to happen, but as far as the overall protection of everybody it's not. (Participant 351, personal communication, August 30, 2018).

Participant 352 stated:

I think that the medical side, both EMS as well as hospitals are slowly starting to see the importance of preparing for active threat response. I think the agencies are a little less siloed than they used to be and I think the realization is there that this is important but the action is not there yet. At the same time that they see it as important and realize that we really should start doing something, that something hasn't necessarily been defined yet or codified, and I think we still need that mechanism for medical review of intelligence info. I think that's sort of a kind of lynchpin, if you will, that will tie a lot of things together. I think the realizations there just the action is slow in coming. So, I think there's good, really good information exchange among the law enforcement side of the house. I think there's poor information exchange between law enforcement and health. It's

gradually getting better though. (Participant 352, personal communication, October 3, 2018).

Participant 353 stated:

Since I am retired, I will say that before I retired I believe that it was good and on a scale of 1 to 10, and this is anecdotal there is no scientific formula to what I have to say, I think it would it would be high. I would say it is at least an 8, maybe a 9. The reason I say that is because of the relationships I had and the relationships I saw between agencies at the various levels. The meetings that we had, the attendance at the HIDTA meetings and the attendance at the other conferences, for example HSLEOA (Hawaii State Law Enforcement Officials Association) conferences. I attend the FBI National Academy re-trainer every year and the attendance is typically high. (Participant 353, personal communication, September 18, 2018).

Participant 354 stated:

I think it is a lot less than it was during APEC in 2011. Gradually after APEC things kind of died down and then once we pulled our personnel from the fusion center, information I think it really went down. I tried to stay involved for a little while and go to the FBI meetings and things like that. I also tried to push our HAZMAT (hazardous material SMEs) guys to go, and I think they did for a certain amount of time, but I'm not sure. So, I saw how much the information sharing decreased. It is sad to think that something has to happen before they realize that it is important and a help to everybody. There is no reason why we

couldn’t have somebody partially going into the fusion center a few days a week or something. I just can’t see what the real drawback is to that. (Participant 354, personal communication, October 25, 2018).

Participant 356 stated:

I would give it a 7.5. I'll say an 8.0. I think there's always room for improvement. So, here's what I base by my number on. Number one, if all agencies had an appointed designee to the fusion center. That to me would make it have a higher rating. If the fusion center did not have a permanent director and staff, that would make my rating go lower, and if all agencies embraced the fusion center with robust two-way information sharing that would make my rating go higher. If there was funding, city, state, and federal for the fusion center that would make my rating go higher. So, I leave it at a 7 to 8 range because I don't think we're quite there with what I just said. But we're better I think than we were ten years ago. So, I think to get to a 10, to be the best you can be, you have to have all the agencies participating and if somebody's not physically there, they at least have to be available electronically to receive and give information. All agencies have to contribute to share reports and to receive reports and there has to be adequate funding. At least at one or two levels, but preferably three levels of government to ensure an adequate and robust response capability and sharing capability. (Participant 356, personal communication, September 14, 2018).

Participant 357 stated, “about an 8 out of 10. I think I kind of covered where we are going to move it up to a 9, or a 10, and how we are going to do it in our earlier conversation” (personal communication, September 18, 2018).

Participant 358 stated:

> I think if we are just talking purely public safety or law enforcement with public health, I honestly think that it is fairly good. If you threw in the emergency management agencies, I would say that it depends. If we are just talking law-enforcement and us, I think that it is pretty good. We have a low threshold to reach out to our law enforcement partners whether we are talking about HPD, our state level public safety division, or FBI. I think we have a very low threshold to reach out to them and I think vice versa. I know there is certain information that they do not share with us and honestly, as I told the FBI guys if you don’t think it is pertinent to the public health and it is more of a national security issue then I don’t mind not knowing. So, but I think we have good relationships with our law enforcement partners. (Participant 358, personal communication, October 3, 2018).

Participant 362 stated:

> I would say it is a 5. When a real threat is known in an agency, secret service, or sheriffs, or police and they find out real credible information that is definitely a public safety issue they will put it out to the different agencies. This also goes for fire, EMS, and public health, if they deemed that those organizations should know. So, only if, and these cases are few and far between. That is why I say it is

a 5 at best. It could go up dramatically just by putting someone in the fusion center and more than one person. One is none, two is one. Three is better. They need an HPD lieutenant or a sergeant and some analysts to be able to really get involved and share information. With that they would have to write a policy or change existing policies. They have an information sharing policy right now, you don't do it, and the only time you can send out a report is in the records division. They could just change that. The unit at the fusion center is authorized to share information within their training that kind of thing. And that way the policy wouldn't have to be written, it could just be tweaked. (Participant 362, personal communication, September 17, 2018).

Participant 363 stated:

I would give it a 5. Because we went from the perfect example of APEC and we quickly digressed right back to 50% or less of information being shared that should be shared. So, I would give it a 5. If we can get back to that model where you don't have a need to know, you have a need to share, or something is going to be missed and something is going to blow up. Once we have an event again the politicians will leave the homeless alone and not worry about saving the whales and say, oh, we've got to save the people. We will be in that mode for a about a year or two and then back to saving the whales. (Participant 363, personal communication, October 4, 2018).

Participant 364 stated:

> On a scale of 1 to 10, I would say the current amount of information sharing is a 1 or a 2. Our department keeps all of the information at the top. Everything is held so secret and then one person finds out and it spreads almost like a rumor and then everyone wants to know. (Participant 364, personal communication, December 3, 2018).

Participant 365 stated, "Public safety agencies take a much lazier approach to threat-related information due to the remote location of Hawaii; the difficulty to get in and out of the islands undetected; and with hardened high value targets" (personal communication, January 11, 2019).

Participant 366 stated:

> Well I think that it is good. I think that the fusion center does what it can. But I think that our real issue is, does everyone look at this, does everyone read it, does everyone take it to heart as to what is out there? Then again, I think there is apathy in our political leadership. To me everyone is reactive. Right now, we get a few requests, but most folks will be reactive if something happens, versus how do we look at this now. With the improvements that we can all do and hopefully have better day-to-day operations, versus waiting until something happens and then everything has to come together at once. You don't have any say. And so, I think that's our biggest problem. If I were to grade it 1 to 10, I would give the fusion center probably about an 8. But I would give the public safety folks probably about a 4 or 5. The same for our political leadership, a 4 or a 5. We can only do so much at the fusion center. Everyone else has to help us and that is

where I think that we are lacking. (Participant 366, personal communication, January 11, 2019).

Interpretation of findings for Interview Question 10. Participant responses were analyzed according to their perception of the current state of threat-related information exchange between public safety agencies in Honolulu. Five of the participants stated that public safety agency participation the fusion center was a factor that may improve information sharing. Collaboration between organizations and different abilities of public safety organizations also ranked in the top three responses to this question. The chart in Figure 10 highlights the number of participants who mentioned certain topics in their responses to Interview Question 10.

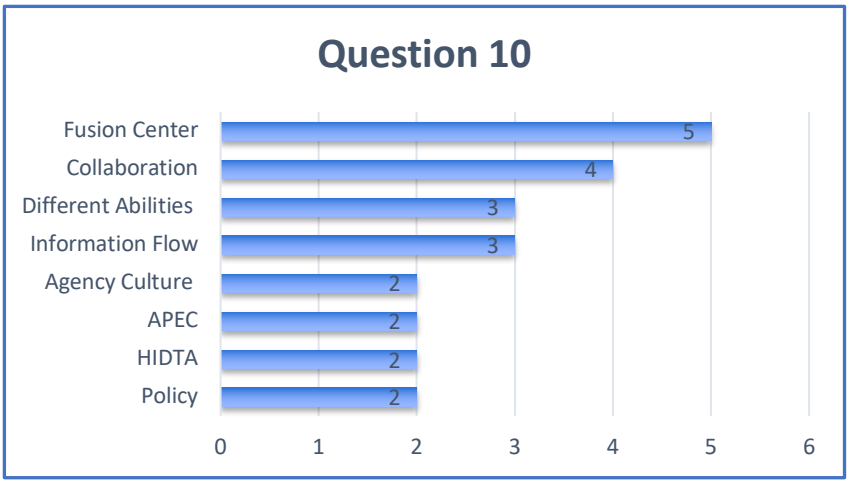

Figure 10. Comparison of topic frequency in participants' responses to Interview Question 10.

