

A Quantitative Analysis of the Capacity of Campus Police to Investigate Cybercrime

BY

HENRY A. DIXON

Dissertation Committee

Brandi Stocker, Ed.D., Mentor

Daniel Wisneski, Ph.D.

Rev. Allen Potts, D.Min.

Submitted in Partial Fulfillment of the
Requirements for the Ed.D. Degree

Saint Peter's University

2022

SAINT PETER'S UNIVERSITY
OFFICE OF ED.D. PROGRAMS

APPROVAL OF SUCCESSFUL DEFENSE

Doctoral Candidate, Henry Dixon, has successfully defended and made the required modifications to the text of the doctoral dissertation for the Caulfield School of Education Ed.D. Program in Educational Leadership Higher Education during the Spring semester 2022.

DISSERTATION COMMITTEE
(Please sign and date beside your name)

Mentor:
Dr. Brandi Stocker Brandi Stocker Date: 4-18-2022

Committee Member:
Dr. Daniel Wisneski DW Date: 4/21/22

Committee Member:
Rev. Dr. Allen Potts Allen Potts Date: 4-21-2022

The mentor and any other committee members, who wish a review to recommend revision, will sign and date this document only when revisions have been completed. Please return this form to the Caulfield School of Education/Ed.D. Program Office.

© 2002

Henry A. Dixon

All Rights Reserved

ABSTRACT

Through quantitative research, this study seeks to identify the specific method campus police employ to investigate cybercrime, then identify demographic characteristics (variables) of the agencies that permit or limit the agency's method of response. The correlation between demographic characteristics and the resulting response method represents the agency's capacity to investigate cybercrime. The tool utilized to capture data for this study is the “Survey of Campus Law Enforcement Agencies” designed by the U.S. Department of Justice (USDOJ), Bureau of Justice Statistics (BJS).

Almost 94% of institutions did not have a dedicated cybercrime unit. Only 6% of institutions did have a dedicated cybercrime unit, which suggests that campus police agencies may not have the resources to dedicate a full-time cybercrime unit or that management determined that the existing campus police officers were enough for the institutions' cybersecurity needs. Approximately 55% of institutions stated that police personnel was designated to investigate cybercrimes as necessary, and another 15% of institutions had no policies addressing cybercrime.

The literature review suggested that these conditions may result in educational institutions being unsuccessful in investigating cybercrimes and unprepared to deal with cybercrimes generally. If the campus police agencies considered in this study successfully investigated cybercrimes, then the disconnection between literature and the study results would suggest a need to reconsider academic understanding of cybercrime investigation. However, if the campus police were largely unprepared and unsuccessful in their investigations, the expectations of literature would largely be confirmed.

ACKNOWLEDGEMENTS

I would like to thank my big brother, Dr. Gerald E. Glisson, and Ms. Cheryl Coy for always providing me with professional growth and development opportunities. Thank you for the friendship and mentorship.

I would like to thank Dr. Larita Alford and Rev. Dr. Allen Potts for guiding me through the many phases of the dissertation process.

Finally, I would like to thank the Dissertation Committee and Dr. Anna Cicirelli, Dean & Director of Ed.D. Higher Education Program.

DEDICATION

May this work serve as a celebration of the pioneering work by Trenton Police Detective Vincent A. Dixon (Ret.) to advance Computing in Policing. Det. Dixon, my dad, built and introduced into service the first computer system utilized by the Trenton Police Department in Trenton, New Jersey. He led the departments' expansion and evolution of computers and networked devices from the early 1980s to his retirement in the early 2000s. Det. Dixon's legacy will live on in the next generation of men and women now facing the new threat of cybercrime.

I want to thank my mother, Lucinda E. Dixon, for her unwavering support, from my adolescent years when I needed motivation to my adult years when my motivation seemed to escape immediate reality. You never gave up on me.

TABLE OF CONTENTS

ABSTRACT	iii
ACKNOWLEDGEMENTS	iv
DEDICATION.....	v
LIST OF TABLES.....	viii
LIST OF FIGURES	ix
CHAPTER 1: THE PROBLEM AND PROCEDURES.....	1
Introduction.....	1
Statement of the Problem	4
Purpose of the Study	5
Theoretical Perspective	6
Research Questions	7
Significance of the Study	8
Limitation and Delimitation	9
Definition of Key Terms	9
Summary	10
CHAPTER 2: REVIEW OF LITERATURE	12
Theoretical Framework	13
Evolution of Campus Police.....	13
From Campus Security to Full Service Police.....	13
Cybercrime and How it Impacts the Campus Community	20
Cybercrime Defined	20
Cybercrime on Campus	21
Current Strategies: Cybercrime Prevent and Investigate	22
Capacity to Investigate Cybercrime	22
External Partnerships.....	24
Summary	26
CHAPTER 3: METHODOLOGY	27
Research Questions	27

Participants.....	29
The Researcher.....	29
Data Collection	30
Data Source(s).....	30
Data Analysis	30
Research Questions	32
Ethical Considerations.....	33
Summary	33
CHAPTER IV: ANALYSIS OF THE DATA.....	35
Research Design.....	35
Characteristics of the Sample	35
Assumptions Testing Results	37
Hypothesis Testing Results	44
Research Question One	44
Research Question Two.....	48
Summary	51
CHAPTER 5: SUMMARY AND CONCLUSIONS.....	52
Introduction.....	52
Summary of Findings	53
Demographic Information	53
Research Question One	55
Research Question Two.....	57
Recommendations	59
Conclusion	62
REFERENCES	65

LIST OF TABLES

Table 1	36
<i>Descriptive Statistics</i>	36
Table 2	36
<i>Frequencies</i>	36
Table 3	37
<i>The Variance Inflation Factors for Independent Variables</i>	37
Table 4	43
<i>Tests of Normality</i>	43
Table 5	43
<i>Durbin-Watson Test for Independence of Residuals</i>	43
Table 6	46
<i>Nonparametric Correlations for Cybercrime Unit and Percentage of Higher Education</i>	46
Table 7	48
<i>Nonparametric Correlations for Required Education Level and Cybercrime Investigation Method</i>	48
Table 8	49
<i>Nonparametric Correlations for Required Training Hours and Cybercrime Investigation Method</i>	49
Table 9	50
<i>Nonparametric Correlations for Budget and Cybercrime Investigation Method</i>	50
Table 10	51
<i>Nonparametric Correlations for Required Training Hours and Budget</i>	51

LIST OF FIGURES

Figure 1 38
Scatterplot for Required Training Hours..... 38
Figure 2 38
Scatterplot for Cybercrime Investigation Method 38
Figure 3 39
Scatterplot for Cybercrime Unit 39
Figure 4 40
Normal Q-Q Plot for Cybercrime Investigation Method..... 40
Figure 5 40
Normal Q-Q Plot for Cybercrime Unit..... 40
Figure 6 41
Normal Q-Q Plot for Budget..... 41
Figure 7 41
Normal Q-Q Plot for Required Education Level 41
Figure 8 42
Normal Q-Q Plot for Required Training Hours 42
Figure 9 42
Normal Q-Q Plot for Percentage of Higher Education..... 42

CHAPTER 1: THE PROBLEM AND PROCEDURES

Introduction

In the late 1800s, Yale University employed two police officers to protect and maintain order on campus (Wada, 2010). This inaugural event established law enforcement's first presence on a college or university campus and has steadily evolved over the last century. Although crime on a college campus is far less prevalent than in the outside community, it does occur (Wada, 2010). Wood describes the act of policing as an activity to provide a safe and secure environment in which people can live and work (Wood, 1998). Higher education institutions are sanctuary-like campuses where students of all backgrounds live and pursue academic scholarships in various fields of study.

For the first half of the 20th century, institutions employed "watchmen," commonly recognized today as security officers (Bromley, 1998, 2003). These individuals worked to secure the campus and maintain order among students under the *doctrine of loco parentis* (Bromley, 1998), which refers to school officials' legal responsibility to assume parent-like authority over students under their care. In 1960, Alabama State University expelled St. John Dixon and eight other students for disrupting the campus learning environment with repeated campus protests and a reported courthouse sit-in. Dixon and fellow students' repeated protests were motivated by a previous event where they were forcibly removed from a public whites-only cafeteria. The students appealed their expulsion through the Alabama court system up to the "Fifth Circuit Court in New Orleans with the aid of Thurgood Marshall, who became the first [black] Supreme Court Judge" (Charles, 2020). In *Dixon vs. Alabama Board of Education* (1961), the court held that the Alabama Board of Education could not use *loco parentis* at the college level as the basis

for expelling students without due process. This court decision marked the end of the *doctrine of loco parentis* as a tool to maintain order among college students.

With the *Dixon* (1961) decision and the threat of the civil unrest of the 1960s and 70s, security officers alone could no longer maintain the sanctuary for learning. Emergency calls for assistance from outside police agencies often worsened situations, as state and municipal police officers were not trained to balance law enforcement with each campus culture's unique needs. Through legislation across the country, state colleges and universities and some private institutions were permitted to establish campus police agencies complete with full powers of arrest and use of firearms. With no template to follow, institutions hired retired local and federal police officials to serve as chiefs and modeled department structure after municipal agencies.

Many institutions established police departments with various levels of authority. Some institutions, guided by optics rather than institutional need, opted not to let their officers carry firearms; this and other limitations ascribed to campus police led to the perception that campus police are not real police (Wada, 2010; Wilson, 2015). Campus police are unique as they take direction from a chief law enforcement officer and institutional leadership. The evolution of campus police is directly related to the expansion of serious crime and the possibility of terrorist activities on campuses across America.

On September 11, 2001 (9/11), four commercial airlines were hijacked by teams of college-aged men and utilized as weapons to attack four American targets. Successful in hitting three of their targets, this attack remains the deadliest on American soil since Pearl Harbor's invasion in 1941. The subsequent investigation into the events on September 11, 2001, shined a spotlight on higher education institutions' vulnerability to infiltration and future terrorist attacks. The September 11th attack, coupled with the Virginia Tech mass shooting in 2007, led to a

heightened security posture in the two decades post 9/11. As a result of these events, campus police adopted their municipal counterparts' recruiting, tools, tactics, and training. They also regularly conducted active shooter and emergency response drills with other local agencies. This synergy has led to the further professionalization of campus police into full-service police agencies. Some exemplary campus police agencies have earned the nationally recognized Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA) certification is awarded to agencies who demonstrate proficiency in many of the 459 CALEA Standards for Law Enforcement Agencies (CALEA, 2021). The standards include the following:

1. Law Enforcement Role and Authority
2. Agency Jurisdiction and Mutual Aid
3. Contractual Agreements for Law Enforcement Services
4. Use of Force
5. Weapons and Training
6. Organization and Administration
7. Planning and Research, Goals and Objectives, and Crime Analysis
8. Classification and Delineation of Duties and Responsibilities
9. Recruitment and Selection
10. Training and Career Development
11. Criminal Investigation
12. Critical Incidents, Special Operations, and Homeland Security

The U.S. Department of Justice's Bureau of Justice Statistics reports that there are "more than 905 U.S. 4-year colleges and universities with 2,500 or more students [who utilize] sworn police officers to provide law enforcement services" (Reaves, 2015, p. 1). Only 20 college and university

campus police agencies in the United States hold CALEA accreditation (CALEA, 2020). It is outstanding to note Montclair State University Police Department is the only institution in the State of New Jersey to have achieved CALEA accreditation (CALEA, 2020).

Statement of the Problem

Institutions of higher education maintain campuses that can sometimes mirror small cities in scope and size with 50,000 or more students. Many state colleges and universities operate open campuses with a mix of staff, students, and visitors. The institution's size does not raise or lessen the institution's duty to warn or investigate once a crime has been committed (Schuh, 1999). "Institutions have a duty to exercise care in operating their facilities, or they may have legal consequences if a person is injured" (Schuh, 1999, p. 197). The legal definition of an injury is defined as "any harm done to a person by the acts or omissions of another. Injury may include physical hurt, as well as damage to reputation or dignity, loss of a legal right, or breach of contract" (Law.com, 2020). For over 100 years, police have investigated crimes where the physical or perceived injury originated in the physical world. With the advancement of information technology, online communication, and mobile devices, the opportunity for injuries to originate in the cyber realm abound.

Injuries as a result of cybercrime are a relatively new concept in the long history of policing. International police agencies have struggled to cobble together investigative practices, jurisdictional agreements, and laws to fight the growing threat in the last two decades. In America, federal and state agencies have created specialized units to investigate cybercrime. The need for specialized investigators has trickled down to local police departments with varying available resources to explore. The capacity of municipal police to investigate cybercrime is unknown and may be a topic for future research. On the other hand, higher education institutions

need cyber investigators as students worldwide turn to cell phones, watches, tablets, laptops, desktops, and multiple other connected devices for social, business, and scholarly communication. The opportunity for cybercrime increases by the hour as computer intrusions, theft, fraud, unauthorized disclosures, harassment, and intimidation occur. When presented with calls for assistance, police agencies must provide an appropriate response (Schuh, 1999). To effectively solve cybercrimes, campus police must have the skill set to follow and collect digital forensic evidence, which ultimately leads to a physical person, not a random person, but the person who committed the crime. Cybercriminals' ability to remain anonymous through various technical means makes this task more difficult. Investigating cybercrimes that span multiple devices, networks, state, and international jurisdictions is far from traditional police work. The skillset required is specialized and not easily attained. With a duty to warn and protect (Schuh, 1999), campus police agencies must respond to all calls for assistance. Considering the highly specialized nature of cybercrime investigation, campus police's capacity to do this work is in question.

Purpose of the Study

Through quantitative research, this study seeks to identify the specific method campus police employ to investigate cybercrime, then identify demographic characteristics (variables) of the agencies that permit or limit the agency's method of response. The correlation between demographic characteristics and the resulting response method represents the agency's capacity to investigate cybercrime. Uncovering the specific structures that enhance campus police's ability to investigate cybercrimes will aid campus police administrators in decision-making and the deployment of resources. This research will provide vital information as the current pandemic has prompted higher education institutions across America to transition to remote

work and instruction. Changes in routine activity (online) put staff and students at increased risk of cybercrime (Hawdon, 2020).

Theoretical Perspective

Routine activity theory (Cohen & Felson, 1979), which is the most influential theory of victimization (Miró, 2014), argues that for crime to occur, three necessary conditions must spatio-temporarily converge: (1) the presence of motivated offenders, (2) the presence of a suitable target, and (3) the absence of a capable guardian. Routine activity theory proposes that victimization stems from the “recurrent and prevalent activities” that individuals are involved in, which in turn influence the likelihood that the three necessary factors are present (Cohen & Felson, 1979). Therefore, routines influence an individual’s risk of being victimized. (Hawdon, 2020, P.547-548)

Routine activity theory provides a framework for the significance of this research.

Currently, American higher education institutions are experiencing a perfect storm of elements that make the increased occurrence of cybercrimes inevitable. Routine activity theory calls for three elements: a target, a motivated offender, and “the absence of a capable guardian” (Hawdon, 2020, pp. 547-548). Thousands of institutions have transitioned to 100% remote work, prompting changes in routine activities that would have otherwise occurred in person. The urgency of the public health crisis has made policy and procedures fluid. As a result, possible loopholes and gaps in cybersecurity provide “motivated” criminals the opportunity to take advantage. If campus police agencies cannot investigate cybercrime, they are ineffective as guardians. Routine activity theory is used in police science to explain variables that increase individuals’ risk of victimization (Hawdon, 2020). While the research shows the internet has been mostly deregulated, with limited monitoring, Hawdon notes the lack of effective guardianship before the pandemic remains unchanged during the pandemic; in effect, the guardianship question is unchanged by the pandemic. Therefore, the focus is on the impact that campus police’s capacity to investigate cybercrime has on the offenders’ motivation. Police wear a uniform, a badge, and a

gun to project a command presence. Command presence is the police officer's ability to project him or herself as one who demands respect and, in some instances, feared. If potential offenders recognize campus police's command presence related to cybercrime, they may be less likely to commit cybercrimes. The agency's cyber posture is directly related to the capacity of the staff it employs. If the agency is perceived as weak, offenders will feel emboldened to operate without fear of investigation or sanction.

Research Questions

Research Question 1: How does the education level of sworn officers impact the capacity of campus police agencies to conduct cybercrime investigations?

Research Question 2: How does the demographic makeup of a campus police department impact the agency's choice of method to investigate cybercrime?