The most prominent theme in the responses to Interview Question 10 focused on the Hawaii State Fusion Center. Five participants stated that consistent agency participation in the fusion center would improve threat-related information sharing. They

indicated that information sharing on a daily basis in a designated facility such as fusion center is important. It is also important that information that is shared is actually reviewed and acted upon by the agencies. Participant 366 explained, “Well I think that it is good. I think that the fusion center does what it can. But I think that our real issue is, does everyone look at this, does everyone read it, does everyone take it to heart” (personal communication, January 11, 2019).

Participant 362 stated, “it is a 5 at best. It could go up dramatically just by putting someone in the fusion center, and more than one person. One is none, two is one. Three is better” (personal communication, September 17, 2018).

Participant 363 stated, “I would give it a 5. Because we went from the perfect example of APEC and we quickly digressed right back to 50% or less of information being shared that should be shared. So, I would give it a 5” (Personal communication, October 4, 2018).

Participant 356 stated:

> I would give it a 7.5. I'll say an 8.0. I think there's always room for improvement. So, here's what I base by my number on. Number one, if all agencies had an appointed designee to the fusion center. That to me would make it have a higher rating. If the fusion center did not have a permanent director and staff, that would make my rating go lower, and if all agencies embraced the fusion center with robust two-way information sharing, that would make my rating go higher. (Participant 356, personal communication, September 14, 2018).

The second theme in the responses to this question was the collaboration between agencies. Many of the participants believed that there was collaboration between agencies due to relationships between individuals in different organizations, but it was not consistent and ongoing. Agencies seemed to collaborate when needed on a certain case or event and then regress back into a non-sharing environment when the event was over. Participant 353 stated:

> Since I am retired, I will say that before I retired, I believe that it was good and on a scale of 1 to 10, and this is anecdotal there is no scientific formula to what I have to say, I think it would it would be high. I would say it is at least an 8, maybe a 9. The reason I say that is because of the relationships I had and the relationships I saw between agencies at the various levels. (Participant 353, personal communication, September 18, 2018).

The third theme in the answers to this question centered around the different abilities of public safety organizations. Several of the participants stated that different public safety organizations have expertise in different areas of public safety. As an example, the Honolulu Fire Department hazardous materials experts may be aware of a threat or hazard (e.g. toxic chemical release) that law enforcement and/or EMS personnel may be unaware of. Participant 358 explained:

> I was recently meeting with the new point of contact for us with the FBI who heads up their WMD (weapons of mass destruction) program. We were meeting to just touch base. Generally, when you have a good relationship with law enforcement and public safety, I think that it is important to have an ongoing

> discussion. Because there may be things that they are aware of that they don't realize to let us know about and visa-versa. I gave him a whole bunch of real-life examples of where I may not know if there is anything that they might be interested in. So, I said to him, look if you hear about something please don't hesitate to reach out to me and ask me, have we considered this, or is there any potential for law enforcement issues or security issues that they need to be aware of. (Participant 358, personal communication, October 3, 2018).

Nine participants ranked what they believed to be the current state of threat-related information sharing between public safety organizations in Honolulu. This ranking was based on a rating scale of 1 to 10, with 1 representing low and 10 representing a high level of information sharing. This was very interesting because several of the participants were firm in their rankings in the lower ranges between 1 and 3, and other participants believed information sharing between agencies was actually very good by ranking in the 8 to 9 range. The average of the nine participant's rankings was 5.9.

Summary

Chapter 4 highlighted multiple aspects of public safety organizations in Honolulu sharing threat-related information. All participants agreed that information sharing between public safety organizations has improved since the attacks of 9/11; however, many of the participants felt that there is more work that needs to be done. This research uncovered four overarching themes.

The first overarching theme in the data focused on the flow of information within and between agencies. Several participants stated that information did not flow smoothly within their departments and consequently out to other organizations. The problem seemed to be intensified by information being shared only during intermittent urgent situations rather than establishing an ongoing information sharing environment. A lack of ongoing collaboration between public safety organizations was the second overarching theme in the data. An ongoing collaborative environment allows multiple agencies with different perspectives to view the threat information and analyze it from different points of view in real-time. Agency participation with the state fusion center was the third overarching theme. Many of the participants stated that it is important that their agency participate in the state fusion center, so that threat-related information can be disseminated across all public safety agencies simultaneously. The complexity of sharing confidential and protected information between public safety organizations was the fourth overarching theme. Often, threat-related data contains confidential personal identifiable information (PII), and/or protected health information (PHI), or sensitive information pertaining to ongoing law-enforcement investigations and therefore can be difficult to share.

Chapter 5 will discuss ramifications of the data collected and recommendations to improve the sharing of threat-related information between public safety agencies in Honolulu. It includes sections on interpretations of the findings, limitations and delimitations of the study, recommendations, implications, and a concise conclusion.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this qualitative exploratory case study was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire, EMS, and public health) in Honolulu, Hawaii. I focused on Honolulu for several reasons. It is a moderate-sized city and faces many of the same challenges as other cities in the continental United States, including the need to share information across agencies to manage emerging threat-related issues. However, Honolulu is unique because of its isolation, being approximately 2,500 miles from the mainland. As a result, there is an increased need to ensure interagency communication is occurring to facilitate the region's ability to manage a large-scale public safety event without immediate assistance from other states.

The gap in the literature is that researchers do not know how public safety organizations communicate threat-related information at the local level. Because it is essential that agencies communicate threat-related information effectively, due to their unique situation, an exploratory case study of Honolulu public safety agencies served as an excellent opportunity for this research. The findings provided a unique understanding of how public safety organizations that currently share threat-related information have encountered challenges and how these challenges may differ between organizations. I determined that a qualitative research design was the best method to answer this study's research questions. I collected data through interviews with SMEs, either currently active or recently retired from four different fields of public safety in Honolulu. The primary

source of data was gathered from conversational style discussions with participants utilizing open-ended questions.

Interpretation of Findings

The findings of this study clearly identified several important themes related to sharing threat-related information between public safety organizations in Honolulu, Hawaii. The findings also confirmed my rationale for using the conceptual framework of general systems theory ("General Systems Theory," 2014) in that the theory effectively described how information is exchanged between public safety organizations to protect the population from attacks. The theory also provided a conceptual platform to explore the specific research questions of this study.

General system theory is often described as "the trans disciplinary study of the abstract organization of phenomena, independent of their substance, type, or spatial or temporal scale of existence" ("Communication Theories," 2019, p. 32). Systems are essentially a set of objects, or variables "that affect one another within an environment and form a larger pattern that is different from any of the parts" ("Communication Theories," 2019, p. 32). Because elements in systems are constantly interacting with one another, when one part of a system changes it results in a change somewhere else within the system ("Communication Theories," 2019, p. 32).

In the literature review for this study, the article entitled "Surveillance and Resilience in Theory and Practice" by Raab et al. (2015) indicated that "a system may not only react to environmental effects by changing its internal properties or organization, but also act on and change its environment, bringing about a new relationship or a new

equilibrium" (p. 26). A general systems framework is effective at illuminating complex collaborative relationships between public safety organizations in rapidly changing environments.

In the article entitled "Practical Challenges of Systems Thinking and Modeling in Public Health," William et al., (2006) explained that utilizing a systems perspective along with incorporating systems modeling in public health could eventually lead to better and more effective public health organizations across the nation. William et al., stated "ambitious attempts are under way to focus practitioners on improving overall system performance" (p. 540). Systems theory is useful when studying the organizational changes and development of a community's public safety system because it allows the researcher to explore the interconnection between individual agencies or subsystems. When public safety organizations within the same region share relevant threat information with one another, it prompts other agencies within that region to prepare for or possibly counter the threat (Carter et al., 2017). Government public safety agencies work together as a system to protect the public ("Public Safety," 2011). Therefore, if miscommunication of threat-related information occurs in one agency within a system, it can lead to poor operational decisions being made in another agency within the system, and potentially lead to a failure of the system to protect the public.

A careful review of the literature helped me determine the relevant challenges of sharing threat-related information. Public safety agencies across the United States extract threat-related information from the Internet and other openly available sources (Chermak et al., 2013). The challenge is how to effectively share this information between public

safety agencies (Carter & Rip, 2013). Currently, there is not a clear understanding of the benefits and challenges of information sharing between local public safety agencies, based on my review of the literature. There appears to be extensive data about how federal agencies exchange threat-related information (e.g., Bharosa, Lee, & Janssen, 2010; Carter et al., 2017; Vacca, 2019), yet there is a lack of information about how local public safety agencies share this same type of data.

Public safety systems are complex, involving large numbers of highly trained professionals interacting with multiple organizations and the general public on a continual basis. Kozuch and Sienkiewicz-Malyjurek (2015) point out that "the process of information sharing in complex systems is multi-dimensional, asymmetrical and dynamic" (p. 727). It involves numerous organizations within local public safety systems communicating effectively on multiple levels to deliver accurate information to the first responders when needed. Many public safety organizations across the United States share information through emergency management agencies and other associations, such as state fusion centers, which were specifically developed to improve coordination and information exchange (Stone, 2015). This information exchange occurs in various forms depending on the organizations involved and the interagency communication structure of the local municipalities.

In theory, local public safety agencies have excellent interagency communication and respond effectively when a public safety event happens. Yet, it is not known if this is the case because minimal research has been done in this area (Chermak et al., 2013). Threat-related information sharing between local agencies is proving to be much more

difficult than it once appeared. What scholars do not know from the current literature are the challenges local public safety agencies face when sharing threat-related information between one another for the purpose of providing public safety. This lack of knowledge is problematic because local agencies hold the primary responsibility of responding to violent public safety threats. Scholars do not fully understand the benefits and challenges of collaboration among these agencies due to "relatively minimal scholarly attention" to this issue (Carter et al., 2017, p. 1).

There is reliable information in the literature about the sharing of information between federal and local agencies, but there is a lack of knowledge of information sharing between local agencies. Local public safety agencies are on the front lines of the struggle against terrorism and targeted violence and are literally the nation's first layer of defense. It is not just threat-related information sharing between law enforcement agencies that is important; we need to see this communication across all public safety agencies including fire services, EMS, and public health. This study identified four important themes related to sharing threat-related information between public safety organizations in Honolulu, Hawaii: 1) information flow within and between public safety organizations, 2) collaboration between public safety organizations, 3) participation with the state fusion center, and 4) the complexity of sharing confidential and protected information between public safety organizations.

The most prominent theme focused on information flow within and between public safety organizations. Data from this study's literature review reveled that information flow within public safety organizations is a complex process. Kozuch and

Sienkiewicz-Malyjurek (2015) pointed out, “The process of information sharing in complex systems is multi-dimensional, asymmetrical and dynamic” (p.727). It involves numerous organizations within local public safety systems communicating effectively on multiple levels to deliver accurate information to the first responders when needed. Participants from several Honolulu public safety organizations were concerned that information did not flow smoothly within their departments and subsequently out to other organizations. Although most participants acknowledged that when urgent events occurred, information flow ramped up between public safety organizations to address the event. Once the event was concluded however, information flow subsided back to a less than ideal level.

What appears to be missing is a constant and ongoing exchange of threat-related information, which was independent of urgent threat events. Several study participants were concerned that much of the information may not flow effectively from the administrative level to the operations level. Also, a concern was that the information was filtered as it moved down through the organization and across to other agencies. This filtering of information may potentially leave out important details other organizations could use to identify threats to the public.

The study participants were concerned that if information is not shared on a continual basis, threat-related information may become siloed within an organization. After an urgent event happens, unfortunately it is too late to analyze threat-related information that might have been used to prevent the event at the outset. Data from this study’s literature review demonstrated that predictive analysis may assist in defusing

events before they occur. Taylor and Russell (2011) explained, “The strategic integration of intelligence, with an emphasis on predictive analysis derived from the discovery of hard facts, information, patterns, and good crime analysis defines intelligence-led policing” (p. 185). Relying solidly on information technology, intelligence lead policing may help combat crime by significantly increasing intelligence decision-making (Bharosa, Lee, and Janssen, 2010). Agencies in Honolulu are currently communicating via an information flow within and between organizations; however, this flow of information is intermittent. Establishing an ongoing information sharing environment between organizations is necessary to ensure that information is effectively shared in an all situations.

The second important theme identified in the study focused on collaboration between public safety organizations. When organizations collaborate on a regular basis it allows information to be shared and viewed from different perspectives in real-time. This allows organizations a common operating picture of emerging threats. Participants stated that a significant benefit of sharing information is this continuous awareness of threats to the public. Some participants believed that there was collaboration between agencies due to relationships between individuals in different organizations, but it was not consistent and ongoing. Agencies seemed to collaborate when needed on a certain case or event, and then regress back into a non-sharing environment when the event was over. Several participants stated that ongoing collaboration was vitally important to public safety but was often overlooked due to personnel shortages and the daily race to keep up with

operational workloads. Because agencies have different skills and expertise it is important that they actively collaborate on the analysis of threat-related information.

The third important theme was participation with the state fusion center. State fusion centers' principal mission across the nation is to share information between law enforcement and public safety organizations at the federal, state, and local level. All participants were aware of the state fusion center, but not all organizations assigned personnel to the fusion center. Data from this study's literature review confirmed that participation with state fusion centers nationwide is increasing. Taylor and Russell (2011) argued since the attacks of 911 there are now hundreds of government and private organizations involved in homeland security and intelligence collection activities. They pointed out that before the attacks, sharing of intelligence between public safety agencies was severely lacking (p. 184). Currently, public safety agencies throughout the nation are beginning to participate in the nationwide network of fusion centers in an effort to better protect the public.

Some Honolulu public safety organizations have a long history of holding information within the agency. Long-held organizational cultural beliefs that law enforcement information should stay within law enforcement agencies is difficult to change. Participant 353 explained:

> Sharing of information between public safety organizations, or for that matter within units within an organization is a newer phenomenon. I will tell you 30 years ago people didn't tell anyone about their investigations, they would not to tell other people within the police department for example, or they wouldn't tell

> federal law enforcement or other state agencies. They just didn't tell anyone because it was a need to know situation. (Participant 353, personal communication, September 18, 2018).

Ongoing agency participation with the state fusion center is vitally important in order to allow threat-related information to be analyzed by multiple agencies with different skills and then disseminated across all public safety agencies simultaneously.

The final theme in this study was the complexity of sharing confidential and protected information between public safety organizations. Often, threat-related data contains very confidential PII and/or PHI, or information pertaining to ongoing law-enforcement investigations. Data from this study's literature review demonstrated that health and medical issues are extremely important to the safety of the public and many public safety organizations integrate medical analysts into their analytical staff to assist in the sharing of health-related information (Carter and Rip, 2012). However, this type of information can be difficult to share to other parties. Federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FIRPA) come into play, which can impede information sharing. Ongoing law enforcement investigations containing sensitive criminal data may also impede the process of sharing threat-related information between organizations. Threat-related information often contains highly protected, or law enforcement sensitive information, and is difficult to share between agencies. It is important that agencies develop a policy-based process, through ongoing collaboration, to share this sensitive information.