Null Hypothesis 1. There is no significant difference between the education level of sworn officers whose agency has a specialized cybercrimes unit.

Alternative Hypothesis 1. The education level of sworn officers whose agency has a specialized cybercrimes unit will be higher.

Null Hypothesis 2. There is no significant difference between the required education level of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 2. The required education level of sworn officers is higher when campus police departments use more formalized methods to investigate cybercrime.

Null Hypothesis 3. There is no significant difference between the required training hours of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 3. The required training hours of sworn officers are higher when campus police departments use more formalized methods to investigate cybercrime.

Null Hypothesis 4. There is no significant difference between the campus police department operating budgets and the methods chosen to investigate cybercrime.

Alternative Hypothesis 4. Campus police department operating budgets are higher when they use more formalized methods to investigate cybercrime.

Null Hypothesis 5. There is no significant difference between the campus police department operating budgets and the number of training hours required for sworn officers.

Alternative Hypothesis 5. Campus police department operating budgets will be higher when the number of training hours required for sworn officers is higher.

Significance of the Study

At the time of this writing, the COVID 19 pandemic of 2020 is in full force with tens of thousands of new daily infections. K-12 schools, businesses, government agencies, and higher education institutions have transitioned to remote work made possible by cloud-based computing and communication tools. In short, more people are online than ever before, and many activities that traditionally took place in person have transitioned online; this presents new opportunities for cybercriminals.

To close the opportunity gap, campus police agencies must deploy resources in such a way as to “deter the would-be offender from committing a crime against an available target” (Hawdon, 2020, p. 550). Targets are the campus community; this is significant as the transition online, which started two decades ago and was recently accelerated by the pandemic (2020-2021), is here to stay. As a result, cybercrime will increase in occurrence and complexity. Campus police forces must have the capacity to investigate and project a hardened cybersecurity posture.

Limitation and Delimitation

The most recent Department of Justice Bureau of Justice Statistics (BJS) campus police survey took place in 2011-2012. Although this data is eight years old, it is the most current nationwide survey data available on the demographics and practices of college and university police agencies. The BJS survey limits cybercrime discussion to one question with four unique methods to investigate cybercrimes. Looking for correlations between the method chosen and demographic data, also captured in the survey, can produce expanded results. While this research seeks to understand campus police's capacity to investigate cybercrime, it is essential to note all campus police agencies are not equal. Some campus police agencies have more autonomy to make operational decisions than others from the institutions' administrations. Also, this research only focuses on four-year institutions with 2,500 or more students. Additional research is needed to address smaller institutions with less than 2,499 students and two-year institutions with campus police agencies.

Definition of Key Terms

Command Presence: Police officers' ability to project themselves as an authority to be respected and obeyed by the general public. The officer's level of command presence is defined by the perceptions of those in their orbit.

The doctrine of Loco Parentis: A legal term holding that educators take on the parents' custody role of students in their care in the absence of parents.

Forensic Evidence: Evidence of a crime captured through scientific methods that may be used in court to determine guilt or innocence with a proper chain of custody.

Injury: A legal term used to describe harm to one's person, property, or infringement of a legal right.

Jurisdiction: A legal term that describes the power to make legal decisions or judgments with a specific location or type of case.

Policing: The act of maintaining law and order.

Third-party policing: When a police agency enlists assistance from an outside agency, corporation, or person to investigate.

Posture: The actions, approach, and attitude police take to gain the upper hand.

Summary

Higher education institutions have a duty to protect the campus community from physical and virtual threats. For 100 years, campus police have provided guardianship over the campus community. Their tactics have evolved and changed to meet the challenges of each era. The cumulative effect has led some departments to reach the status of a full-service police agency on campus. While many agencies have progressive policies and procedures, all campus police are not created equal. Some campus police agencies have greater capacity than others, a reality acceptable in concept but disastrous for many injured persons seeking assistance. Injured parties expect campus police to respond appropriately to all calls for assistance. As it relates to cybercrime, campus police have a duty to investigate. The method utilized to perform this work is in question and is a research topic.

Each agency's staff and resources' specific characteristics either limit or support the investigative techniques the agency has chosen to employ to investigate cybercrime. Together the characteristics and investigative techniques used constitute the agency's capacity to

investigate cybercrime. This research is vital as it can provide campus police administrators insight that guides future staffing and/or procedural decisions.

CHAPTER 2: REVIEW OF LITERATURE

Law enforcement, otherwise known as “the police,” is described by Wood as a state-based security force with a monopoly over the use of force within an identified territory (Wood, 1998). Law Enforcement exists to maintain social order and regulation as defined by law or, in the case of campus police, enforcing university regulations and policy (Brown, 2015; Wilson, 2015; Wood, 1998). Policing as an American institution started in the 1700s, with armed patrols to capture and return runaway slaves becoming a more formal institution in the 1800s as immigrants poured into American cities. Modern policing or law enforcement has evolved over the last 200 years to meet society’s changing needs and crime prevention. Many believe “armed guards are the best way to prevent violence in schools” (Neil, 2009, P.41). On a college or university campus, the armed guards are the campus police force. This research reviewed campus police’s origin and evolution, from watchmen (security officers) to full-service police agencies, and the expectation of protection on campus from all crime.

As campus police continue to evolve, so will the threats they face. How campus police prevent and investigate emerging threats is the focus of this research, specifically, the threat of cybercrime and its impact on the campus community. Campus police have adopted firearms, body-worn cameras, and various technologies and tactics commonplace in traditional police organizations. Campus police have also mirrored their recruiting, training, and supervision after traditional police agencies, which have led to campus police’s mutual respect and legitimacy in the eyes of their municipal peers. With new techniques to fight crime, how are campus police addressing cybercrime on campus?

Theoretical Framework

Routine activity theory provides a compelling theoretical framework for this research. “According to the theory, criminal opportunities emerge when motivated offenders converge in time and space with suitable targets in environments lacking capable guardianship” (Reyns, 2013, p. 218). The theory has been utilized to examine many types of crimes requiring the target and offender to be in close physical proximity (Reyns, 2013). The theory’s versatility in identifying and explaining elements that motivate crime has made it popular among researchers (Reyns, 2013). Some have started to use the theory to study crimes that occur from a distance, in which the target and the offender never come into physical contact (Reyns, 2013). Cybercrimes such as computer intrusions, theft, fraud, unauthorized disclosures, harassment, and intimidation do not require close physical proximity. As Reyns noted, “although the routine activity approach was originally written to account for direct-contact offenses, the perspective also has utility in explaining crimes at a distance” (p. 218). On a college or university campus, the targets are students and staff who spend extended periods online. Campus police officers are the guardians with the duty to warn and protect the campus community. The ability of campus police to warn and protect students and staff from cyber threats is mostly unknown. In the absence of strong cyber guardianship, offenders may feel motivated to commit cybercrimes. Routine activity theory explains why campus police’s capacity to investigate cybercrime is vital to protecting students and staff.

Evolution of Campus Police

From Campus Security to Full Service Police

Higher education has evolved steadily over the last 400 years. Attending an institution of higher education has become a natural step in the progression from student to young

professional. Once reserved for the rich, it is now an expected growth and development experience. As institutions have evolved, so too have the services that they provide. With many young people attending school away from home, the institution took on a parental role and responsibility, requiring institutions to provide a safe and secure learning environment (Wada, 2010). Colleges and universities hired retired police officers, former military service members, and untrained men to serve as campus watchmen (Bromley, 1998, 2003; Patten, 2016). Their primary function was to protect campus property and maintain appropriate student behavior aligned with the “doctrine of loco parentis” (Bromley, 1998, 2003). With World War II’s conclusion in 1945, the resulting GI Bill made colleges and universities accessible to millions of returning service members. In response, many institutions expanded their campuses’ size and scope (Bromley, 1998, 2003).

By the 1950s and early 1960s, the watchman style of law and order no longer met campus security needs. The Dixon vs. Alabama Board of Education decision by the United States Court of Appeals ended colleges’ and universities’ authority to discipline under loco parentis (Bromley, 1998). In addition to the loss of loco parentis, civil unrest on campuses due to the anti-war and civil rights movements required a complete police response (Bromley, 1998, 2003; Dache-Gerbino, 2016; Perez & Bromley, 2015; Roberg & Bonn, 2004). Perez and Bromley (2015) posited local law enforcement made situations worse when called for assistance by institutions. Lai’s (2016) research shows that student-led movements created a legacy of confrontation with the police. In general, students observed cultural norms and took direction from student leaders, but some students still presented problematic behavior necessitating a police response (Lai, 2016). Many state legislatures recognized campus policing’s unique nature

and granted full police powers to campus law enforcement units by deputization or state law (Bromley, 1998, 2003; Hummer, 1998; Perez & Bromley, 2015).

With new police powers, campus departments recruited former federal and local law enforcement to serve as chiefs. As campuses grew in size and scope, sometimes resembling small cities, the campus police department adopted municipal departments' methods and training. The research states that campus police departments employ more women and minority officers (Perez & Bromley, 2015). Yet, pay for these officers lags municipal agencies (Perez & Bromley, 2015). Lower pay translates to increased recruiting and higher officer turnover. Perez and Bromley (2015) noted that campus police received more training hours than municipal officers (Wilson, 2015), pointing out the additional hours needed to familiarize the new officers with campus culture, communities, and organizations. This implies that campus police are specially trained and uniquely qualified to deal with law enforcement issues on college and university campuses. On the flip side, as illustrated by the 2015 shooting of an unarmed black man by a University of Cincinnati campus police officer, campus police are not trained to deal with situations off-campus (Perez & Bromley, 2015).

Bromley noted that campus Social unrest of the 1960s prompted white people to move out of inner cities to the suburbs, a process that is colloquially known as white flight (Dache-Gerbino, 2016). Many downtown 4-year colleges and institutions moved as well to sprawling campuses (Dache-Gerbino, 2016). By the 1980s and 1990s, higher education institutions started to move back to the inner cities with a heightened law enforcement presence. Dache-Gerbino's research stated that the increased security was "necessary to keep nonstudents out and to keep faculty and staff safe" (Dache-Gerbino, 2016, p. 65), which is significant because the larger suburban campuses were security guard free (Dache-Gerbino, 2016).

police continued to evolve into full-service law enforcement agencies during the 1980s and 1990s by adopting much of municipal agencies' hiring practices, standards, training, and equipment (Bromley, 1998) . The increased professionalization of campus police also includes the use of firearms and college coursework (Farnworth, 1998; Hummer, 1998). Not all campuses have evolved at the same rate. While the large metropolitan colleges and universities are adapting to the realities of increased violent crimes on campus, many small institutions have resisted change.

1.2 Expectation of Protection

A safe campus environment is an integral part of the student learning experience (Wada, 2010). This point is exemplified by Yale University's decision to employ two police officers full-time back in 1894 (Border & Peterson, 1983; Paoline, 2003; Wada, 2010). Institutions have a duty to provide "reasonable security" (Schuh, 1999). At public institutions, protecting students and protecting the rights of non-students are in conflict. Although non-students cannot be banned from campus if they have not committed a crime, institutions have a duty to anticipate criminal activity and provide a warning to potential victims (Schuh, 1999). Does an institution's duty to foresee the danger to the school community's members override an individual's right to be on campus? That is a question with no definite answer as opinions differ from court to court (Schuh, 1999). Ultimately, institutions must protect the campus community by providing reasonable notice or warning. This duty to warn is not without conflict as it may require surveillance techniques and or disclosure of information that may or may not violate a person's civil rights (Brunson, 2018; Halder, 2013; Schuh, 1999).

Parker's (2016) research reported that stereotyping and stigmatization are still significant issues for black men at predominantly white institutions (PWI) of higher education (Parker,

2016). While some students reported feeling safe and welcomed at the institution, an equal number reported feeling unsafe. For example, one student came from a very violent neighborhood back home; he experienced a feeling of safety being on campus (Parker, 2016). In contrast, another student described being called ““nigger, nigger, nigger”” (Parker, 2016, p. 34) by white students. This led to a feeling of being unsafe—two very different experiences on PWI campuses. Campus police were cited as a source of stress for black male students. Distrust of campus police supports a toxic institutional environment (Brunson, 2018; Parker, 2016; Weitzer, 2005). A student recalled being profiled and treated with suspicion, making him feel that he was being targeted (Kahn, 2017; Parker, 2016; Weitzer, 2005). Students in the study related to “being targeted by campus police in a way that felt intrusive and unjustified” (Parker, 2016, p. 85). Although students expressed conflicting views of safety on a predominantly white campus, most black males in the study expressed a feeling of safety (Parker, 2016).

Incidents of police shooting unarmed black men have ushered in the use of body-worn cameras (BWC). Body-worn cameras reduce the number of complaints about police and positively affect officer interactions with the public (Lyle, 2016; Pelfrey, 2016). Campus police officers deal disproportionately with alcohol and drug issues since most college campus offenses involve intoxicated individuals (Pelfrey, 2016). The school environment presents additional privacy issues. Campus police officers must be aware of privacy issues related to residence halls, medical campus facilities, and underage students under the influence of drugs or alcohol. Additional research is needed on how police body-worn cameras square with federal student data, privacy, and health information laws (HIPAA, FERPA, and COPPA).

Wada (2010) stated that scholars do not identify campus police as real police. Universities do not view campus police as part of the university system because they are cops

(Wada, 2010; Wilson, 2015). Conversely, scholars do not consider campus police to be real police because they only operate within the university system (Wada, 2010; Wilson, 2015). Campus police are not viewed as legitimate by the students they serve (Wada, 2010). This perception of campus police is not without merit. The history and slow transition of campus security groups to full-service police organizations follow a path of variation rather than standardization. Many institutions seek to maintain the campus community's sanctuary-like quality away from crime (Bromley, 2003; Hummer, 1998). The research describes this view as idealistic and outdated. It states that it is unrealistic to consider a campus immune from violence. "Seventy-eight (78) percent of violent crimes which occur on campuses are committed by students rather than by outsiders" (Hummer, 1998, p. 1). The occurrence of violent crime on campus is an internal issue (Hummer, 1998).

Colorado, Oregon, Mississippi, and Utah each allow the carrying of concealed handguns on campus (Thompson, 2013). Three other states permit firearms in the parking areas. A U.S. Department of Education study "found that the overall homicide rate on college campuses was 0.07 per 100,000 persons" (Thompson, 2013, p. 366). College campus police chiefs do not support the carrying of concealed handguns on campus (Thompson, 2013). In response to a research question regarding whether campus police be allowed to carry firearms? The research points to the deference given to law enforcement to make life and death decisions, depending highly on the judgment of individual police officers. In the U.S. Supreme Court decision in *Tennessee vs. Garner*, the court held that deadly force is subject to the Fourth Amendment's reasonableness requirement (Gross, 2016). It is common practice for police departments only to authorize the use of deadly force in defense of human life, the officer, or another person from serious injury (Gross, 2016). The reasonableness of the officer's decision to use deadly force is

based on the information the officer had at the time. It is also noted that the level of force used is relative to the severity of the crime (Gross, 2016); in fact, police mostly use force offensively rather than defensively (Gross, 2016).

Police must maintain a positive public perception of how they work to succeed (Brown, 2015). The research suggests that voluntary interactions with police produce a positive view; involuntary interactions create a negative view (Lai, 2016). As a result, the public's perception of police is influenced mainly by direct personal interaction (Lai, 2016; Wada, 2010). If police interactions are perceived as fair, citizens are more likely to comply and cooperate (Goodman-Delahunty). Thus, how police officers treat people is a determining factor in public opinion and public cooperation (Goodman-Delahunty, 2013). Allen (2016) noted that stop and question policing (SQP) is a constitutional police practice under the 1968 Supreme Court decision. It confirmed that police officers could stop and question citizens if the officer has a “reasonable suspicion,” which has a lower threshold than probable cause (Allen, 2016). In a subsequent court ruling, police were given the additional power to frisk (Allen, 2016). What may seem to be an invasion of privacy to the public was granted to ensure officers’ and the general public’s safety. The court established SQP as legal, but the public has varying views of how fair it is—Allen (2016) cites “procedural fairness” and “distributive fairness” as points of conflict. Procedural fairness is the perceived fairness of the actions taken leading to a result or decision (Allen, 2016; Brunson, 2018; Goodman-Delahunty, 2014). The research reports a majority of those surveyed had a favorable view of SQP procedurally. On the other hand, distributive fairness is related to how the process and procedure are enacted on people and communities (Allen, 2016). Citizen cooperation and compliance are inextricably linked to the public's perception of the fairness of policing procedures and outcomes (Goodman-Delahunty, 2014).

Campus police engage almost exclusively with students between 18 and 24 (Allen, 2015). The research describes four types of sanctions generally carried out by police: an arrest, a written ticket, verbal warnings, and written warnings (Allen, 2015). Officers have significant discretion to sanction or not based on the perceived seriousness of the crime. Seriousness is a judgment of “situational factors,” further defined as “legal and extralegal factors” (Allen, 2015). The research describes legal factors as the level of seriousness. Many officers believe the punishment should equal the crime (Allen, 2015). Some specific offenses require the officer to sanction as prescribed by law. Extralegal factors are described as the structure of how the officer became involved in the encounter, meaning that sanctioning decisions are impacted by the sequence of events that brought the officer to the scene (Allen, 2015). The encounter could be officer-initiated or in reaction to a call for assistance. The age and status of enrolled students on campus may influence the level of sanction sought.

It is expected that the police will investigate and hold those responsible accountable when an individual, group, or entity is harmed. Campus police—like municipal, state, and federal law enforcement—have evolved to keep pace with an equally resilient and progressive criminal element. The research describes in detail the various ways in which this has happened over the last century. Absent from the research was the identification and investigation of cybercrime.

Cybercrime and How it Impacts the Campus Community

Cybercrime Defined

Davis (2012) noted that the Internet is a tool with the potential to accelerate crime, but it is not the cause of crime (Davis, 2012; Williams, 2008). The research identifies two working definitions of cybercrime. “The ‘use of a networked computer or internet technology to commit or facilitate the commission of a crime’” (Brown, 2015, p. 57), as defined by the Association of

Chief Police Officers (2009). The more basic definition is “offenses committed using an electronic data storage or communications device” (Australian Institute of Criminology, 2011; Brown, 2015, p. 57). Brown (2015) noted that unethical or harmful behavior online does not equate to a crime. Conduct or actions online can only be prosecuted if they are forbidden by law (Brown, 2015). Computers also reduce the probability of prosecution due to cybercrimes’ indirect and anonymous nature (Davis, 2012; Williams, 2008). While many agencies and levels of the criminal justice system have varying views and definitions of cybercrime, the following criteria can be used to test if online behavior meets the requirements of a cybercrime:

The conduct is facilitated by information and communications technology; The conduct is motivated by intent to commit harm against a person or organization; The perpetrated or intended harm encompasses conduct amounting to interference or damage to either tangible or intangible property owned by a person or organization; and the conduct concerned is criminalized within either the jurisdiction of the victim or the jurisdiction of the accused. (Brown, 2015, p. 57)

Even with new definitions of cybercrime and the enactment of new laws to “police” online activity, “the pace of technological change will continue unabated, and the adaptability of cyber-criminals will continue to pose challenges for law enforcement” (Broadhurst, 2006, p. 409).

While identifying the perpetrator is essential, “the avoidance of wrongful accusations deserves equal attention” (Da-Yu, 2009, p. 202). Many law enforcement agencies are ineffective at responding to cybercrime, as many “play catch-up” to identify and apprehend computer-savvy criminals (Broadhurst, 2006, Sussmann, 1999). Broadhurst (2006) drew attention to the Internet’s decentralized nature, comparing it to a lawless open highway. The conventional technical fix (i.e., firewall, virus protection) will not deter cybercriminals; public and private police agencies must get involved to curtail criminal activity online (Broadhurst, 2006).

Cybercrime on Campus

The research points to a decline in most violent crimes on campus; the concern now is vulnerability to terrorist attacks and safety from other students or non-students on campus (Dameron, 2009; Thompson, 2009). Campus safety now goes beyond the students' physical security; it has now moved into the "cyber-realm" (Dameron, 2009). Many cybercrimes go unreported due to a lack of understanding of the police's capacity to investigate and apprehend offenders (Brown, 2015; Spencer, 2020). Brown (2015) also cites a lack of confidence in the ability of police to investigate cybercrimes. The use of digital devices by staff and students is ubiquitous on campus, which lends credence to the research that cites the prevalence of digital devices as critical evidence in criminal investigations (Davis, 2012). Emerging cybercrimes that are a specific threat to the campus community include "non-consensual image sharing, voyeurism, and the unauthorized sharing of intimate images (Spencer, 2020).

Current Strategies: Cybercrime Prevent and Investigate

Capacity to Investigate Cybercrime

There has been an ongoing debate since the early 1900s over the value and necessity of a college education for police work (Roberg, 2004). Most police officers do not need a four-year degree; however, "police work is changing in ways that call for higher education" (Baro, 1999, p. 58). Simply "'bagging-and-tagging,' or 'monkey see, monkey do'" (Brown, 2015, p. 65) policing will not do. With over a century of investigative practice, police officers are very confident in their ability to investigate traditional crimes of robbery, burglary, and murder (Davis, 2012). The question is whether police are prepared or perceive themselves to be prepared to investigate cybercrimes. In other words, should police agencies recruit the educated or educate the recruited (Roberg, 2004)? Lersch (2001) noted the college experience provides officers with a more significant foundation for making decisions leading to more creative and innovative

practices. Cybercrimes require police to have the aptitude to find relationships between pieces of information or unrelated events (Brown, 2015). That is the “independent verification of digital clues... finding corresponding information from different sources, and . . . adequate preparation of a valid argument” (Da-Yu, 2009, p. 205). “Finding the right blend of competencies to meet the rigors of cybercrime inquiry is very difficult” (Brown, 2015, p. 65). The criminal justice system could not prosecute cybercrime offenses if a proper investigation were not completed (Bossler, 2020). Bossler (2020) pointed to research that suggests that law enforcement agencies, in general, are not equipped to investigate serious cybercrime, even though some agencies have specialized units for cyber investigation and digital forensics. Many frontline officers feel unprepared due to a lack of technical knowledge and resources (Bossler, 2020). Barro (1999) argued that a lack of higher education among officers in supervisory roles and those in specialized units is problematic. Brown (2015) cited the inability of police stakeholders to understand fundamental aspects of computer-based crime. This is significant as the capacity of police investigators to understand illicit use of information technology directly impacts investigative outcomes (Brown, 2015). Initiatives to target specific crime types (i.e., cybercrime) are only successful if there are understanding and buy-in from leadership (Davis, 2012).

Paoline (2003) identified college and university police as “specialized” police who operate with full powers of arrest and use of force. Most campus police departments structure and organize themselves after municipal agencies (Paoline, 2003). The campus police also employ separate specialized units to handle core tasks (Paoline, 2003). Many variables, such as the size and cost associated with running the agency, impact the level of resources available to specialized units (Paoline, 2003). Cybercrime is invisible, as it often has no physical component or face. Cybercriminals can commit crimes with no footprint in time and space (Burrus, 2020;

Yar, 2005). Many officers are disinterested when there is no physical nature to the crime, reinforcing the idea that crimes that do not occur in the real world are less important (Burruss, 2020); Gannon and Doig, 2010). As a result, these crimes do not garner the needed support or political response from government and law enforcement leaders (Davis, 2012). Paoline (2003) argued that campus police at public institutions have more autonomy in organizing and deploying resources. Alternatively, private institutions exert more administrative control over campus police agencies out of fear of the negative impact an overly visible campus police presence may have (Paoline, 2003). Hauser (2015) has the opposite view, citing research that finds police visibility reduces the fear of crime. Campus police will often be the first responders to a report of cybercrimes; victims will expect a police response immediately (Burruss, 2020; Wilson, 2015). “Unfortunately, in general, law enforcement officers are not capable of responding to calls involving cybercrime (Leukfeld et al., 2013)” (Burruss, 2020, p. 107). In addition to unprepared officers, other challenges exist with jurisdiction, constitutionally protected freedoms of speech and privacy, and fear of sharing information internally and externally with other agencies (Halder, 2013).

External Partnerships

Improving police capacity to prevent and investigate crime has been a central focus of problem-oriented policing (POP; Cherney, 2008). POP is a policing model utilized by many law enforcement agencies worldwide to address emerging threats and challenges and drive innovation in policing. The POP approach requires agencies to analyze the problem, identify the vulnerability, develop a strategy, and implement the solution (Cherney, 2008). Cherney (2008) posited that POP is not merely about the police’s motivation to change their approach to police problems. It is about motivating police “to re-conceptualize how they address the problems the

public expects them to handle” (Cherney, 2008, p. 632; Goldstein, 2003). The research cites the reluctance of police organizations to think outside of the “traditional reactive policing strategies” and embrace “innovative problem solving” to address crime (Cherney, 2008). Police need to develop various collaborations to combat cybercrime and collaborate with other agencies, private institutions, and other nations' law enforcement (Broadhurst, 2006; Cherney, 2008). Utilizing the investigative and crime control capacity of other agencies or institutions is known as “leveraging or “third-party policing” (Cherney, 2008). “The level of inter-dependency that exists between participants in such contexts and the pooling of capacity that can result, capabilities and resources are enhanced and extended beyond the narrow functional responsibilities of any one single agency” (Cherney, 2008, p. 633). Connor (2009) identified this process of sharing knowledge and technical assistance as capacity-building, long-term.

Because third parties can profit from cybercrime (Cherney, 2008), Brown (2015) suggested creating new laws to compel third parties like internet service providers to report nefarious activity on their networks. Broadhurst (2006) offers hacking, cracking, and computer trespass as examples of activities that should be made illegal and criminalized. When cybercrime is reported, forensic data can be shared with law enforcement by ISPs. In this case, the ISP takes responsibility for its influence in facilitating or investigating possible cybercrime.

It is a legitimate policing strategy to leverage third-party groups, agencies, or individuals (Cherney, 2008). In some cases, the police should financially reward the third party for their assistance (Cherney, 2008). In other cases, the third party should pay the government sanctions for not taking responsibility for crime reduction over which it has influence (Cherney, 2008). Ultimately, it is reasonable for campus police to leverage institutional systems and individuals or collaborate with other agencies to fight cybercrime (Cherney, 2008).

Summary

Law enforcement, collectively known as the police, exists to maintain order as defined by law, regulation, or policy on college campuses. The research describes the institution of police as a state-based security force with a monopoly over the use of force within an identified territory (Wood, 1998). Campus policing started in the late 1800s and evolve. Bromley (1998) described how the anti-war and civil rights movements of the 1960s motivated the evolution from campus security forces to full-service police departments. These new departments were given full police powers to arrest and use force to quell campus violence. Professionalization of campus police continued to include adopting equivalent tactics, recruiting, training, and command structures as municipal agencies (Bromley, 1998). Seventy-five college and university police agencies have passed a rigorous self-assessment and been awarded the prestigious CALEA® (Commission on Accreditation for Law Enforcement Agencies, Inc.) accreditation.

Many campus police organizations provide full-service police services that mirror local municipal agencies. Campus police have the training, experience, and accreditation to investigate and resolve traditional crimes. Cybercrime presents a new threat to the campus community. Investigating cybercrime requires specific technical skills, decision-making, and creativity to backtrack the events leading to the crime (Lersch, 2001). To meet the need, should campus police agencies buy or build? In other words, should they recruit the educated or educate the recruited (Roberg, 2004). Individuals with technical expertise would expect a higher salary than would be offered to a new officer. The research suggests an alternative is a partnership with third-party agencies, groups, or individuals. These partnerships would expand the capacity of campus police organizations to fight cybercrime.

CHAPTER 3: METHODOLOGY

This chapter introduces the quantitative research study. A causal-comparative design was chosen to understand the impact of education/training, recruiting, or partnerships with on-campus police capacity to investigate cybercrime. This research design will analyze survey results of more than 905 U.S. 4-year higher education institutions with 2,500 or more students who utilize sworn police officers to provide law enforcement services (Reaves, 2015). The tool utilized to capture data for this study is the “Survey of Campus Law Enforcement Agencies” designed by the U.S. Department of Justice (USDOJ), Bureau of Justice Statistics (BJS). The researcher’s choice to utilize a causal-comparative design was due to the need to compare the demographic makeup of each agency to the resources deployed to investigate cybercrime. Cause-effect comparison identified which demographic variable enhances an agency's investigative capacity. The research plan includes the setting of the study, participants, data collection, data sources, data analysis, and ethical concerns.

Research Questions

To effectively solve cybercrimes, campus police administrators need to understand the capacity of their departments to investigate cybercrime. This study aims to identify what financial, education/training, recruiting criteria, or partnerships enhance the capacity of campus police to investigate cybercrime; this will allow campus police administrators to reallocate resources to better support cybercrime investigations.

Setting & Sample

This study was conducted at Saint Peter’s University (SPU) during the spring and fall semesters of 2021. SPU is a private 4-year Jesuit institution of higher education located in Jersey

City, New Jersey. Due to the pandemic in America and worldwide, I conducted most of this research in the virtual environment.

To understand the nature of law enforcement services available to campuses within the Student Right to Know Act and Campus Security Act of 1990 frameworks (Reaves, 1996), the Bureau of Justice Statistics developed the Survey of Campus Law Enforcement Agencies (SCLEA) and published the results 1995. It was “the largest study of police and security services at institutions of higher education ever conducted” (Reaves, 1996, p. 1). The 1994-95 report captured survey responses from approximately 600 campus police agencies. In the 1995 report computers were cited as utilized for record-keeping, management, and other research functions; there was no mention of computer-based or cybercrimes (Reaves, 1996).

When the survey was conducted again in the 2004-05 school year, approximately 750 campus agencies responded (Reaves, 2008). The survey evolved with the addition of cybercrime as a problem to be addressed with a specialized unit or designated personnel (Reaves, 2008). The most recent SCLEA survey data available was conducted in 2011-12. Approximately 900 campus agencies provided data. The survey evolved once again, asking the agencies to identify the specific method utilized to investigate cybercrime.

Based on the 2011-12 SCLEA, “data will be collected on personnel, functions, expenditures and pay, operations, equipment, computers and information systems, community policing activities, specialized units, and emergency preparedness activities” (Davis, 2012). The survey was sent to 4-year institutions with 2,500 or more students (Davis, 2012). Based on the historical eight to ten-year gap in the administration of this survey by the USDOJ’s BJS, the next administration of the survey could be within the next two years. Due to the fast pace and

evolution of technology and cybercrime, an additional future study should compare how agencies have evolved since 2011-2012.

Participants

I utilized publicly available survey data from 905 colleges and universities. To become a participant in this research study, the institution must meet the following criteria: (a) Be a four-year institution located in the United States or territory, and (b) have answered the cybersecurity question in the USDOJ's BJS SCLEA survey. Of the 905 institutions that met the criteria for inclusion, 450 colleges and universities responded to the cybercrimes investigation question in the survey and were included as participants in this study. For this research, the term participant is descriptive of the participating campus police agency rather than a person or group of persons. No students will participate in this research study. The 2012 SCLEA survey was targeted at institutions with 2500 or more students only.

The Researcher

I have worked in education for 14 years and hold a Bachelor of Arts (B.A.) in Information Technology & Informatics, a Master of Science (M.S.) in Learning Technologies, and Specialist in Education (Ed.S.) in Educational Leadership. The researcher is also a State of New Jersey certified School Safety Specialist and Educational Facilities Manager. Although the researcher has trained and worked with local and state law enforcement on K12 school security matters, there is no direct relationship with campus police agencies that would cause a conflict of interest. With years of work experience as a school district Director of Technology and leadership and security training, I have the technical skills needed to conduct this research study. In addition, I have completed the Collaborative Institutional Training Initiative (CITI) Program course in Human Subject Research and a research methods course at Drexel University.

Data Collection

The data for this study were captured using a self-reporting agency questionnaire (survey) from the Bureau of Justice Statistics (BJS). As per the BJS, “public reporting burden for this collection of information is estimated to average 2 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information” (Davis, 2012). The survey results were made available for download by the National Archive of Criminal Justice Data hosted by the University of Michigan in partnership with the BJS.

Data Source(s)

Publicly available survey results from the 2011-2012 BJS Campus Police survey provided a single data source for this research study. The survey asked each agency 56 questions with additional sub-questions to many of the primary questions. Results of the questionnaire are available in excel or tab-delimited CSV file format. Each question is identified in the results only by number-letter code. Each number-letter code combination is identifiable with the associated codebook—the codebook assists in identifying and labeling each question for further data analysis.