There is a chance that poor information flow, poor collaboration, and inadequate participation in fusion centers could possibly allow another catastrophic man-made terrorist event to occur. This type of catastrophe would likely temporarily improve interagency threat-related information sharing due to an increase in national security concerns by all public safety professionals involved. Nonetheless, eventually, the country would lapse back into mediocrity and the cycle would continue. The eventual retirement of public safety officials with decision-making authority would be replaced by those that do not see prevention as important as those that were involved in the last catastrophic event. Other concerns and issues in organizations, such as organizational growth, fiscal budgets, hiring new employees, etc., will become the priorities pushing aside the priority of information gathering and sharing, collaboration, and fusion center participation.

The results of this study will create positive social change by identifying the benefits and challenges of sharing threat-related information between local public safety agencies. As public safety organizations throughout the nation develop their ability to share threat-related information, they should review lessons learned from organizations examined in this study that have faced this important and complex undertaking. Horrific events such as the Boston marathon bombing (Hu et al, 2014), the Paris attacks ("BBC News," 2105) and the assault on the Las Vegas Harvest Music Festival (Bui et al., 2017) are a stark reminder that individuals with aspirations of violence can strike without warning. With targeted violent attacks on the rise globally, it is even more critical to effectively share threat-related information between public safety organizations.

Limitations of the Study

Several limitations were identified in the study. All of the participants worked in public safety organizations and routinely dealt with sensitive information in one form or the other. This may consist of law enforcement sensitive information pertaining to ongoing criminal cases. It could also include PII and/or PHI, such as health status, prescription medications, or other health-related data. Therefore, it was important that the participants ensured the information they shared during the interviews did not include any form of sensitive data related to an individual or an agency. Another limitation to the study was the lack of review of internal agency documentation. I had access to publicly available documents but was not allowed access to internal agency policy documents.

Delimitations of the Study

A delimitation for this study focused on the sample selection. SMEs from four public safety organizations located in Honolulu, Hawaii, were selected. Patton (2002) pointed out that qualitative research sample size "depends on what you want to know, the purpose of the inquiry, what's at stake, what will be useful, what will have credibility, and what can be done with available time and resources" (p.244). This study purposely did not collect information from across the entire nation, as the enormous dataset would be unmanageable.

The intent and design of this study was to capture the experiences of SMEs in public safety organizations within a particular region. Individuals who had at least 15 years of experience sharing threat-related information between public safety organizations in Honolulu were selected as participants. Some individuals that had

recently retired were included as long as they met the research study selection criteria. This research was an opportunity to capture extensive institutional knowledge from these retired public safety SMEs before the knowledge was lost forever. Further, research for this study was collected from a limited number of participants in Honolulu, Hawaii. Different perspectives and factors could have been received from the interview if additional participants were included from other regions of the country. Consequently, different experiences may have been disclosed.

Recommendations

This focus of this study was on public safety organizations in Honolulu, Hawaii. Honolulu is a mid-sized modern metropolitan city. It faces many of the same challenges as other cities in the continental U.S., including the need to share information across agencies to deal with emerging threat-related issues. However, Honolulu is unique because unlike other cities it is remotely isolated, being approximately 2,500 miles from the mainland. As a result, there is an increased need to ensure interagency communication is occurring to facilitate the regions ability to deal with a large-scale public safety event without immediate assistance from other states. Understanding how threat information is shared in Honolulu is critical because of its isolation. The findings of this study will help to fill a gap in literature by determining the benefits and challenges of sharing threat-related information between public safety organizations in Honolulu, Hawaii.

Currently, there is plenty of data in the literature about how threat-related information sharing at the federal level has improved since the terror attacks of 9/11

(Bharosa, Lee, & Janssen, 2010; Carter et al., 2017; Vacca, 2019). What is not clear are the challenges local public safety agencies face when sharing threat-related information between one another. This is problematic because local agencies hold the primary responsibility of responding to public safety threats. We do not fully understand the benefits and challenges of collaboration among these agencies due to "relatively minimal scholarly attention" to this issue (Carter et al., 2017, p. 1). This study helped to uncover the information sharing challenges public safety organizations face in Honolulu, Hawaii; however, there is much more work to be done throughout the rest of the nation.

It is recommended that other mid-size cities throughout the nation conduct similar research to uncover the benefits and challenges of sharing threat-related information between public safety organizations within their regions. Research at the local level is also needed to uncover the benefits and challenges of sharing information between public and private organizations within their regions. Once there is a significant data set available for comprehensive analysis, researchers could offer recommendations on how to improve threat-related information sharing at the local level nationwide.

Implications

Publishing the results of this study via Walden University and ProQuest, as well as sharing the research with Honolulu public safety organizations, may stimulate critical discussion of the necessity for optimal information sharing environments. Positive social change may occur through the identification of the benefits and challenges of sharing threat-related information between local public safety organizations. As public safety organizations throughout the nation develop their ability to share threat-related

information, they should review lessons learned from organizations examined in this study that have faced this important and complex undertaking.

Attacks such as the Boston marathon bombing (Hu et al, 2014), and the assault on the Las Vegas Harvest Music Festival (Bui et al., 2017) are a clear reminder that individuals with aspirations of violence can strike without warning. With targeted violent attacks on the rise globally (Hesterman, 2019) it is even more critical to effectively share threat-related information between public safety organizations. All public safety agencies must overcome the obstacles that keep them from sharing threat-related information effectively in order to better protect the public from attacks.

I found that Honolulu Public Safety agencies are currently communicating through information flow within and between organizations; however, this flow of information is intermittent. Several problems stem from information being shared only during urgent situations. Establishing an ongoing information sharing environment between organizations is necessary to ensure that information is effectively shared in all situations. Because public safety agencies have different skills and expertise, it is important that they actively collaborate on the analysis of threat-related information.

I also found that threat-related information often contains highly protected, or law enforcement sensitive information, and is difficult to share between agencies. It is important that agencies develop a policy-based process, through ongoing agency collaboration, to share this sensitive information. The implication is that ongoing agency participation with the state fusion center is vitally important to allow threat-related

information to be analyzed by multiple agencies with different skills and expertise, and then disseminated across all public safety agencies simultaneously.

The 9/11 Commission, shortly after the terrorist attacks of September 11th published recommendations to help protect the nation from another major terrorist attack. Many of these recommendations focused directly on information sharing between public safety agencies ("State & Major Urban," 2014). Since the 9/11 attacks, federal, state, and local governments have invested billions of dollars and countless work hours in an attempt to protect the public from violent attacks. Threat-related information sharing at the federal level has improved since the tragic events of 9/11; however, there is a lack of information on how local public safety agencies share this same type of information. Therefore, it is vitally important that more research is focused on this topic, because rather than violent attacks on the public decreasing from year to year throughout the nation, they are increasing at an alarming rate.

Conclusion

Horrendous attacks such as the Marjory Stoneman Douglas High School shooting (Chuck, Johnson, & Siemaszkoin, 2018) in Parkland, Florida, clearly demonstrate that individuals who strive to commit violence can strike anywhere without warning, whether they are recruited and trained by extremist organizations or self-motivated. Local public safety organizations must work together to adapt to this new asymmetrical threat environment. Local threat-related information gathering and sharing capabilities must be improved between the public safety organizations who are tasked with the responsibility of keeping the public safe.

The responsibility to keep the public free from violent attacks cannot be assigned solely to federal agencies or even to local law enforcement organizations. It must be a shared responsibility between multiple agencies. As one of the participants in this study so articulately pointed out, “It is going to take all of us to be responsive, not just one agency. Security is not one agency’s responsibility, it is all of our responsibility” (Participant 366, personal communication, January 11, 2019).