Data Analysis

With approval to conduct the study, survey results were analyzed for fitness to participate in this research study and identified institutions will be sorted out for further analysis. When all participant institutional agencies have been identified, a series of binary logistic regression, logistic regression, and simple linear regression analyses will be conducted to determine a statistical difference between two variables to test hypotheses about the relationships between the data.

Before the inferential analyses, descriptive statistics were used to describe the characteristics of participants, determine the frequency of responses, and test the assumptions of parametric testing. The assumptions for binary and logistic regression analysis are that data are free from multicollinearity and outliers (Pallant, 2016). The presence of outliers will be assessed using scatterplots, where the absence of outliers is confirmed when data points fall within the 3.3 and -3.3 range (Pallant, 2016).

The assumptions of linear regression analysis also include multicollinearity and outliers but add the assumptions of linearity, normality, homoscedasticity, and independence of residuals. The assumption of linearity will be assessed through a visual inspection of normal Q-Q plots. Normal Q-Q plots illustrate how data points run along a straight line (Pallant, 2016). Normality will be assessed through visual inspection of histograms and the results of the Kolmogorov-Smirnov test. The assumptions of homoscedasticity were assessed using scatterplots. A visual analysis of the scatterplots showed whether the dependent variable data cluster is rectangular, signifying that the assumption of homoscedasticity is met (Pallant, 2016). Finally, the Durbin-Watson test was used to assess whether dependent variable data meet the assumption of independence of residuals. The acceptable ranges for the Durbin-Watson test are 1.5-2.5 (Pallant, 2016).

Following assumptions testing, the main hypothesis testing analyses were conducted. Specifically, binary logistic regression analysis will be used to test hypothesis one, logistic regression analysis will be used to test hypotheses two through four, and simple linear regression analysis will be used to test hypothesis five.

Research Questions

Research Question 1. How does the education level of sworn officers impact the capacity of campus police agencies to conduct cybercrime investigations?

Research Question 2. How does the demographic makeup of a campus police department impact the agency's choice of method to investigate cybercrime?

Null Hypothesis 1. There is no significant difference between the education level of sworn officers whose agency has a specialized cybercrimes unit.

Alternative Hypothesis 1. The education level of sworn officers whose agency has a specialized cybercrimes unit will be higher.

Null Hypothesis 2. There is no significant difference between the required education level of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 2. The required education level of sworn officers is higher when campus police departments use more formalized methods to investigate cybercrime.

Null Hypothesis 3. There is no significant difference between the required training hours of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 3. The required training hours of sworn officers are higher when campus police departments use more formalized methods to investigate cybercrime.

Null Hypothesis 4. There is no significant difference between the campus police department operating budgets and the methods chosen to investigate cybercrime.

Alternative Hypothesis 4. Campus police department operating budgets are higher when they use more formalized methods to investigate cybercrime.

Null Hypothesis 5. There is no significant difference between the campus police department operating budgets and the number of training hours required for sworn officers.

Alternative Hypothesis 5. Campus police department operating budgets will be higher when the number of training hours required for sworn officers is higher.

Ethical Considerations

Each campus police department voluntarily submitted all information obtained. This research may identify specialized units and police titles with descriptions of duties and or general demographic information, including but not limited to race, sex, salary, education, and training of sworn officers, civilian staff, and contractors. No individual first and last names would be recorded as part of the research. Although no direct human subjects will participate in this study, the researcher will continue to protect each agency's confidentiality and privacy interests by not utilizing institution or agency names in reporting. Because the years-old data is publicly available, the researcher will not obtain a signed informed consent form from each agency. The researcher does not plan to utilize data from this study in future research. All data collected will be stored for six months after completing the research project and destroyed via a commercial document shredder.

Summary

This research project seeks to understand the relationship between specific demographics of campus police agencies and their methods (capacity) to investigate cybercrime. The tool utilized to capture this data is The United States Department of Justice's Bureau of Justice Statistics designed "Survey of Campus Law Enforcement Agencies." The publicly available 2011-2012 BJS Campus Police survey results will provide the data for analysis. With the approval of the Institutional Review Board, the researcher will download the survey results and

identify institutional agencies for participation in the study. The numeric data limited to specific institutions that meet the research study criteria will be compiled and added to a database. A series of *t*-tests will be conducted to determine the significance level of each null or alternative hypothesis. The resulting data analysis will be reported in Chapter 4. This research study does not require collecting or recording personally identifiable data of students.

CHAPTER IV: ANALYSIS OF THE DATA

This research study aimed to identify what financial, education/training, recruiting criteria, or partnerships enhanced the capacity of campus police to investigate cybercrime. The results may aid campus police administrators in their decision-making and allocation of resources to investigate cybercrime. The research design called for analyzing survey results made publicly available by the U.S. Department of Justice's (USDOJ) Bureau of Justice Statistics (BJS). This chapter includes a discussion of the research design, sample characteristics, assumptions testing results, and hypothesis testing results.

Research Design

A causal-comparative design was chosen to understand the impact of education/training, recruiting, or partnerships with on-campus police capacity to investigate cybercrime. The researcher's choice to utilize a causal-comparative design was due to the need to compare the demographic makeup of each agency to the resources deployed to investigate cybercrime. This cause-effect comparison identified which demographic variable enhances an agency's investigative capacity. Data were collected from the 2011 Survey of Campus Law Enforcement Agencies results. The survey consisted of 64 questions with many sub-questions requiring multiple answers. Eight of the sixty-four survey questions were integral to answering the quantitative research questions.

Characteristics of the Sample

Of the 905 institutions that met the criteria for inclusion, 450 colleges and universities responded to the survey and were included as participants in this study. However, 203 cases were removed for containing invalid data, with codes indicating refusals to respond, missing data, or other out-of-bounds values. The sample institutions are mid-sized to very large institutions with

student bodies ranging from 3,398 to 38,000 students. The average student population is 15,863.

Table 1 provides the mean responses to the scale study variables, including a budget, required training hours, and percentage of officers with higher education. Table 2 provides the frequencies in responses to nominal variables, including whether the department had a designated cybercrime unit (1 = yes, 2 = no), cybercrime investigation method, and required education level.

Table 1

Descriptive Statistics

Variable	Mean
Budget	1,706,328.57
Required Training Hours	935.85
Percentage of Officers with Higher Education	.38

Table 2

Frequencies

		N	%
Required Education Level	High school diploma	192	77.7%
	Some college, no degree	21	8.5%
	2-year college degree	25	10.1%
Cybercrime Investigation Method	Unit with personnel assigned full time	15	6.1%
	Designated Personnel used as needed	136	55.1%

	Policies and procedures only	38	15.4%
	Not officially addressed	58	23.5%
Has Designated Cybercrime Unit	Yes	15	6.1%
	No	232	93.9%

Assumptions Testing Results

The assumptions for binary and logistic regression analysis are that data are free from multicollinearity and outliers. Multicollinearity was assessed through the variance inflation factor (VIF) by running a collinearity diagnostic. Variance inflation factors less than 10 indicate acceptable levels of multicollinearity. Based on the VIF statistics, data met the assumption of multicollinearity (see Table 3).

Table 3

The Variance Inflation Factors for Independent Variables

	Collinearity Statistics	
	Tolerance	VIF
Required Training Hours	1.00	1.00
Budget	1.00	1.00
Required Education Level	1.00	1.00

The presence of outliers was assessed using scatterplots, where the absence of outliers is confirmed when data points fall within the 3.3 and -3.3 range. The scatterplots showed several outliers within the dataset. The outliers were removed for required training hours and cybercrime investigation method so that data would meet the assumption of outliers (see Figure 1 and Figure 2). Outliers could not be removed for the cybercrime unit because the detected outliers were all the “yes” responses to this dichotomous variable. Therefore, cybercrime unit data did not meet the assumption of outliers (see Figure 3).

Figure 1

Scatterplot for Required Training Hours

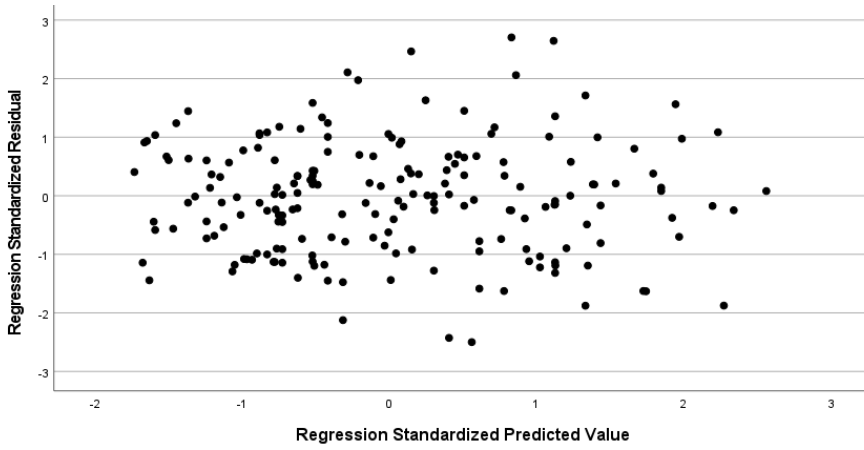


Figure 2

Scatterplot for Cybercrime Investigation Method

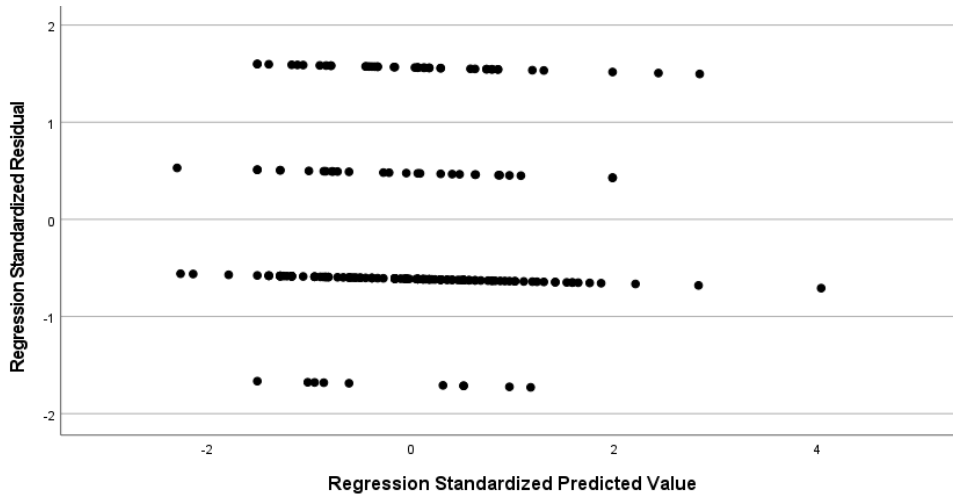
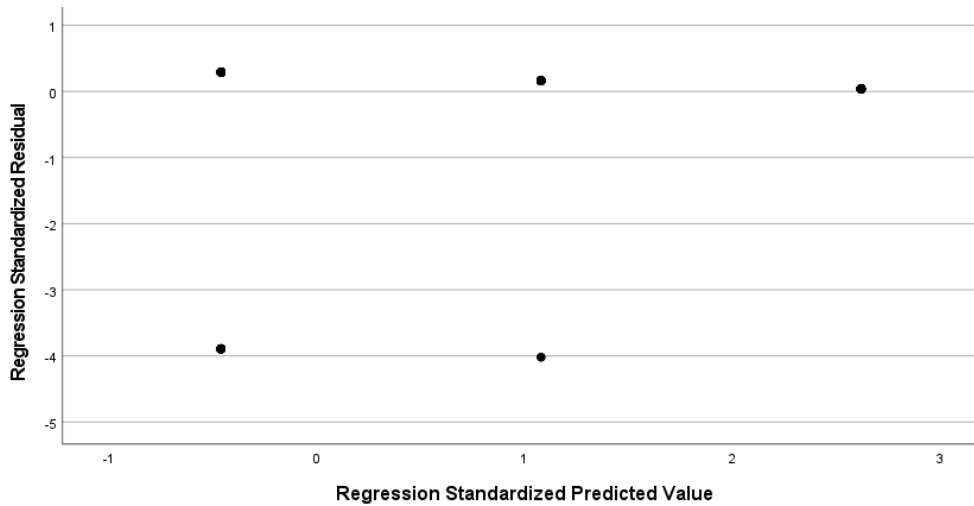


Figure 3

Scatterplot for Cybercrime Unit



The assumptions of linear regression analysis also include multicollinearity and outliers but add the assumptions of linearity, normality, homoscedasticity, and independence of residuals. The assumption of linearity was assessed through a visual inspection of normal Q-Q plots. Normal Q-Q plots illustrate how data points run along a straight line. A visual inspection of the Q-Q plots produced from the descriptive statistical analyses showed that all variables met the assumption for linearity. Figures 4-9 include the output for the Q-Q plots.