References

25 Deadliest mass shootings in U.S. history fast facts. (2015, May 9). Retrieved May 22, 2015, from http://www.cnn.com/2013/09/16/us/20-deadliest-mass-shootings-in-u-s-history-fast-facts

Abold, J. L., Guidetti, R., & Keyer, D. (2012). Strengthening the value of the national network of fusion centers by leveraging specialization: Defining "centers of analytical excellence." *Homeland Security Affairs*, *8*(1), 2–28. Retrieved from https://www.hsaj.org

Aftergood, S. (2014). Director of national intelligence open source center. Retrieved from http://fas.org/irp/dni/osc/

Allen, D. K., Karanasios, S., & Norman, A. (2014). Information sharing and interoperability: The case of major incident management. *European Journal of Information Systems, 23*(4), 418-432. doi:10.1057/ejis.2013.8

Bean, H. (2007). The DNI's Open Source Center: An organizational communication perspective. *International Journal of Intelligence and Counterintelligence*, *20*(2), 240–257. doi:10.1080/08850600600889100

Bean, H. (2013). The paradox of open source: An interview with Douglas J. Naquin. *International Journal of Intelligence and Counterintelligence*, *27*(1), 42–57. doi:10.1080/08850607.2014.842797

Better information sharing, or "share or be damned"? (2015). *The Journal of Adult Protection*, (5), 308. https://doi-org.ezp.waldenulibrary.org/10.1108/JAP-01-2015-0001

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers, 12*(1), 49–65. doi:10.1007/s10796-009-9174-z

Boczkowski, P. J. Matassi, M. & Mitchelstein. E. (2018). How young users deal with multiple platforms: The role of meaning-making in social media repertoires, *Journal of Computer-Mediated Communication,* Volume 23, Issue 5, September 2018, Pages 245–259, https://doi.org/10.1093/jcmc/zmy012

Bui, L., Zapotosky, M., Barrett, D., & Berman, M. (2017, October 02). At least 59 killed in Las Vegas shooting rampage, more than 500 others injured. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2017/10/02/police-shut-down-part-of-las-vegas-strip-due-to-shooting/?noredirect=on&utm_term=.73d565a17f83

Carter, J. G., Carter, D. L., Chermak, S., & Mcgarrell, E. (2017). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police and Criminal Psychology, 32*(1), 11-27. doi:http://dx.doi.org.ezp.waldenulibrary.org/10.1007/s11896-016-9199-4

Carter, J. G., & Rip, M. (2013). Homeland security and public health: A critical integration. *Criminal Justice Policy Review*, *24*(5), 573–600. https://doi-org.ezp.waldenulibrary.org/10.1177/0887403412452425

Chermak, S., Carter, J., Carter, D., McGarrell, E. F., & Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly*, *16*(2), 211–244. https://doi-org.ezp.waldenulibrary.org/10.1177/1098611113477645

Chuck, E., Johnson, A., & Siemaszko, C. (2018, February 15). 17 killed in mass shooting at high school in Parkland, Florida. Retrieved from https://www. nbcnews .com /news/us-news/police-respond-shooting-parkland-florida-high-school-n848101

Clandinin, D. J., & Connelly, F. M. (2000). *Narrative inquiry: Experience and story in qualitative research*. San Francisco: Jossy-Bass.

Cohn, A. (2013). A terrorist's tool for tactical coordination. *Journal of Counterterrorism & Homeland Security International*, *19*(2), 64. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=tsh&AN=87654991&site=eds-live&scope=site

Communication theories. (2019). Retrieved from https://www.utwente.nl/.uc/f32b97e4401021a2d8f00d5e2e5030c0add13d6eed6e400/Communication%20Theories%20University%20of%20Twente%20-%20UTwente%20-%20The%20Netherlands.pdf

Counterintelligence. (n.d.). Retrieved from http://www.merriam-webster.com/dictionary/counterintelligence

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2013). *Qualitative inquiry and research design: choosing among five approaches* (3rd ed.). Thousand Oaks, SAGE Publications.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed method approaches*. Thousand Oaks, CA: SAGE Publications.

Creswell, J.W. and Clark, V.L.P. (2017). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

David, P. A. (1985). Clio and the economics of QWERTY. *American Economic Review*, 332. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org /login.aspx?direct=true&db=edsgea&AN=edsgcl.3748036&site=eds-live&scope=site

Defense Intelligence Agency. (2012). *2012–2017 Defense Intelligence Agency strategy* Retrieved from http://www.dia.mil/Portals/27/Documents/About/2012-2017-DIA-Strategic-Plan.pdf

Developing a policy on the use of social media in intelligence and investigative activities: Guidance and recommendations. (2013). United States Department of Justice, Global Justice Information Sharing Initiative. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=732153

Desilver, D. (2014) Chart of the week: The ever-accelerating rate of technology adoption. Retrieved from https://www.pewresearch.org/fact-tank/2014/03/14/chart-of-the-week-the-ever-accelerating-rate-of-technology-adoption/

Ellis, R., & Botelho, G. (September 11, 2015). Man accused of bomb plot at 9/11 event, FBI says. Retrieved from http://www.cnn.com/2015/09/10/us/9-11-memorial-bomb-plot-kansas-city-missouri/

Fantz, A., Karimi, F., & McLaughlin, E. C. (2016, June 13). 49 killed in Florida nightclub terror attack. Retrieved from http://www.cnn.com/20185rlando12 /us/orlando-nightclub-shooting/index.html

Faulkner, S. L. and Trotter, S. P. (2017). *Data saturation.* In the International Encyclopedia of Communication Research Methods (eds J. Matthes, C. S. Davis and R. F. Potter). doi:10.1002/9781118901731.iecrm0060

FBI intelligence analyst careers. (2015). Retrieved from http://www.fbiagentedu.org /careers/intelligence/fbi-intelligence-analyst/

Federal Bureau of Investigations. (2015). Retrieved from https://www.fbi.gov/about-us/quick-facts

Federal Emergency Management Agency. (2015). About the agency. Retrieved from http://www.fema.gov/about-agency

Field testing, pilot studies, and IRB review timing. (2016). Retrieved ps://research. phoenix.edu/news/irb-corner-august-2015

Frankfort-Nachmias, C., & Nachmias, D. (2008). *Research methods in the social sciences*. New York, NY: Worth.

Fugard, A. J. B., & Potts, H. W. W. (2015). Supporting thinking on sample sizes for thematic analyses: A quantitative tool. *International Journal of Social Research Methodology, 18*(6), 669-684. doi:10.1080/13645579.2015.1005453

General systems theory. (2014). Retrieved August 28, from https://is.theorizeit .org/wiki/General_systems_theory

Gettleman, J., & Kulish, N. (2013, September 21). Gunmen kill dozens in terror attack at Kenyan mall. Retrieved from http://www.nytimes.com/2013186rland /186rlandofrica/nairobi-mall-shooting.html?pagewanted=all

Guest, G., MacQueen, K.M., & Namey, E.E. (2012). *Applied thematic analysis*. Sage Publications, Inc., Thousand Oaks.

Hammersley M., & Atkinson P. (2007). *Ethnography: Principles in practice*. London (UK): Taylor and Francis.

Hesterman, J. (2019). *Soft target hardening*. New York: Routledge, https://doi.org/10.4324/9780429422966

Homeland security. (2014, December 17). Retrieved from http://www.dhs.gov/state-and-major-urban-area-fusion-centers

Howard, P., Duffy, A., Freelon, D., Hussain, M., Mari, W., & Mazaid, M. (2011). Opening closed regimes what was the role of social media during the Arab spring? *Project on Information Technology and Political Islam,* (2011.1), 1-30. http://dx.doi.org/10.2139/ssrn.2595096

Hsiung, P. (2010). A process of reflection. Retrieved from http://www.utsc.utoronto.ca/~pchsiung/LAL/reflexivity

Hu, Q., Knox, C. C., & Kapucu, N. (2014). What have we learned since September 11, 2001? A network study of the Boston marathon bombings response. *Public*

Administration Review, *74*(6), 698-712. https://doi-org.ezp.waldenulibrary .org/10.1111/puar.12284

Huda, M., Maseleno, A., Atmotiyoso, P., Siregar, M., Ahmad, R., Jasmi, K. & Muhamad, N. (2018). Big data emerging technology: Insights into innovative environment for online learning resources. *International Journal of Emerging Technologies in Learning (IJET)*, (01), 23. https://doi-org.ezp.waldenulibrary.org/10.3991 /ijet.v13i01.6990

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence*, *15*(4), 565–579. doi:10.1080/08850600290101767

Husain, E. (2015). A global venture to counter violent extremism. Retrieved from http://www.cfr.org/radicalization-and-extremism/global-venture-counter-violent-extremism/p3049

Information sharing: DHS is assessing fusion center capabilities and results but needs to more accurately account for federal funding provided to centers. (2014, November 4). Retrieved from http://www.gao.gov/products/GAO-15-155

Inquvent. (2013, January 1). COE model. Retrieved from http://www.inquvent.com/coe-model.html

Intelligence cycle. (2010, May 21). Retrieved from https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Intelligence: Open source intelligence. (2013). Retrieved from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

Jackson, A. L., & Brown, M. (2007). Ensuring efficiency, interagency cooperation, and protection of civil liberties: Shifting from a traditional model of policing to an intelligence-led policing (ILP) paradigm. *Criminal Justice Studies: A Critical Journal of Crime, Law & Society*, *20*(2), 111–129. https://doi-org.ezp.waldenulibrary.org/10.1080/14786010701396855

Jones, S., & Chassany, A. (2015, November 15). Paris attacks: Security services struggle in terrorist battle. Retrieved from https://next.ft.com/content/1069e45c-8aec-11e5-a549-b89a1dfede9b

Kalu N. K. (2009). Strategic fusion: What lessons for international counterterrorism? *Defence Studies*, Vol. 9, Iss. 1. Retrieved from http://www.tandfonline .com/doi/abs/10.1080/1470 2430802673310?journalCode=fdef20

Kaste, M. (2014) As police monitor social media, legal lines become blurred. Retrieved from http://www.npr.org/sections/alltechconsidered/2014/ 02/28/284131881/as-police-monitor-social-media-legal-lines-become-blurred

Kozuch, B., & Sienkiewicz-Małyjurek, K. (2015). Information sharing in complex systems: A case study on public safety management. *Procedia - Social and Behavioral Sciences*, *213*, 722–727. https://doi-org.ezp.waldenulibrary .org/10.1016/j.sbspro.2015.11.493

Lenart, B., Albanese, J., Halstead, W., Schlegelmilch, J., & Paturas, J. (2012). Integrating public health and medical intelligence gathering into homeland security fusion centres. *Journal of Business Continuity & Emergency Planning*, *6*(2), 174–179. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=mnh&AN=23315252&site=eds-live&scope=site

Ludwig von Bertalanffy: General system theory - 1950. (2014). Retrieved from http://www.nwlink.com/~donclark/history_isd/bertalanffy.html

Mack, N., Woodsong, C., MacQueen, K. M., Guest, G., & Namey, E. (2005). *Qualitative research methods: A data collector's field guide.* (pp. 1-119). Retrieved from http://repo sitory.umpwr.ac.id:8080/bitstream/handle/123456789/3721/Qualitative%20Research%20Methods_Mack%20et%20al_05.pdf?sequence=1

Mah, R. (2014). Information sharing for counter terrorism in Canada after 9/11: Issues in the administrative coordination of multi-agency intelligence. Retrieved from ttps://dspace.library.uvic.ca:8443/bitstream/handle/1828/5862/Mah_Richard_MPA_2014.pdf?sequence=1&isAllowed=y

Marrin, S. (2004). Preventing intelligence failures by learning from the past. *International Journal of Intelligence and Counter Intelligence*, *17*(4), 655–672. doi:10.1080/08850600490496452

Maxwell, J. (2013). *Qualitative research design: An interactive approach* (3rd ed.). [Kindle DX version]. Thousand Oaks, CA: Sage Publications.

Miles, M., Huberman, A., & Saldana, J. (2014). *Qualitative data analysis: A methods sourcebook* (3nd ed.). [Kindle DX version]. Thousand Oaks, CA: Sage Publication.

Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage.

National commission on terrorist attacks upon the United States, Kean, T. H., & Hamilton, L. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. Washington, D.C.: U.S. Government Printing Office publication.

National strategy for information sharing and safeguarding. (2012). Retrieved from https://nsi.ncirc.gov/documents/NSISS_2012_White_House.pdf

New information and intelligence needs in the 21st century threat environment. (2008). Stimson (Report Number 70), 1-53. Retrieved from https://www.stimson .org/sites/default/files/file-attachments/SEMA-DHS_FINAL_1.pdf

Office of the director of national intelligence (ODNI). (2004). Retrieved from https: //www.dni.gov/

Orlando terror attack reminds us to be vigilant. (2015, November). Retrieved from https://publicsafety.utah.gov/2016/06/13/orlando-terror-attack-reminds-us-to-be-vigilant/

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and*

Mental Health Services Research, 42(5), 533-544. doi:http://dx.doi.org.ezp.waldenulibrary.org/10.1007/s10488-013-0528-y

Pasha Hawaii. (2019). Retrieved from https://www.pashahawaii.com/schedules/estimated-pasha-hawaii-vehicle-transit-days

Patton, M. (2002). *Qualitative research and evaluation methods (3rd ed.).* Thousand Oaks, Calif.: Sage Publications.

Perrow, C. (April 2006). The disaster after 9/11: The department of homeland security and the intelligence reorganization. *Homeland Security Affairs 2*, Article 3 https://www.hsaj.org/articles/174

Plano-Clark, V. L., & Creswell, J. W. (2010). *Understanding research: A consumer's guide*. Upper Saddle River, New Jersey: Pearson Education.

Public safety. (2016). Retrieved from https://definitions.uslegal.com/p/public-safety/

Public safety: A public safety a guidebook for government (pp. 1-28). (2011). Government Technology. Retrieved from http://media.govtech.net/govtech_website/resources/case_studies/Public_Safety_Guidebook.pdf

Public safety law and legal definition. (2019). Retrieved from https://definitions.uslegal.com/p/public-safety/

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. Media and Communication, *3*(2). https://ssrn.com/abstract=2645973

Rosenbach, E., & Peritz, A. J. (2009). Domestic intelligence: Belfer center for science and international affairs. Retrieved from http://www.belfercenter.org/publication/domestic-intelligence

Sandelowski, M. (1995). Sample size in qualitative research. Research in Nursing & Health, 18, 179–183. https://doi.org/10.1002/nur.4770180211

Schmidt, M. S., & Masood, S. (2015). San Bernardino couple spoke of attacks in 2013, F.B.I. Says. Retrieved from http://www.nytimes.com/2015/12/ 10/us/san-bernardino-massacre-fbi.html

Shepherd, D. (2011). The role of the private sector in fusion centers. *Security: Solutions for Enterprise Security Leaders*, *48*(1), 36–39. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=tsh&AN=57669547&site=eds-live&scope=site

Silverman, D. (2014) *Interpreting qualitative data*. Thousand Oaks, CA: Sage Publications.

Simon T, Goldberg A, Aharonson-Daniel L, Leykin D, Adini B (2014) Twitter in the cross fire—the use of social media in the Westgate mall terror attack in Kenya. PLoS ONE 9(8): e104136. doi:10.1371/journal.pone.0104136

State and major urban area fusion centers. (2014). Retrieved from http://www.dhs.gov/state-and-major-urban-area-fusion-centers

Steele, R. D. (2008). The open source program: Missing in action. *International Journal of Intelligence and CounterIntelligence*, *21*(3), 609–619. doi:10.1080/08850600802050279

Stone, A. (2015). Fusion centers 2.0. Retrieved from emergencymgmt.com

Strauss, A. (1987) *Qualitative analysis for social scientists.* Cambridge, England: Cambridge University Press.