Figure 4

Normal Q-Q Plot for Cybercrime Investigation Method

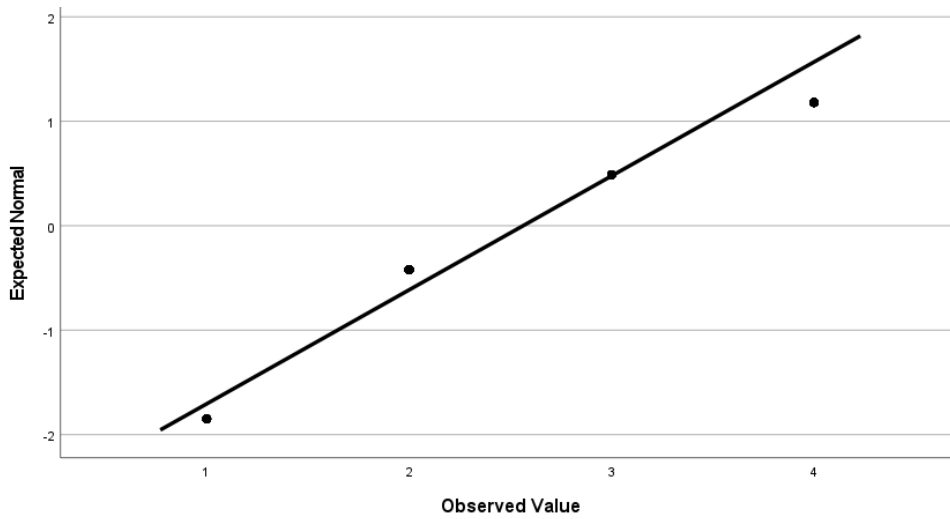


Figure 5

Normal Q-Q Plot for Cybercrime Unit

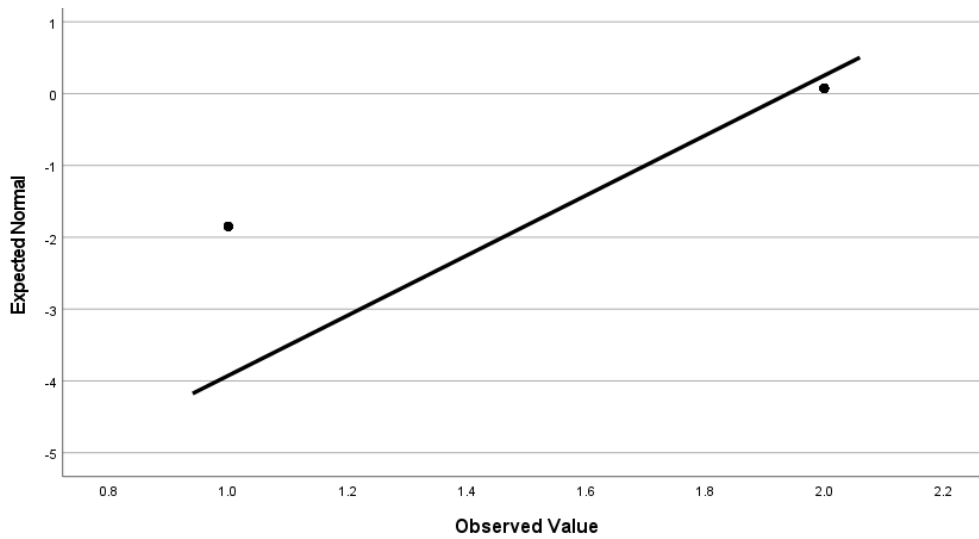


Figure 6

Normal Q-Q Plot for Budget

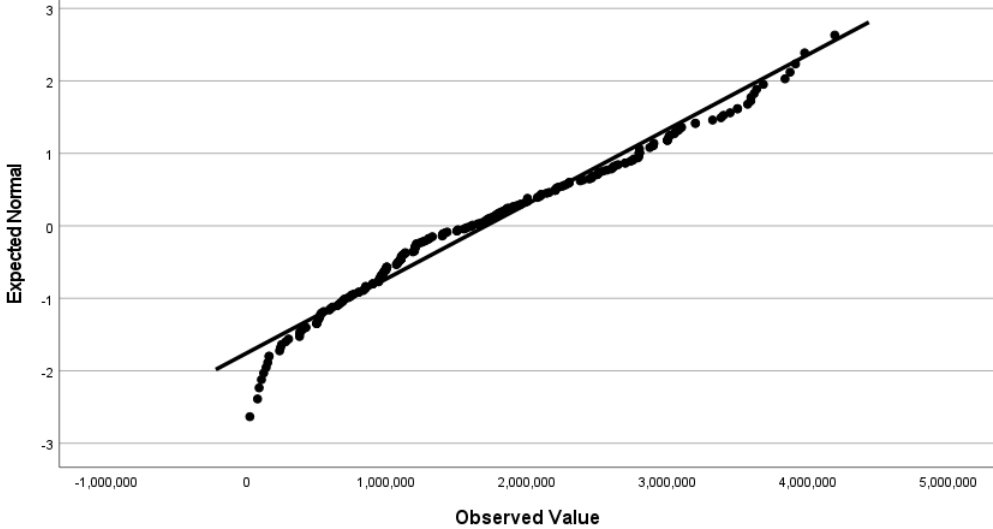


Figure 7

Normal Q-Q Plot for Required Education Level

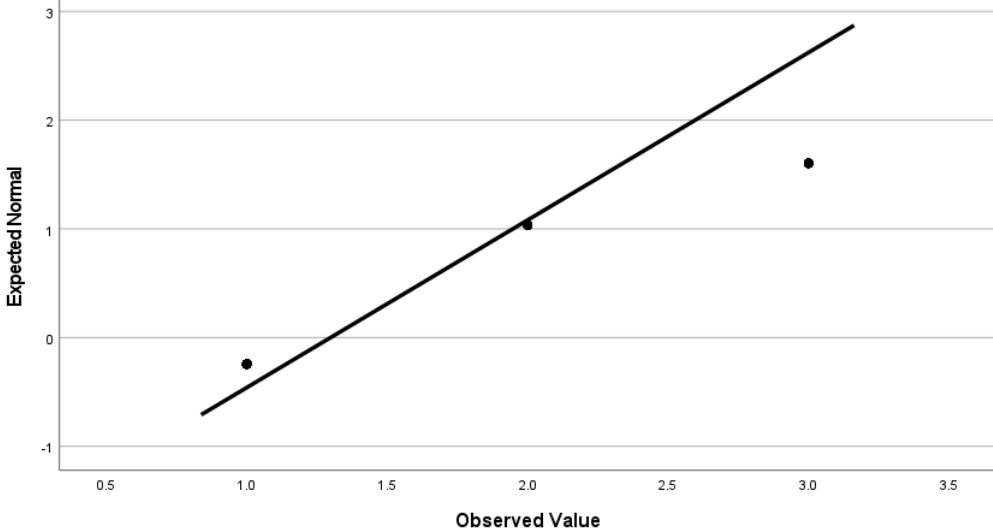


Figure 8

Normal Q-Q Plot for Required Training Hours

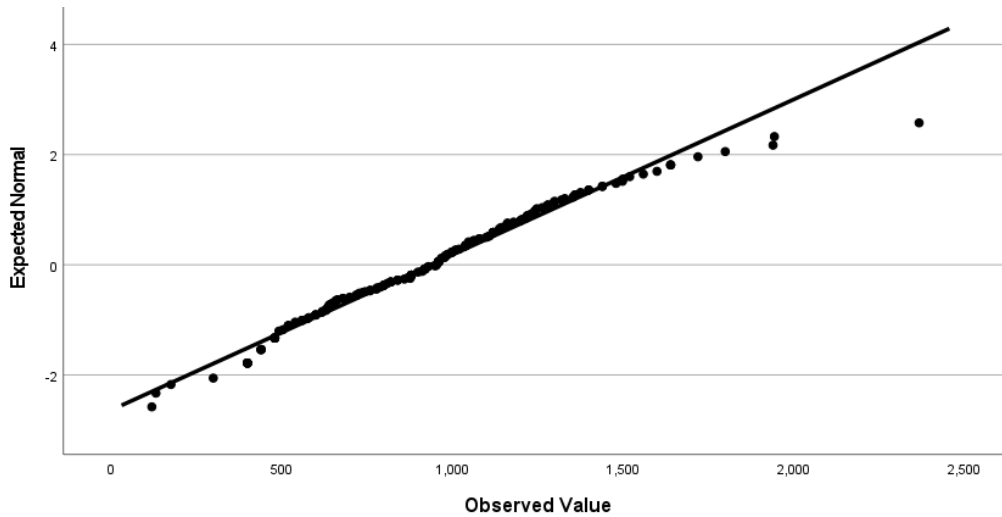
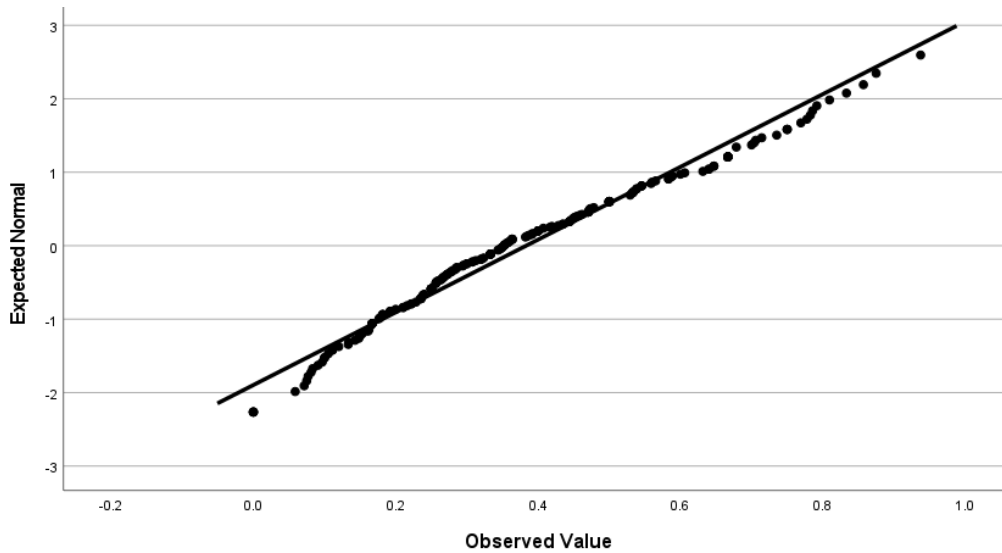


Figure 9

Normal Q-Q Plot for Percentage of Higher Education



Normality was assessed through visual inspection of histograms and the results of the Kolmogorov-Smirnov test. Based on the results of the Kolmogorov-Smirnov test, only required training hours met the assumption of normality, $p > .05$. Table 4 shows the results of normality testing.

Table 4*Tests of Normality*

	Kolmogorov-Smirnov		
	Statistic	df	Sig.
Required Education Level	.484	238	<.001
Budget	.100	235	<.001
Cybercrime Unit	.539	247	<.001
Cybercrime Investigation Method	.342	247	<.001
Required Training Hours	.045	200	.200
Percentage of Higher Education	.084	211	.001

The assumption of homoscedasticity was assessed using scatterplots. A visual analysis of the scatterplots shows that data for the dependent variable required training hours cluster in a rectangular shape, signifying that the assumption of homoscedasticity was met (see Figure 1). However, the data for the dependent variables of the cybercrime investigation method and cybercrime unit did not meet the assumption of homoscedasticity (see Figure 2 and Figure 3).

Finally, the Durbin-Watson test was used to assess whether dependent variable data met the assumption of independence of residuals. The acceptable ranges for the Durbin-Watson test are 1.5-2.5. Based on the results of the Durbin-Watson test, all data met the assumption of independence of residuals (see Table 5).

Table 5*Durbin-Watson Test for Independence of Residuals*

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1 Budget*Required Training Hours	.238	.057	.052	345.38	2.040
1 Budget*Cybercrime Method	.216	.047	.043	.89707	1.898

1 Required Training Hours*Cybercrime Method	.024	.001	-.004	.92	2.016
1 Required Education Level*Cybercrime Method	.057	.003	-.001	.92	1.867
1 Required Education Level*Cybercrime Unit	.082	.007	.003	.24	1.802

Hypothesis Testing Results

Research Question One

How does the education level of sworn officers impact the capacity of campus police agencies to conduct cybercrime investigations?

Hypothesis 1 - Education Level vs. Method

Null Hypothesis 1: There is no significant difference between the education level of sworn officers whose agency has a specialized cybercrimes unit.

Alternative Hypothesis 1: The education level of sworn officers whose agency has a specialized cybercrimes unit will be higher.

The proposed analysis method for this hypothesis was binary logistic regression analysis. However, binary logistic regression was not used because the data violated the assumption of outliers. A Chi-square test could not be used because some categories contained less than five observations. Because the assumptions of parametric testing were violated, Spearman's Rank Order Correlation (ρ) was used. They revealed no significant relationship between sworn officers' education level (i.e., percentage of higher education) and a specialized cybercrimes unit, $\rho = -.12, n = 211, p = .08$. Specifically, the percentage of sworn officers with higher education participation in a department is not related to whether a cybercrimes unit is present within that department. It was hypothesized that, because of the more intensive training and knowledge needed to investigate cybercrimes, departments with cybercrimes units might have a higher

proportion of officers with participation in higher education. Based on the results, the null hypothesis was retained.

Table 6*Nonparametric Correlations for Cybercrime Unit and Percentage of Higher Education*

		Cybercrime Unit	Percentage of Higher Education
Spearman's rho	Cybercrime Unit	Correlation Coefficient	1.00
		Sig. (2-tailed)	.077
		N	211
	Percentage of Higher Education	Correlation Coefficient	-.122
		Sig. (2-tailed)	.077
		N	211

Hypothesis 2 - Required Education Level vs. Method

Null Hypothesis 2. There is no significant difference between the required education level of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 2. The required education level of sworn officers is higher when campus police departments use more formalized methods to investigate cybercrime.

The proposed analysis method for this hypothesis was multinomial logistic regression analysis. However, multinomial logistic regression was not used because some categories had less than five observations. A Chi-square test also could not be used for the same reason. Because the assumptions of parametric testing were violated, Spearman's Rank Order Correlation (rho) was used. The results of the analysis revealed there is no significant relationship between the required education level of sworn officers and cybercrime investigation method, $\rho = -.05$, $n = 238$, $p = .40$. Specifically, it was hypothesized that departments with requirements for higher levels of educational attainment for sworn officers would be those that

could take on more knowledge- and skill-intensive methods for cybercrime investigation.

However, based on the results, the null hypothesis was retained.

Table 7

Nonparametric Correlations for Required Education Level and Cybercrime Investigation Method

			Required Education Level	Cybercrime Investigation Method
Spearman's rho	Required Education Level	Correlation Coefficient	1.00	-.055
		Sig. (2-tailed)		.396
		N	238	238
	Cybercrime Investigation Method	Correlation Coefficient	-.055	1.00
		Sig. (2-tailed)	.396	
		N	238	247

Research Question Two

How does the demographic makeup of a campus police department impact the agency's choice of method to investigate cybercrime?

Hypothesis 3 - Required Training Hours vs. Method

Null Hypothesis 3: There is no significant difference between the required training hours of sworn officers and the method chosen to investigate cybercrime.

Alternative Hypothesis 3. The required training hours of sworn officers are higher when campus police departments use more formalized methods to investigate cybercrime.

The proposed analysis method for this hypothesis was multinomial logistic regression analysis. However, multinomial logistic regression was not used because some categories had less than five observations. A Chi-square test also could not be used for the same reason.

Because the assumptions of parametric testing were violated, Spearman's Rank Order Correlation (rho) was used instead of Pearson's correlation. The analysis revealed no significant relationship between the required training hours of sworn officers and the cybercrime

investigation method, $\rho = .01$, $n = 200$, $p = .92$. It was hypothesized that given the need for practical training in investigating cybercrime properly. Departments with more knowledge- and skill-intensive methods to investigate cybercrime require more sworn officers' training. Based on the results, the null hypothesis was retained.

Table 8

Nonparametric Correlations for Required Training Hours and Cybercrime Investigation Method

			Required Training Hours	Cybercrime Investigation Method
Spearman's rho	Required Training Hours	Correlation Coefficient	1.00	.007
		Sig. (2-tailed)		.918
		N	200	200
	Cybercrime Investigation Method	Correlation Coefficient	.007	1.00
		Sig. (2-tailed)	.918	
		N	200	247

Hypothesis 4 - Operating Budget vs. Method

Null Hypothesis 4. There is no significant difference between the campus police department operating budgets and the methods chosen to investigate cybercrime.

Alternative Hypothesis 4. Campus police department operating budgets are higher when they use more formalized methods to investigate cybercrime.

The proposed analysis method for this hypothesis was multinomial logistic regression analysis. However, multinomial logistic regression was not used because some categories had less than five observations. A Chi-square test also could not be used for the same reason.

Because the assumptions of parametric testing were violated, Spearman's Rank Order Correlation (ρ) was used. The results of the analysis revealed there is a small significant

negative relationship between operating budget and cybercrime investigation method, $\rho = -.20$, $n = 235$, $p = .00$. That is, when the operating budget is higher, less formalized methods of cybercrime investigation are used. Even though a significant relationship was found, the result was in a different direction than expected; it was hypothesized that investigating cybercrimes via more formalized methods would be resource-intensive from a financial standpoint, thus requiring larger operating budgets for police departments undertaking more formalized methods. Based on the results, the null hypothesis was rejected.

Table 9

Nonparametric Correlations for Budget and Cybercrime Investigation Method

			Budget	Cybercrime Investigation Method
Spearman's rho	Budget	Correlation Coefficient	1.00	-.203
		Sig. (2-tailed)		.002
	Cybercrime Investigation Method	N	235	235
		Correlation Coefficient	-.203	1.00
		Sig. (2-tailed)	.002	
		N	235	247

Hypothesis 5 - Operating Budget vs. Required Training Hours

Null Hypothesis 5. There is no significant difference between the campus police department operating budgets and the number of training hours required for sworn officers.

Alternative Hypothesis 5. Campus police department operating budgets will be higher when the number of training hours required for sworn officers is higher.

The proposed analysis method for this hypothesis was linear regression analysis. However, linear regression was not used because the data did not meet the assumptions of

parametric testing. Because the assumptions of parametric testing were violated, Spearman's Rank Order Correlation (ρ) was used instead of Pearson's correlation. The results of the analysis revealed there is a small significant positive relationship between an operating budget and required training hours, $\rho = .23$, $n = 192$, $p = .00$. Specifically, a higher operating budget is associated with more required training hours. It was hypothesized that an association would exist between a department's operating budget and training hours, with a larger budget associated with more stringent requirements for training for sworn officers. Based on the results, the null hypothesis was rejected.

Table 10

Nonparametric Correlations for Required Training Hours and Budget

			Required Training Hours	Budget
Spearman's rho	Required Training Hours	Correlation Coefficient	1.00	.233
		Sig. (2-tailed)		.001
		N	200	192
	Budget	Correlation Coefficient	.233	1.00
Sig. (2-tailed)		.001		
N		192	235	

Summary

Two hundred and forty-seven colleges and universities were included in this study. The proposed data analysis plan was to use logistic regression analysis and simple linear regression analysis. However, after testing the assumptions of parametric testing and exploring the number of observations for each variable, it was determined that the planned analyses could not be used. The appropriate test based on the available options was the nonparametric Spearman's Rank Order Correlation. The correlation analyses revealed that only hypotheses four and five were significant.

Specifically, the analyses showed a small significant negative relationship between operating budget and cybercrime investigation method and a small significant positive relationship between an operating budget and required training hours. Chapter 5 provides an interpretation of these results.