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian journal of hospital pharmacy*, *68*(3), 226–231. doi:10.4212/cjhp.v68i3.1456

Taylor, R. W., & Russell, A. L. (2011). The failure of police "fusion" centers and the concept of a national intelligence sharing plan. *Police Practice and Research*, *13*(2), 184–200. doi:10.1080/15614263.2011.581448

The role of fusion centers in countering violent extremism. (2012). Retrieved from https://it.ojp.gov/documents/roleoffusioncentersincounteringviolentextremism_compliant.pdf

Threat, definition and meaning. (2017). Retrieved from http://www.businessdictionary.com/definition/threat.html

Tierney, J. (1972). The use of systems theories in international political analysis. *World Affairs*, *134*(4), 306-324. Retrieved from http://www.jstor.org/stable/20671334

United States Coast Guard. (1998). Situational awareness. Retrieved from https://www.scribd.com/document/132226965/United-States-Coast-Guard-Situational-Awareness-Exercise

United States Department of Homeland Security: About fusion centers. (2018, December 17). Retrieved from https://www.dhs.gov/state-and-major-urban-area-fusion-centers

United States Intelligence Community. (2015). Retrieved April 8, 2015, from http://www.finedictionary.com/United States Intelligence Community.html

Vacca, J. R. (2019). *Online terrorist propaganda, recruitment, and radicalization.* Boca Raton, FL: CRC Press

Von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. New York: George Braziller.

Waterman, K., & Wang, S. (2010, November 8). Prototyping fusion center information sharing: Implementing policy reasoning over cross-jurisdictional data transactions occurring in a decentralized environment. Retrieved June 27, 2015, from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5655091

William M., T., Derek A., C., Bobby, M., Richard S., G., & Scott J., L. (2006). Practical challenges of systems thinking and modeling in public health. *American Journal of Public Health*, (3), 538. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edsovi&AN=edsovi.00000469.200603000.00028&site=eds-live&scope=site

Witte, G., & Morris, L. (2015, November 28). Failure to stop Paris attacks reveals fatal flaws at heart of European security. Retrieved from https://www.washingtonpost.com/world/europe/paris-attacks-reveal-fatal-flaws-at-the-heart-of-european-security/2015/11/28/48b181da-9393-11e5-befa-99ceebcbb272_story.html

Worst mass shootings in the U.S. as of February 2019. (2019, April). Retrieved from https://www.statista.com/statistics/476101/worst-mass-shootings-in-the-us/

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International Journal of Information Management,* (31), 6-13. doi:10.1016

Appendix A: Invitation to Participate

Date: _____
Dear: _____

Thank you for your interest in my dissertation research, to identify and explore the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii. The purpose of this letter is to go over some important issues and to obtain your signature on the attached Informed Consent form.

I will be utilizing an exploratory qualitative process that will allow me to capture a comprehensive description of your experience. I hope to answer the following:

> RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?
>
> RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?
>
> RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

Specifically, I am looking for your thoughts and feelings about the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu and what can be done to improve information exchange between these agencies.

All of the information you share with me will be stored in a secure manner. Any demographic information that may connect you to the information will be removed. A copy of your transcript will be e-mailed to you for review and you can make any revisions you feel are necessary, prior to it being entered into the study.

I value your participation and contribution to my study and thank you for your commitment of personal time. If you have any further questions or concerns feel free to contact me at [telephone number redacted], or [e-mail address redacted].

Sincerely,
Cort M. Chambers

Appendix B: Interview Protocol

Part I: Overview

Overview

1. Interviews recorded (with permission)
2. Interview conducted in a neutral setting
3. Interview time period 60 to 90 minutes

Interview Methodology

The methodology involved in this research study will include conversational style in-depth interviews. Follow-up questions used to stimulate conversation, if needed. A semi structured question design will be utilized. Interviews will include:

1. 10 predetermined questions
2. Identical questions for all participants

Location of Interview: To be determined
Date: To be determined
Start Time: Prearranged time
Finish Time: 60 to 90 minutes

Part II: Interview Components

1. Interview Components

a. Introduction
b. Consent and confidentiality agreement review
c. Interview

2. Purpose of the interview

The purpose of the research was to explore the benefits and challenges of sharing threat-related information between public safety agencies (law enforcement, fire services, EMS, and public health) in Honolulu, Hawaii

3. Permission to record interview

I would like to tape-record our discussion, with your permission. Only I will have access to the recording. No responses will be ascribed to you by name. The research results will describe in summary what is said during the conversation. The recording will be erased after the dissertation is completed.

The interview will consist of open-ended questions intended to obtain your personal experience and perceptions. The interview is scheduled to last 60 to 90 minutes. If you agree to participate in this research process, please sign the informed consent agreement.

Part III: Interview Questions

1. What are the benefits of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

2. How does sharing threat-related information between public safety organizations help identify and prevent threats to the public?

3. How does communication software play a role in the sharing of threat-related information?

4. What are the challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

5. Please describe the top three barriers, at your organization, to sharing threat-related information between public safety organizations.

6. How does politics play a role in the sharing of threat-related information between public safety organizations?

7. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

8. What role could agency policies, within your organization, play in improving the sharing of threat-related information?

9. Please describe any past lessons learned at your organization that could improve the exchange of threat-related information between public safety organizations.

10. What is your perception of the current state of threat-related information exchange between public safety agencies in Honolulu, Hawaii?

Appendix C: Chart Linking Research Questions to Interview Questions

Interview questions	RQ1	RQ2	RQ3
1. What are the benefits of sharing threat-related information between public safety agencies in Honolulu, Hawaii?	RQ1		
2. How does sharing threat-related information between public safety organizations help identify and prevent threats to the public?	RQ1(a)		
3. How does communication software play a role in the sharing of threat-related information?	RQ1(b)		
4. What are the challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?		RQ2	
5. Please describe the top three barriers, at your organization, to sharing threat-related information between public safety organizations.		RQ2(a)	
6. How does politics play a role in the sharing of threat-related information between public safety organizations?		RQ2(b)	
7. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?			RQ3
8. What role could agency policies, within your organization, play in improving the sharing of threat-related information?			RQ3(a)
9. Please describe any past lessons learned at your organization that could improve the exchange of threat-related information between public safety organizations.			RQ3(b)
10. What is your perception of the current state of threat-related information exchange between public safety agencies in Honolulu, Hawaii?			RQ3(c)

Appendix D: Coding Protocol

A process of coding will be utilized to assist with the process of analyzing the data. The key to coding is to allow themes to emerge from the data that makes sense to the researcher. Creswell (2013) stated that researchers should develop a codebook for each research study. To ensure that I have captured the essence of the of the interviews I will use a coding strategy that consists of first reading through all of the transcripts to get a deep understanding of what took place in the interviews. I will also thoroughly review my written notes, making memos of important facts and details.

The next step will include classifying the data. Creswell (2013) pointed out "coding involves aggregating text into small categories of information" and then assigning an appropriate label (p. 184). I will then develop a short list of codes, or a codebook, which will be expanded upon as I continue processing the data (Creswell, 2013). Lastly, I will separate all the codes into four or five overarching themes that will assist me while writing my discussion and narrative of the data. I will utilize NVivo computer software throughout the coding process.