CHAPTER 5: SUMMARY AND CONCLUSIONS

Introduction

Much like small cities, higher education campuses are responsible for overseeing the safety and security of tens of thousands of students, staff, and visitors (Schuh, 1999). In the modern, technological era, campus police's responsibilities include investigating physical and cybercrime (Schuh, 1999; Wada, 2010). Preventing cybercrimes from occurring on campuses and investigating crimes after they occur can be challenging. The officers are required to have a technologically based skill set that is divergent from traditional investigative training (Schuh, 1999).

This study aimed to gather and understand more information about sworn officers' skillsets, educational backgrounds, and demographics and understand what relationship exists between those characteristics and their investigation techniques and capabilities. Understanding the relationship of each demographic variable and the method each campus police agency chooses to investigate cybercrime can assist leadership in decision making.

The study was conducted at Saint Peter's University. The participants were college and university police departments who responded to the U.S. Department of Justice's (USDOJ) Bureau of Justice Statistics (BJS) 2011 Survey of Campus Law Enforcement Agencies. Four hundred and fifty agencies were selected for this study based on their response to the cybercrimes investigation question in the survey. The researcher identified the method each

campus police agency utilized to investigate cybercrime and utilized a causal-comparative design to understand why the method was chosen. “A causal-comparative design is a research design that seeks to find relationships between independent and dependent variables after an action or event has already occurred” (Salkind, 2010). The correlation between demographic characteristics and the resulting response method represents the agency's capacity to investigate cybercrime. Uncovering the specific structures that enhance campus police’s ability to investigate cybercrimes will aid campus police administrators in deploying resources.

This chapter begins by summarizing the study topic, problem, and purpose. Next, a summary of the research findings will be presented, including a review of the research questions. After the findings are summarized, the results will be interpreted and analyzed. Based on the data analysis, future research and practice recommendations are presented. The chapter ends with a conclusion and a review of the major study points.

Summary of Findings

The study included two research questions. The summary of findings section is organized around each of the research questions. Additionally, the researcher collected demographic information about campus police officers and the cybersecurity policies of the campus. In this section, I first analyze findings from the demographic data and then analyze the findings related to each research question.

Demographic Information

A review of the data collection related to demographic information revealed that under 40% of campus police officers had higher education degrees. The average number of training hours was 935, which equates to approximately 116 full workdays of training for the position. Regarding educational requirements for the position, 77% of employers require at least a high

school education to be considered, with the remaining requiring either some college or a two-year degree. This suggests that many individuals employed as campus police officers have more education than is technically required. This could indicate that to be competitive during hiring, having a college degree is helpful, though not required.

Almost 94% of institutions did not have a dedicated cybercrime unit. Only 6% of institutions did have a dedicated cybercrime unit, which suggests that campus police agencies may not have the resources to dedicate a full-time cybercrime unit or that management determined that the existing campus police officers were enough for the institutions' cybersecurity needs. The notion that a lack of resources prevents departments from sustaining dedicated cybercrimes units aligns with findings by Bossler (2020), who suggested a shift in agency priorities toward reducing budgets, management structures, and community engagement contributes to the lack of specialized units. Approximately 55% of institutions stated that police personnel was designated to investigate cybercrimes as necessary, and another 15% of institutions had no policies addressing cybercrime. These statistics suggest that campus police likely do not prioritize cybercrime investigation, though the reason for the lack of prioritization is unknown.

These findings confirm the literature on cybercrime investigation on college campuses. Brown (2015) found that cybercrime often goes unreported, partially due to the impression that campus police would not be able to investigate the crime adequately. This is a reasonable assumption confirmed by the findings that 15% of institutions have no policies regarding cybercrime investigations. With no such policies in place, students who are victims of cybercrimes may be unaware that it is even within the jurisdiction of the campus police to

investigate. In fact, it is unclear if the institutions that have no policies regarding cybercrimes would investigate such crimes if they were brought forward by a student or faculty member.

Research Question One

The first research question asked how the education level of sworn officers impacts the capacity of campus police agencies to conduct cybercrime investigations. The null hypothesis for research question one was that the education level of sworn officers does not affect the capacity of campus police agencies to conduct cybercrime investigations. The researcher hypothesized that the education level of sworn officers impacts their ability to conduct investigations due to the technical nature of cybercrimes and the specialized knowledge of computer systems that research suggests is impactful for cybercrime prevention. For example, Spencer (2020) found that many students do not report cybercrimes to campus police because campus police are not prepared to investigate technologically based crimes. Spencer (2020) found that common campus cybercrimes included non-consensual image sharing and voyeurism. Additionally, Bossler (2020) found that prosecution of cybercrime is not possible without a proper investigation of the crime, and most traditional campus police officers are not prepared to conduct such investigations.

The study results related to research question one indicate no significant relationship between the education level of sworn officers and the presence of a specialized cybercrime unit ($\rho = -.12, n = 211, p = .08$). Similarly, there was no significant relationship between the education level of officers required and the technique used to investigate cybercrimes. The similarity in these results shows a consistency between the hiring practices and the job requirements related to cybercrime investigation.

Based on the results, the null hypothesis was retained. It is possible that these findings were influenced by the minimal number of institutions that had dedicated cybercrime units, though the sampling technique was sufficient to obtain reliable data. If more campus police agencies prioritized cybercrime investigation and developed dedicated cybercrime units, those units may use different recruiting strategies and have separate educational and experiential requirements.

However, if the findings are taken at face value, they contradict the literature on cybercrime investigation on college campuses. Lersch (2001) noted that college experience helps officers be more creative and employ more innovative practices. For investigating complicated crimes such as cybercrime, it makes sense that creativity and innovation would be prioritized in hiring sworn officers. However, the results suggest that campus agencies largely determined that a college degree was unnecessary for the type of policing they prioritized on campus.

Additionally, Bossler (2020) noted that many police officers feel unprepared to investigate cybercrimes due to a lack of knowledge. This finding implies that if institutions were to develop cybercrime investigation units, it would be logical for them to hire individuals who did have the training to feel that they could be successful in investigations. Echoing this sentiment, Barro (1999) stated that a lack of higher education among sworn officers in a supervisory or leadership capacity was problematic, especially for individuals in specialized units such as the cybercrime unit. Finally, Davis (2012) noted that specialized units, including cybercrime units, are only successful if management and officers have a subject matter understanding of how the crimes are committed and how they can be successfully investigated and prevented.

Research Question Two

The second research question asked how the demographic makeup of a campus police department impacts the agency's choice of method to investigate cybercrime. In terms of demographic makeup, research question 2 included the number of hours of training required and the department's operating budget. The results of the analysis revealed no relationship between the hours of training required for sworn officers and the method of investigating cybercrimes (i.e., if the campus police agency had a dedicated cybercrime unit or if sworn officers from the regular unit investigated cybercrimes).

Based on the literature, the researcher hypothesized that officers included in dedicated cybercrime units might be required to have more training than officers who were included in the traditional investigation units. Cybercrime units are "designed to provide support to frontline officers to recover and make use of (potentially overlooked) digital evidence and to assist local police with digital investigations" (Schreuders, 2020, p. 321). This description clarifies that the demands on a cybercrimes unit officer are more technology-driven than those of a traditional investigative officer. As previously mentioned, Bossler (2020) argued that frontline investigation officers often feel unprepared to handle specialized investigations due to a lack of training and knowledge. This suggests that individuals in specialized units should receive additional training to succeed. Schreuders (2020) indicated that specialized units need more advanced training and refresher training provided in a self-directed format. Still, the results of this study indicate that individuals who are in specialized units did not receive additional training compared to individuals in the regular units. Leukfeld et al. (2013) argued that general law enforcement officers were not capable of responding to calls involving cybercrimes, which presents a disconnect between the study findings and literature.

However, the results did reveal a small significant negative relationship between the operating budget and the cybercrime investigation method ($\rho = -.20, n = 235, p = .00$). This result suggests that when the operating budget is higher, less formalized methods of cybercrime investigation are used. This finding contradicts the literature, implying that specialized units are the preferred manner for dealing with cybercrimes. It logically follows that those institutions with more resources would be more likely to use that funding to pursue the most effective techniques. One possible explanation for the deviation in literature and study results is that institutions with more significant operating budgets hire officers who are generally able to handle both cybercrimes and other types of crimes. Still, this conclusion is unlikely based on a lack of policy regarding cybercrime investigation and the educational requirements of most institutions.

Another explanation for the deviation between the literature and the study findings is that campus police agencies with larger operating budgets may consider outsourcing their cybercrime investigation practices to external partnerships. Cherney (2008) argued that traditional police forces are not trained to conduct cybercrime investigations; therefore, it is better to collaborate with agencies specializing in cybercrime investigation when necessary. The research suggests management of campus police agencies are those with prior careers in law enforcement outside of the institution. Bossler and Holt (2020) found that older officers, often found in leadership positions in campus police departments, are more likely to develop partnerships with state and federal law enforcement agencies to outsource investigations of cybercrimes rather than investigate them locally. This observation supports the finding that campus police agencies with significant financial resources would seek partnerships rather than develop specialized units to address cybercrime. If campus police agencies were outsourcing their cybercrime investigation

to outside agencies, it would be logical for sworn officers to serve generalized functions rather than having a dedicated cybercrime unit. To understand if this is a possible cause for the deviation, it would be necessary to conduct additional data collection to confirm that campus police agencies are not relying on outside partnerships in ways not revealed in the initial data collection.

The final data collection piece revolved around the connection between an operating budget and employee training requirements. The data collection revealed that institutions with more significant operating budgets for sworn officers conducted more training for employees ($\rho = .23, n = 192, p = .00$). Unlike the other findings, this finding confirms and extends the literature on preparation for sworn officers employed by educational institutions. Bossler (2020) stated that officers feel unprepared to address specialized crimes due to a lack of resources. The study results suggest that when institutions have resources to spend on sworn officers, they direct those resources towards addressing training issues. Similarly, Paoline (2003) stated that specialized units were influenced by the resources available, which coincides with the study findings.

Recommendations

This section includes information on study recommendations for future research and recommendations for practice. Regarding the recommendations for future research, it is essential first to understand how successful educational institutions are at addressing cybercrime. The literature suggested that cybercrime was a campus problem and needed to be addressed (Brown, 2015). The data analysis revealed that educational institutions did not require higher education from their job applicants. They did not have specialized cybercrime units. They were less likely to develop dedicated cybercrimes units when their budget increased .

The literature review suggested that these conditions may result in educational institutions being unsuccessful in investigating cybercrimes and unprepared to deal with cybercrimes generally. If the campus police agencies considered in this study successfully investigated cybercrimes, then the disconnection between literature and the study results would suggest a need to reconsider academic understanding of cybercrime investigation. However, if the campus police were largely unprepared and unsuccessful in their investigations, the expectations of literature would largely be confirmed.

Secondly, future research could determine to what extent campus police agencies rely on external partnerships for cybercrime investigation. The study results suggested that, as operating budgets increased, campus police were more likely to rely on informal cybercrime investigation methods and were less likely to have dedicated cybercrime units. Literature on cybercrime suggests that reliance on partnerships is one possible way of handling a lack of internal expertise (Cherney, 2008). Institutions with larger police budget allocations may have elected to form external partnerships rather than creating their own units. However, there is insufficient information in the present data to confirm this.

Assuming sworn officers employed by educational institutions are responsible for investigating cybercrimes, it would be helpful to know to what degree those individuals felt prepared to investigate cybercrimes and other specialized duties. The literature suggests that sworn officers without higher education or technical training would likely struggle to undertake such responsibilities (Perez & Bromley, 2015). However, there is a disconnection between the literature on cybercrime investigation and the actions of academic institutions. If the educational institutions do not change the educational requirements or training of officers or do not have specialized units, the employed individuals either must be successful, or the institution must not

have the budgets to make meaningful changes. A third option is that institutions do not prioritize cybercrime investigations and do not think it is a serious concern. Further research should clarify which of these conditions apply or if there is another explanation.

Regarding practice recommendations, (a) it is recommended that institutions implement policies regarding cybercrime investigation, even if they do not have units dedicated to the investigation of cybercrimes. By (a) clarifying the expectations around cybercrime investigation, students and faculty will at least understand if they should report cybercrimes to the institution's police force. Brown (2015) noted that many cybercrimes go unreported because individuals do not think sworn officers are prepared to investigate. The study results show that 15% of institutions did not have a policy on cybercrime investigation, which is likely to confuse campus constituents on whether their reports will be investigated.

The collective findings of the literature suggest that it would be beneficial for institutions to have dedicated police forces for cybercrime investigation and that the individuals employed by such parties receive appropriate education and training for their job responsibilities. This would imply a (c) recommendation for dedicated cybercrimes units, including officers with higher educational degrees and specialized training. According to the data collection, these conditions do not currently exist universally at academic institutions. However, before recommending that educational institutions have dedicated cybercrimes units with highly trained individuals, it is essential to address some of the research recommendations addressed in this section. Specifically, before recommending changes to the makeup of police forces, further research should confirm that educational institutions are not successful at investigating cybercrime using their generalized police forces without higher education requirements.

It would be ideal to analyze newer SCLEA data, from 2021, compared to the 2012 data. It is expected that, as society becomes more reliant on technology and more vulnerable due to that reliance, cybercrime also becomes more prevalent. The researcher expects police departments to be responsive to this shift, and it would be essential to examine the evolution of cybercrime investigation during the 10 years between 2012 and 2021.

In the same way that responsiveness to cybercrime might compel police departments to develop cybercrime investigation capabilities, it is also logical to think that police departments will develop increasingly formalized and increasingly knowledge- and skill-intensive methods of investigating cybercrime, resulting in greater professionalization in this area. Repeating this study but with more recent data would enable an understanding of this evolution.

Conclusion

This study aimed to gather more information about the skillset, educational background, and demographics of sworn officers and understand what relationship, if any, exists between those characteristics and investigation techniques and capabilities. The first research question asked how the education level of sworn officers impacts the capacity of campus police agencies to conduct cybercrime investigations. The data results contradicted the literature by implying that there was no significant relationship between the educational level or requirements of sworn officers and the presence of a dedicated cybercrime unit. The second research question asked how the demographic makeup of a campus police department impacts the agency's choice of method to investigate cybercrime. The study results show no relationship between the hours of training required and a specialized cybercrime unit but found a negative relationship between institutional funding level and the formality of cybercrime investigations. These results contradict the literature, suggesting that specialized units would require more training and that

institutions with higher budgets would likely employ dedicated cybercrime units. Finally, the data results indicated a positive relationship between funding levels and required training, largely confirming the literature.

The analysis yielded a recommendation that future research establish whether campus police are successful in investigating cybercrimes given their lack of specialized units and lower educational requirements for officers. If campus police are successful, then the literature on the subject will largely be refuted. If they are not successful, the conditions which the literature suggests would be unfavorable would be explained and confirmed. Finally, it is recommended that educational institutions that do not have policies on cybercrimes develop them to prevent under-reporting and confusion among individuals impacted by cybercrimes.

REFERENCES

- Allen, A. (2016). Stop and question campus policing. *Policing*, 39(3), 507-520. <http://dx.doi.org/10.1108/PIJPSM-04-2016-0054>
- Allen, A. N. (2015). Campus police-citizen encounters: Influences on sanctioning outcomes. *American Journal of Criminal Justice: AJCJ*, 40(4), 722-736. <http://dx.doi.org/10.1007/s12103-014-9282-2>
- Baro, A. L., & Burlingame, D. (1999). Law enforcement and higher education: Is there an impasse? *JCJE: Journal of Criminal Justice Education*, 10(1), 57-73.
- Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2020). Policing fraud in England and wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*, 33(2), 311-328. <http://dx.doi.org/10.1057/s41284-019-00187-5>
- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing*, 29(3), 408-433. <http://dx.doi.org/10.1108/13639510610684674>
- Bromley, M. L. (2003). Comparing campus and municipal police community policing practices. *Journal of Security Administration*, 26(2), 37-50,75.
- Bromley, M. L., & Reaves, B. A. (1998). Comparing campus and municipal police: The human resource dimension. *Policing*, 21(3), 534. <http://dx.doi.org/10.1108/13639519810228813>
- Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55-119.
- Brunson, R. K., & Pegram, K. (2018). "Kids do not so much make trouble, they are trouble": Police-youth relations. *The Future of Children*, 28(1), 83-102.

- Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing*, 43(1), 105-119. <http://dx.doi.org/10.1108/PIJPSM-08-2019-0142>
- Burruss, G., Christian, J. H., Bossler, A., & Holt, T. J. (2020). Self-perceptions of English and Welsh constables and sergeants' preparedness for online crime: A latent class analysis. *Policing*, 43(1), 105-119. <http://dx.doi.org/10.1108/PIJPSM-08-2019-0142>
- Charles, S. (2020, February 24). "Unwilling to just wait": Alabama State sit-in brought change, cost protesting students dearly. *Montgomery Advisor*. <https://www.montgomeryadvertiser.com/story/news/2020/02/21/alabama-state-sit-in-brought-change-but-cost-students-dearly/4793116002/>
- Bell, R. E. (2002). The prosecution of computer crime. *Journal of Financial Crime*, 9(4), 308-325. <http://dx.doi.org/10.1108/eb026030>
- Cherney, A. (2008). Harnessing the crime control capacities of third parties. *Policing*, 31(4), 631-647. <http://dx.doi.org/10.1108/13639510810910607>
- Dache-Gerbino, A., & White, J. A. (2016). College students or criminals? A postcolonial geographic analysis of the social field of whiteness at an urban community college branch campus and suburban main campus. *Community College Review*, 44(1), 49-69. <http://dx.doi.org/10.1177/0091552115616677>
- Dameron, S. L., Detardo-bora, K. A., & Bora, D. J. (2009). An assessment of campus security and police information on college/university websites. *Security Journal*, 22(4), 251-268. <http://dx.doi.org/10.1057/palgrave.sj.8350082>

- Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing*, 35(2), 272-284. <http://dx.doi.org/10.1108/13639511211230039>
- Davis, E. (2012). Bureau of Justice Statistics Home page. <https://www.bjs.gov/index.cfm?ty=dcdetail>
- Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing*, 35(2), 272-284. <http://dx.doi.org/10.1108/13639511211230039>
- Da-Yu, K., & Wang, S. (2009). The IP address and time in cyber-crime investigation. *Policing*, 32(2), 194-208.
- D'ovidio, R. (2007). The evolution of computers and crime: Complicating security practice. *Security Journal*, 20(1), 45-49. <http://dx.doi.org/10.1057/palgrave.sj.8350045>
- Farnworth, M., Longmire, D. R., & West, V. M. (1998). College students' views on criminal justice*: Jcje. *Journal of Criminal Justice Education*, 9(1), 39-180.
- Goodman-Delahunty, J., Verbrugge, H., Sowemimo-Coker, C., Kingsford, J., & Taitz, M. (2013). Procedural justice violations in police-citizen interactions: Insights from complaints about police. *Journal of the Institute of Justice and International Studies*, 13, F1-XIII.
- Gross, J. P. (2016). Judge, jury, and executioner: The excessive use of deadly force by police officers. *Texas Journal on Civil Liberties & Civil Rights*, 21(2), 155-181.
- Hawdon, J., Part, K., & Dearden, T. (2020). Cybercrime in America amid covid-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, 45, 546-562. <https://doi.org/10.1007/s12103-020-09534-4>

- Halder, D. (2013). Book review of policing cyber hate, cyber threats and cyber terrorism. *International Journal of Cyber Criminology*, 7(2), 169-170.
- Hauser, W., & Kleck, G. (2017). The impact of police strength and arrest productivity on fear of crime and subjective assessments of the police. *American Journal of Criminal Justice: AJCJ*, 42(1), 86-111. <http://dx.doi.org/10.1007/s12103-016-9334-x>
- Holt, T. J., & Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice: AJCJ*, 37(3), 396-412. <http://dx.doi.org/10.1007/s12103-011-9131-5>
- Hummer, D., Austin, T. L., & Bumphus, V. W. (1998). Arming the campus cops: A descriptive and multivariate assessment of support. *Policing*, 21(2), 255. <http://dx.doi.org/10.1108/13639519810220208>
- Jahnig, L. J. (2016). Under school colors: Private university police as state actors under § 1983. *Northwestern University Law Review*, 110(1), 249-282.
- Janosik, S. M., & Plummer, E. (2005). The Clery Act, campus safety, and the views of assault victim advocates. *College Student Affairs Journal*, 25(1), 116-130.
- Kim Michelle Lersch, & Kunzman, L. L. (2001). Misconduct allegations and higher education in a southern sheriff's department. *American Journal of Criminal Justice: AJCJ*, 25(2), 161-172.
- Kimberly, B. K., McMahon, J. M., & Stewart, G. (2018). Misinterpreting danger? stereotype threat, pre-attack indicators, and police-citizen interactions. *Journal of Police and Criminal Psychology*, 33(1), 45-54. <http://dx.doi.org/10.1007/s11896-017-9233-1>
- Law.com. (2020). <https://dictionary.law.com/Default.aspx?selected=964>

- Lai, Y. (2016). College students' satisfaction with police services in Taiwan. *Asian Journal of Criminology*, 11(3), 207-229. <http://dx.doi.org/10.1007/s11417-015-9227-9>
- Lyle, P., & Esmail, A. M. (2016). Sworn to protect: Police brutality - A dilemma for America's police. *Race, Gender & Class*, 23(3/4), 155-185.
- Neil, B. A. (2009). Should armed guards be allowed in schools in light of the recent right-to-carry laws? *Contemporary Issues in Education Research*, 2(4), 41-45.
- Nordberg, A., Crawford, M. R., Praetorius, R. T., & Hatcher, S. S. (2016). Exploring minority youths' police encounters: A qualitative interpretive meta-synthesis: C & A. *Child & Adolescent Social Work Journal*, 33(2), 137-149. <http://dx.doi.org/10.1007/s10560-015-0415-3>
- O'Reilly, C. (2009). Crafting transnational policing: Police capacity building and global. *Law & Society Review*, 43(1), 229-231.
- Pallant, J. (2016). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS* (6th ed.). McGraw-Hill Education.
- Paoline, E. A., III, & Sloan, J. J., III. (2003). Variability in the organizational structure of contemporary campus law enforcement agencies: A national-level analysis. *Policing*, 26(4), 612-639. <http://dx.doi.org/10.1108/13639510310503541>
- Parker, W. M., Puig, A., Johnson, J., & Anthony, C., Jr. (2016). Black males on white campuses: Still invisible men? *College Student Affairs Journal*, 34(3), 76-92.
- Patten, R., Alward, L., Thomas, M., & Wada, J. (2016). The continued marginalization of campus police. *Policing*, 39(3), 566-583. <http://dx.doi.org/10.1108/PIJPSM-04-2016-0055>

- Pelfrey Jr, W. V., & Keener, S. (2016). Police body worn cameras: A mixed-method approach assessing perceptions of efficacy. *Policing*, 39(3), 491-506. <http://dx.doi.org/10.1108/PIJPSM-02-2016-0019>
- Perez, N. M., & Bromley, M. (2015). Comparing campus and city police human resource and select community outreach policies and practices. *Policing*, 38(4), 664-674. <http://dx.doi.org/10.1108/PIJPSM-07-2015-0084>
- Radda, S. I., & Ndubueze, P. N. (2013). Fear of online victimization among undergraduate students: A comparative study of two selected urban universities. *African Journal of Criminology and Justice Studies: AJCJS*, 7(1/2), 35-46.
- Reaves, B. A. (2015). Campus Law Enforcement, 2011–12 (pp. 1-27). United States, U.S. Department of Justice, Office of Justice Programs: Bureau of Justice Statistics.
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *The Journal of Research in Crime and Delinquency*, 50(2), 216. <http://dx.doi.org/10.1177/0022427811425539>
- Roberg, R., & Bonn, S. (2004). Higher education and policing: Where are we now? *Policing*, 27(4), 469-486. <http://dx.doi.org/10.1108/13639510410566226>
- Salkind, N. J. (2010). *Encyclopedia of research design* (Vols. 1-0). SAGE Publications. <https://doi.org/10.4135/9781412961288>
- Schreuders, C. Z., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A. R., & Shan-A-Khuda, M. (2020). Needs assessment of cybercrime and digital evidence in a UK police force. *International Journal of Cyber Criminology*, 14(1), 316-340.
- Schuh, J. H. (1999). Duty to warn and foresee danger created by nonstudents: Challenges for colleges and universities. *Journal of College Student Development*, 40(2), 178.

- Selby, N. (2021, October 6). Perspective | local police don't go after most cybercriminals. we need better training. *The Washington Post*. <https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/>
- Spencer, D. C., Ricciardelli, R., Ballucci, D., & Walby, K. (2019). Cynicism, dirty work, and policing sex crimes. *Policing*, 43(1), 151-165. <http://dx.doi.org/10.1108/PIJPSM-07-2019-0123>
- Sussmann, M.A. (1999), The critical challenges from international high-tech and computer-related crime at the millennium. *Duke J. of Comp. & Int'l L.*, 9, 451.
- Thompson, A., Price, J. H., Mrdjenovich, A J., & Khubchandani, J. (2009). Reducing firearm-related violence on college campuses-police chiefs' perceptions and practices. *Journal of American College Health*, 58(3), 247-254. <http://dx.doi.org/10.1080/07448480903295367>
- Thompson, A., Price, J. H., Dake, J., & Teeple, K. (2013). Faculty perceptions and practices regarding carrying concealed handguns on university campuses. *Journal of Community Health*, 38(2), 366-73. <http://dx.doi.org/10.1007/s10900-012-9626-0>
- Wada, J. C., Patten, R., & Candela, K. (2010). Betwixt and between: The perceived legitimacy of campus police. *Policing*, 33(1), 114-131. <http://dx.doi.org/10.1108/13639511011020629>
- Weitzer, R., & Tuch, S. A. (2005). Racially biased policing: Determinants of citizen perceptions*. *Social Forces*, 83(3), 1009-1030. <http://dx.doi.org/10.1353/sof.2005.0050>
- Wilson, C. P., & Wilson, S. A. (2015). Evaluating legitimacy and marginalization: Campus policing in the state of Rhode Island. *Cogent Social Sciences*, 1(1), n/a. <http://dx.doi.org/10.1080/23311886.2015.1006091>

Williams, K. (2008). Using Tittle's control balance theory to understand computer crime and deviance. *International Review of Law Computers & Technology*, 22(1-2), 145-55.

Wood, J., & Shearing, C. (1998). Securing safety on campus: A case study. *Canadian Journal of Criminology*, 40(1), 81-95.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, 8(1), 36-46.

APPENDIX A: SURVEY INSTRUMENT

2011 Survey of Campus Law Enforcement Agencies

U.S. Department of Justice
Bureau of Justice Statistics

BURDEN STATEMENT

Federal agencies may not conduct or sponsor an information collection, and a person is not required to respond to a collection of information, unless it displays a currently valid OMB Control Number. Public reporting burden for this collection of information is estimated to average 2 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate, or any other aspects of this collection of information, including suggestions for reducing this burden, to the Director, Bureau of Justice Statistics, 810 Seventh Street, NW, Washington, DC 20531. The Omnibus Crime Control and Safe Streets Act of 1968, as amended (42 USC 3732), authorizes this information collection. Although this survey is voluntary, we urgently need your cooperation to make the results comprehensive, accurate, and timely. We greatly appreciate your assistance.

INSTITUTION INFORMATION

1. For which college/university campus(es) are you reporting?

If we have follow-up questions, we might need to contact you. Your name and contact information will be kept strictly confidential. In addition, if you provide your e-mail address, we can e-mail you a notification when the survey results are available for download from the BJS web site (www.bjs.gov).

2. Please provide your contact information below:

a. Name:

b. Position/ Title:

c. Telephone number:

d. Fax number:

e. E-mail address:

Please return survey to: MAIL: Alisha Creel
ICF International
9300 Lee Highway
Fairfax VA 22031

FAX: 1-855-254-5882

For help with this survey: EMAIL: CampusLaw2011@icfi.com

PHONE: 1-866-255-1282

AGENCY INFORMATION

3. Who employs the officers that provide the **routine law enforcement services such as patrol or responding to calls for service** on campus?

Please select ALL that apply.

- Campus police/security agency
- Municipal/county police agency
- Sheriff's office/department
- State law enforcement agency (non-campus)
- Private security firm
- Other – please specify: _____
- None of these

4. Who employs the officers that provide the **security for special events** on campus? Please select ALL that apply.

- Campus police/security agency
- Municipal/county police agency
- Sheriff's office/department
- State law enforcement agency (non-campus)
- Private security firm
- Other – please specify: _____
- None of these

NOTE: If your college/university does NOT have a campus police/security agency, please stop here and return this questionnaire in the envelope provided. If your college/university does have a campus police/security agency, please continue with Question 5.

PERSONNEL INFORMATION

5. How many PAID employees were employed in your campus police/security agency as of September 30, 2011? A **full-time** employee is defined as working 35 or more hours per week. A **part-time** employee is one who works less than 35 hours per week, excluding those who work just for special events.

	# Full Time	# Part Time
a. Sworn police officers (full arrest powers)		
b. Nonsworn security officers (limited or no arrest authority)		
c. Civilian personnel (non-student)		
d. Student employees (non-officers)		

NOTE: The total number of full-time SWORN officers for both question 6 and question 7 MUST equal the total number of full-time SWORN officers given in question 5 above.

6. As of September 30, 2011, how many FULL-TIME SWORN agency personnel were in each racial/ethnic category?

Mark here if not applicable -- no full-time SWORN officers. Go to Question 8.

	# of Sworn Officers (Full-time)
a. White, non-Hispanic	
b. Black or African American, non-Hispanic	
c. Hispanic or Latino, any race	
d. American Indian or Alaska Native	
e. Asian, Native Hawaiian, or Pacific Islander	
f. Two or more races	
g. Don't know/No information available	

7. As of September 30, 2011, how many FULL-TIME SWORN agency personnel were in each gender category?

Mark here if not applicable -- no full-time SWORN officers. Go to Question 8.

	# of Sworn Officers (Full-time)
a. Female	
b. Male	

8. As of September 30, 2011, how many FULL-TIME officers in your agency were in the military Reserves, National Guard, or other organization which may require a call to service?

	# Officers (Full-time)	Not applicable
a. Sworn police officers		<input type="radio"/>
b. Nonsworn security officers		<input type="radio"/>

9. For the following years, how many of your FULL-TIME officers were called to service for military assignments, thus leaving their current position with your agency on a temporary basis?

Calendar Year	# of full-time sworn police officers called to service	# of full-time non-sworn security officers called to service
a. 2011		
b. 2010		
c. 2009		
Not Applicable	<input type="radio"/>	<input type="radio"/>

PERSONNEL DUTIES AND FUNCTIONS

10. As of September 30, 2011, how many FULL-TIME sworn police officers and nonsworn security officers in your agency had REGULARLY ASSIGNED DUTIES that included responding to citizen calls/requests for service? For each type of officer, how many were uniformed and how many were non-uniformed officers? *If your agency had none, please enter '0'.*

	# Uniformed	# Non-uniformed	Not applicable
a. Full-time responding sworn police officers			<input type="radio"/>
b. Full-time responding nonsworn security officers			<input type="radio"/>

11. Does your agency perform the following **security functions** on a regular basis? *Please select ONE response per row.*

	Not responsible for this	Perform this on occasion	Perform this regularly
a. Access control (including electronic access)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Building lockup/unlock	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Central alarm monitoring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Key control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Monitoring surveillance cameras	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Executive protection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

12. Does your agency provide **on-site security** for the following on a regular basis? *Please select ONE response per row.*

	Not responsible for this	Perform this on occasion	Perform this regularly
a. Arena events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Auditorium events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Library or cultural facilities (e.g., museums)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Daycare facilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Educational (K-12) facilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Medical facilities (e.g., hospital, clinic)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g. Nuclear/Radioactive materials	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
h. Hazardous biological/chemical materials	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
i. Stadium events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

13. Does your agency perform the following **specialized functions** on a regular basis? *Please select ONE response per row.*

	Not responsible for this	Perform this on occasion	Perform this regularly
a. Bomb/Explosive disposal or detection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Search and rescue	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Tactical operations (SWAT)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Task force participation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Underwater recovery	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

14. Does your agency perform the following **vehicle-related functions** on a regular basis? *Please select ONE response per row.*

	Not responsible for this	Perform this on occasion	Perform this regularly
a. Parking administration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Parking enforcement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Traffic accident investigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Traffic direction and control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Traffic law enforcement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Transportation system management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g. Vehicle registration for on-campus use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15. Does your agency perform the following **public safety functions** on a regular basis? *Please select ONE response per row.*

	Not responsible for this	Perform this on occasion	Perform this regularly
a. Animal control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Dispatching calls for service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Emergency fire services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Emergency medical services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Environmental health/safety	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Fire inspection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g. Fire prevention education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
h. Emergency management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

16. Does your agency operate the following types of facilities? *Please select ONE response per row.*

	Yes	No
a. Temporary lock-up facility (overnight)	<input type="radio"/>	<input type="radio"/>
b. Temporary holding cell (not for overnight)	<input type="radio"/>	<input type="radio"/>

PERSONNEL DUTIES AND FUNCTIONS (cont'd)

17. How often does your agency have the following **uniformed** officers on duty (regardless if full time or part time)? *Please select ONE response per row.*

Not applicable
Not used at any time
Some of the time
At all times

- a. Sworn police who are uniformed
- b. Nonsworn security who are uniformed .