Reference

Creswell, J. W. (2013) *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Appendix E: Code Book

Code name	Description	Sources	References
Information flow	The consistent and effective exchange of information	13	97
Between state and county	Information sharing between state and county organizations	4	8
Co-locate dispatch	Locating the 911 dispatch centers for all public safety organizations in the same location	1	2
Communication	Effective communication between organizations	4	7
Include decision makers	Include decision makers in the decision-making process	2	9
Information sharing in real time	Information sharing in real-time	7	13
Less information than before	Agencies are sharing less information	4	6
Right information to right people	Ensuring the right information gets to the right people within a public safety organization	8	19
Sharing information internally	Sharing information internally within a public safety organization	6	13
Withholding information	Threat-related information is withheld/not shared for some reason	6	14
Threat information not acted upon	Threat related information is not acted upon by a public safety organization	6	10
Collaboration	Working with another organization cooperatively to achieve a goal	13	70
After action report	Agencies complete after action reports	1	1
Agencies are equally invested	Agencies are equally invested	5	6
Coordinated response	Agencies coordinate response to incidents	6	9
Coordination of resources	Agencies coordinate their resources during a response	4	7
Engagement with the visitor industry	Agencies engage with the Hawaii visitor industry	1	1
Everyone on the same page	All agencies on the same page (coordinated) during an incident	11	30

(*table continues*)

Code name	Description	Sources	References
Common operating picture	Common operating picture, all agencies have the same operating information in real-time during an incident	3	6
Interoperability	Agencies work together as one	8	12
Obligated to share	Agencies are obligated to share threat related information	1	1
Fusion center	State agency - primary purpose is analysis and sharing of threat-related information	11	56
Identifying gaps	Identifying gaps related to threat-related information sharing	1	1
TTO	Threat Team Oahu	1	1
Validating threats	Determining if a potential threat is valid	3	5
Confidential information	Information that is sensitive or protected	12	48
Clearances	Agencies have personnel that have the proper national security clearances to view classified information	2	3
Goes to the wrong people	Confidential information leaks to people outside public safety	7	15
Gets out to the news media	Confidential information leaks to the news media	4	9
Law enforcement confidential informants	Law enforcement confidential informants	1	2
Need to know	Individuals within public safety organizations that have a need to know sensitive/confidential information	3	8
People must be vetted	Individuals within public safety organizations should be properly vetted to handle sensitive/confidential information	5	5
Understand when to share confidential information	Individuals within public safety organizations know when to share confidential information	3	5

(*table continues*)

Code name	Description	Sources	References
Agency culture	The culture within the organization	11	45
Allocation of funding	Allocation of funding	1	1
Buy in	Agency willingness to actively participate	7	17
Control over information	Attempting to control information	7	12
Wants the credit	Agency seeks credit for accomplishments	5	8
Different abilities	Public safety agencies have different skillsets and unique areas of expertise	11	38
Different jargon	Public safety agencies use different and unique jargon within their organizations	1	2
Different knowledge base	Public Safety agencies hold different and unique knowledge base within their organizations	5	8
Different perspectives	Public Safety agencies have different perspectives depending on their field of public safety	5	10
Medical perspective	Individuals with medical training can view situations with a health/medical perspective	7	17
Policy	Policy issues within a public safety organization	11	29
Accountability	Public safety organizations are accountable for their actions	2	2
Discipline for not following policy	Public safety organizations personnel are disciplined for not following policy	1	1
FIRPA	Family Educational Rights and Privacy Act (FERPA), Federal law that protects the privacy of student education records	1	1
Not enforcing policy	Public safety organizations that do not enforce their personnel to follow the organizations policy	2	3

(*table continues*)

Code name	Description	Sources	References
Responder safety	The safety of a public safety organizations responders	10	28
Police	Police officer safety	5	11
Fire	Fire fighter safety	4	7
EMS	Paramedic safety	4	13
Secure websites	Websites that have enhanced security features to ensure only vetted individuals can access	10	24
HSIN	Homeland security information network	3	3
LEEP	Law enforcement enterprise portal	1	1
Politics	Activities associated with local governance	9	21
Political will to share information	An organization's political will to share information	3	3
Unions	A labor union or trade union	3	5
Training	Information sharing training	5	20
Cross training of personnel	Training personnel across agencies to perform duties	1	2
Lack of training	A lack of training pertaining to information sharing	3	6
Training together	Agencies training together	1	1
Electronic communication	Communication using electronic devices	8	18
Email	Information sharing through email	1	2
Push notifications to the public	Information is shared to a wide audience via text messages to the public	3	4
Virtual communication	Webcasts/virtual meetings	2	2
Safety of the public	The safety of the public	7	15
HIDTA	High intensity drug trafficking area – A federal law enforcement program	3	12
WSIN	Western states information network - A federal law enforcement program	2	6
Personnel shortage	Lack of personnel	8	11
Lack of finances	Lack of budget	8	11

(*table continues*)

Code name	Description	Sources	References
Deconfliction	The attempt to reduce the possibility of undercover law enforcement personnel accidently encountering each other by sharing information on their operational movements	3	10
Software	Digital programs used by a computer	5	9
Cyber attack	Digital software attack	2	2
Hacking	gaining of unauthorized access to a computer	1	1
eGuardian	Federal law enforcement web portal	1	1
Misallocation of resources	Resources are not put to the best use	5	9
Misallocation of human capital	Human capital is not put to its best use	3	5
Homeless	Individuals who have no permanent residence	2	7
Meetings	Formal meetings between public safety agencies	2	6
Discussions	Informal discussions among agency representatives	2	3
Social media	Websites that allow users to participate in sharing social information	3	5
Misinformation	Inaccurate information	2	2
APEC	Asian pacific economic cooperation a regional economic meeting involving world leaders	3	5
Single point of failure	An individual, or part of a system, which if fails may cause the entire system to fail	2	4
Education	Training in information sharing	2	3
View threat info as LE	An individual or organization that views threat information as a law enforcement responsibility	3	3
See something say something	National see something say something campaign	3	3

(*table continues*)

Code name	Description	Sources	References
Non-law enforcement left out	Agencies that are not responsible for law enforcement responsibilities are not given threat-related information	1	2
SLEC	Hawaii state law enforcement coalition	1	2
Lack of time	Not enough time to complete operational tasks	1	1
JTTF	Joint terrorism task force - A federal law enforcement program	1	1

Appendix F: Field Test

Dear_____

I would first like to sincerely thank you for participating in this doctoral field test.

I am currently in the process of completing dissertation research on the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii.

The general overarching problem addressed in this study is the importance of communication between public safety agencies as they deal with serious emerging threat-related issues such as terrorism. It is unknown whether there are challenges or benefits to sharing threat-related information between local public safety agencies in the United States. The findings of this study will help to fill this gap in the literature by determining the perceived benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii.

Multiple factors affect the sharing of information between public safety organizations including technical and political issues, as well as the lack of communication and coordination between agencies. These problems will be addressed in this research by examining how public safety agencies share threat-related information between one another. The intention is to explore any possible issues that might reduce their ability to prevent terror attacks.

The theoretical framework that I am using for this study is General Systems Theory.

For this research I hope to answer the following Research Questions:

> RQ1. How are public safety agencies communicating threat-related information between one another in Honolulu, Hawaii?
>
> RQ2. What are the benefits and challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?
>
> RQ3. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

I plan to ask the following Interview Questions to the participants:

1. What are the benefits of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

2. How does sharing threat-related information between public safety organizations help identify and prevent threats to the public?

3. How does communication software play a role in the sharing of threat-related information?

4. What are the challenges of sharing threat-related information between public safety agencies in Honolulu, Hawaii?

5. Please describe the top three barriers, at your organization, to sharing threat-related information between public safety organizations.

6. How does politics play a role in the sharing of threat-related information between public safety organizations?

7. What can be done to improve the sharing of threat-related information between public safety agencies in Honolulu, Hawaii?

8. What role could agency policies, within your organization, play in improving the sharing of threat-related information?

9. Please describe any past lessons learned at your organization that could improve the exchange of threat-related information between public safety organizations.

10. What is your perception of the current state of threat-related information exchange between public safety agencies in Honolulu, Hawaii?

By conducting this research, I hope to explore the benefits and challenges that exist in sharing threat-related information between public safety organizations. Experienced public safety officials will be interviewed utilizing open-ended questions.

Please record below any suggestions that you have regarding the purpose of this study, the proposed research questions, proposed interview questions, or the process for capturing data. Please add additional pages if needed.

_____

_____

_____

_____

_____

Please return the form with your feedback in the enclosed postage paid envelope. If you have any questions, please contact me at [telephone number redacted]. Your time and input for this doctoral study are greatly appreciated!

Sincerely,
Cort M. Chambers