18. What level of routine patrol coverage with uniformed **sworn** police officers (full and part time) does your agency provide for the following periods? *Please select ONE response per row.*

Mark here if not applicable -- no SWORN officers. Go to Question 19.

No routine patrols
Less than 24-hour patrol coverage
24-hour patrol coverage

- a. Weekdays during academic terms
- b. Weekends during academic terms
- c. Breaks between academic terms
- d. Summer term

19. What level of routine patrol coverage with uniformed **nonsworn** security officers (full and part time) does your agency provide for the following periods? *Please select ONE response per row.*

Mark here if not applicable -- no NONSWORN officers. Go to Question 20.

No routine patrols
Less than 24-hour patrol coverage
24-hour patrol coverage

- a. Weekdays during academic terms
- b. Weekends during academic terms
- c. Breaks between academic terms
- d. Summer term

20. How many larceny-theft incidents were reported to your agency for the following years? *For this item, use the FBI's Uniform Crime Reporting (UCR) Program definition, which defines larceny-theft as the unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another. Examples are thefts of bicycles, motor vehicle parts and accessories, shoplifting, pocket-picking, or the stealing of any property or article that is not taken by force and violence or by fraud. Attempted larcenies are included. Such crimes as embezzlement, confidence games, forgery, check fraud, etc. are excluded.*

	Calendar Year		
	2011	2010	2009
Total larceny-theft events reported to your agency			
a. Of the total, how many occurred in on-campus residence halls/housing?			
b. Of the total, how many occurred elsewhere on campus, other than in on-campus residence halls/housing?			
c. Of the total, how many occurred in non-campus facilities?			
d. Of the total, how many occurred on public property?			
e. No information available for this year.			

ADMINISTRATION

21. What was your agency's **total police and security services operating budget** for the fiscal or calendar year that includes September 30, 2011? *Do not include building construction costs or major equipment costs.*

\$.00

21a. Is the above budget an estimate?

- Yes No

21b. Of the total operating budget amount listed above, how much is allocated to overtime costs? If none, enter 0.

\$.00

ADMINISTRATION (cont'd)

22. Does your agency receive income from any of the following sources that is not contained in the budget?
Please select ONE response per row.

	Yes	No
a. Providing security at athletic special events	<input type="radio"/>	<input type="radio"/>
b. Providing security at non-athletic special events	<input type="radio"/>	<input type="radio"/>
c. Parking tickets/Traffic citations	<input type="radio"/>	<input type="radio"/>
d. Parking permits	<input type="radio"/>	<input type="radio"/>
e. Guest parking	<input type="radio"/>	<input type="radio"/>
f. Other (specify below):	<input type="radio"/>	<input type="radio"/>

23. Do officers in your agency (any officers - full time, part time, sworn, nonsworn) receive extra duty pay directly from an entity outside the agency when working a special event? Yes No

24. As of September 30, 2011, what was the minimum and maximum annual base salary for the following full-time positions? If you have only one value for a particular position, please enter it as a 'Minimum'. For any salaries paid at an hourly rate, please multiply the hourly rate by 2,088 to get the annual salary.

Full-time Position	Minimum Annual Salary (in dollars)	Maximum Annual Salary (in dollars)	Not Applicable - No Such Position	Don't Know At All
a. Chief/Director			<input type="radio"/>	<input type="radio"/>
b. Shift Supervisor			<input type="radio"/>	<input type="radio"/>
c. Entry-level sworn police officer			<input type="radio"/>	<input type="radio"/>
d. Entry-level nonsworn security officer			<input type="radio"/>	<input type="radio"/>
e. Sworn police officer with 5 years of experience			<input type="radio"/>	<input type="radio"/>
f. Nonsworn security officer with 5 years of experience			<input type="radio"/>	<input type="radio"/>
g. Dispatch operator (as an annual salary if hourly rate)			<input type="radio"/>	<input type="radio"/>

25. Does your agency offer any of the following forms of special pay or benefits to FULL-TIME **sworn** police officers? Please select ONE response per row.

Mark here if not applicable -- no full-time SWORN officers. Go to Question 26.

	Yes	No
a. Training officer pay	<input type="radio"/>	<input type="radio"/>
b. Educational incentive pay	<input type="radio"/>	<input type="radio"/>
c. Tuition waiver/reimbursement/discount	<input type="radio"/>	<input type="radio"/>
d. Health incentive (e.g., for maintaining a specific weight range)	<input type="radio"/>	<input type="radio"/>
e. Merit/Performance pay	<input type="radio"/>	<input type="radio"/>
f. Overtime pay/Comp time	<input type="radio"/>	<input type="radio"/>
g. Shift differential pay	<input type="radio"/>	<input type="radio"/>
h. Longevity pay*	<input type="radio"/>	<input type="radio"/>

* 25a. If longevity pay is offered, how many years of service are required for sworn police officers?

 years of service

26. Does your agency offer any of the following forms of special pay or benefits to FULL-TIME **nonsworn** security officers? Please select ONE response per row.

Mark here if not applicable -- no full-time NONSWORN officers. Go to Question 27.

	Yes	No
a. Training officer pay	<input type="radio"/>	<input type="radio"/>
b. Educational incentive pay	<input type="radio"/>	<input type="radio"/>
c. Tuition waiver/reimbursement/discount	<input type="radio"/>	<input type="radio"/>
d. Health incentive (e.g., maintaining a specific weight range)	<input type="radio"/>	<input type="radio"/>
e. Merit/Performance pay	<input type="radio"/>	<input type="radio"/>
f. Overtime pay/Comp time	<input type="radio"/>	<input type="radio"/>
g. Shift differential pay	<input type="radio"/>	<input type="radio"/>
h. Longevity pay*	<input type="radio"/>	<input type="radio"/>

* 26a. If longevity pay is offered, how many years of service are required for nonsworn security officers?

 years of service

27. Does your agency require a written agreement to serve a minimum number of years for FULL-TIME officers in order to join the force? *Please select ONE response per row.*

	Not Applicable	
	No	
	Yes	
a. Service agreement for sworn police officers	<input type="radio"/>	<input type="radio"/>
b. Service agreement for nonsworn security officers	<input type="radio"/>	<input type="radio"/>

If 'Yes', how many years of service are required?

	# Years of Service Required
a. Sworn police officers	
b. Nonsworn security officers	

28. Is **collective bargaining authorized** for non-supervisory FULL-TIME personnel by your agency? *Please select ONE response per row.*

	Not applicable	
	For none	
	For some	
	For all	
a. Full-time sworn police officers	<input type="radio"/>	<input type="radio"/>
b. Full-time nonsworn security officers	<input type="radio"/>	<input type="radio"/>

TECHNOLOGY AND COMMUNICATION

29. Does your campus have a **"blue-light" [or equivalent] emergency phone system**?
 Yes No

30. Does your agency participate in an **emergency telephone system** with any of the following features? *Please select ONE response per row.*

	Yes	No
a. Enhanced 9-1-1 system (providing both caller location and identification when available)	<input type="radio"/>	<input type="radio"/>
b. Basic 9-1-1 system	<input type="radio"/>	<input type="radio"/>
c. On-campus 3- or 4-digit emergency number (other than 9-1-1)	<input type="radio"/>	<input type="radio"/>
d. "Phone patch" call forwarding when dispatch is not available	<input type="radio"/>	<input type="radio"/>
e. Reverse 9-1-1 call back available	<input type="radio"/>	<input type="radio"/>
f. Recorded calls are available for immediate playback	<input type="radio"/>	<input type="radio"/>
g. Other (specify below):	<input type="radio"/>	<input type="radio"/>

31. Does your agency have an emergency telephone system with the following capabilities for incoming calls from **wireless/cellular phones**? *Please select ONE response per row.*

	Yes	No
a. Displays phone number of wireless caller.	<input type="radio"/>	<input type="radio"/>
b. Displays general location of wireless caller.	<input type="radio"/>	<input type="radio"/>
c. Displays exact location of wireless caller.	<input type="radio"/>	<input type="radio"/>

32. Does your agency use 800 MHz radios? Yes No

33. Does your agency utilize the following for **dispatch**? *Please select ONE response per row.*

	Yes	No
a. Mobile data dispatch	<input type="radio"/>	<input type="radio"/>
b. Over-air commands via non-800 MHz radio	<input type="radio"/>	<input type="radio"/>
c. Over-air commands via 800 MHz radio	<input type="radio"/>	<input type="radio"/>
d. Over-air commands via "push to talk" (PTT)	<input type="radio"/>	<input type="radio"/>
e. Other (specify below):	<input type="radio"/>	<input type="radio"/>

34. Is the campus public safety radio system **interoperable** with the local police, fire, and other first responders?
 Yes, fully Yes, partially Not at all

35. Effective Jan. 1, 2013, all public safety radio systems will be required to be compliant with the FCC mandate concerning narrowband broadcasts. Is your campus public safety radio system **compliant** with the FCC narrowband mandate?
 Yes, fully Yes, partially Not at all

36. Does your campus use the following in conjunction with its **mass notification systems**? *Please select ONE response per row.*

	Yes	No
a. Cell phone calling	<input type="radio"/>	<input type="radio"/>
b. Siren	<input type="radio"/>	<input type="radio"/>
c. Outdoor public-address speakers	<input type="radio"/>	<input type="radio"/>
d. Radio announcements	<input type="radio"/>	<input type="radio"/>
e. Text message alerts	<input type="radio"/>	<input type="radio"/>
f. E-mail alerts	<input type="radio"/>	<input type="radio"/>
g. Voicemail alerts	<input type="radio"/>	<input type="radio"/>
h. TV announcements	<input type="radio"/>	<input type="radio"/>
i. CCTV monitor announcements	<input type="radio"/>	<input type="radio"/>
j. LCD billboard announcements	<input type="radio"/>	<input type="radio"/>
k. College/University website	<input type="radio"/>	<input type="radio"/>
l. Voice-over fire alarms	<input type="radio"/>	<input type="radio"/>
m. Other (specify below):	<input type="radio"/>	<input type="radio"/>

TECHNOLOGY AND COMMUNICATION (cont'd)

37. How does the **mass notification system** on your campus **enroll** the following types of people? *Please select ONE response per row.*

	Not available	Other system	Mandatory, opt-out	Voluntary, opt-in
a. First-year students	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. On-campus students	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Off-campus students	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Faculty/Administration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

OFFICER SELECTION AND TRAINING REQUIREMENTS

38. What is the **PREFERRED** minimum educational level and **REQUIRED** minimum educational level used in vacancy announcements for **FULL-TIME** entry-level **sworn** officers? *Please select ONE response per row.*

Mark here if not applicable -- no full-time SWORN officers. Go to Question 39.

	None stated	Other	4-year college degree	2-year college degree	Some college, no degree	High school diploma or GED
a. <u>Preferred</u> educational attainment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Required educational attainment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

39. What is the **PREFERRED** minimum educational level and **REQUIRED** minimum educational level used in vacancy announcements for **FULL-TIME** entry-level **nonsworn** officers? *Please select ONE response per row.*

Mark here if not applicable -- no full-time NONSWORN officers. Go to Question 40.

	None stated	Other	4-year college degree	2-year college degree	Some college, no degree	High school diploma or GED
a. <u>Preferred</u> educational attainment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Required educational attainment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

40. As of September 30, 2011, how many **FULL-TIME** officers on your force had achieved each of the following educational levels? *Please enter the total number for each category.*

	Number of Officers by Highest Educational Attainment			
	2-year college degree	4-year college degree	Graduate degree	Not applicable
a. Sworn police officers				<input type="text"/>
b. Nonsworn security officers				<input type="text"/>

41. Over the past 3 years, what proportion of **FULL-TIME** personnel received at least 8 hours of **community policing training** on topics such as problem solving, the SARA model (Scanning, Analysis, Response and Assessment), community partnerships, etc.? *Please select ONE response per row.*

	All	Some	None	Not applicable
a. New sworn police recruits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. New nonsworn security recruits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. In-service sworn police officers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. In-service nonsworn security officers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

42. Does your agency use the following methods to screen new applicants for **FULL-TIME** **sworn** police officer positions? *Please select ONE response per row.*

Mark here if not applicable -- no full-time SWORN officers. Go to Question 44.

	Yes	No
Background/record checks		
a. Background investigation	<input type="radio"/>	<input type="radio"/>
b. Credit history check	<input type="radio"/>	<input type="radio"/>
c. Criminal record check	<input type="radio"/>	<input type="radio"/>
d. Reference check	<input type="radio"/>	<input type="radio"/>
e. Driving record check	<input type="radio"/>	<input type="radio"/>
Personal attributes		
f. Personal interview	<input type="radio"/>	<input type="radio"/>
g. Personality inventory	<input type="radio"/>	<input type="radio"/>
h. Polygraph exam	<input type="radio"/>	<input type="radio"/>
i. Psychological evaluation	<input type="radio"/>	<input type="radio"/>
j. Voice stress analyzer	<input type="radio"/>	<input type="radio"/>
k. Written aptitude test	<input type="radio"/>	<input type="radio"/>
Community relations skills		
l. Assessment of analytical problem-solving ability	<input type="radio"/>	<input type="radio"/>
m. Assessment of understanding of cultural diversity	<input type="radio"/>	<input type="radio"/>
n. Assessment of mediation/conflict management skills	<input type="radio"/>	<input type="radio"/>
o. Second-language ability test	<input type="radio"/>	<input type="radio"/>
p. Volunteer/Community service check	<input type="radio"/>	<input type="radio"/>
q. Role-play assessment center	<input type="radio"/>	<input type="radio"/>
Physical attributes		
r. Drug test	<input type="radio"/>	<input type="radio"/>
s. Medical exam	<input type="radio"/>	<input type="radio"/>
t. Physical agility test	<input type="radio"/>	<input type="radio"/>

43. Excluding in-service training, how many hours of academy and field training are required for FULL-TIME **sworn** police officer **recruits** for entry into service?

Mark here if not applicable -- no full-time SWORN officers. Go to Question 44.

For full-time SWORN police recruits	Total # hours	# Academy hours	# Field hours	No training of that type required
a. State-mandated training hours				<input type="radio"/>
b. Additional agency-required hours				<input type="radio"/>

44. Does your agency use the following methods to screen new applicants for FULL-TIME **nonsworn** security officer positions? *Please select ONE response per row.*

Mark here if not applicable -- no full-time NONSWORN officers. Go to Question 46.

	Yes	No
Background/record checks		
a. Background investigation	<input type="radio"/>	<input type="radio"/>
b. Credit history check	<input type="radio"/>	<input type="radio"/>
c. Criminal record check	<input type="radio"/>	<input type="radio"/>
d. Reference check	<input type="radio"/>	<input type="radio"/>
e. Driving record check	<input type="radio"/>	<input type="radio"/>
Personal attributes		
f. Personal interview	<input type="radio"/>	<input type="radio"/>
g. Personality inventory	<input type="radio"/>	<input type="radio"/>
h. Polygraph exam	<input type="radio"/>	<input type="radio"/>
i. Psychological evaluation	<input type="radio"/>	<input type="radio"/>
j. Voice stress analyzer	<input type="radio"/>	<input type="radio"/>
k. Written aptitude test	<input type="radio"/>	<input type="radio"/>
Community relations skills		
l. Assessment of analytical problem-solving ability	<input type="radio"/>	<input type="radio"/>
m. Assessment of understanding of cultural diversity	<input type="radio"/>	<input type="radio"/>
n. Assessment of mediation/conflict management skills	<input type="radio"/>	<input type="radio"/>
o. Second-language ability test	<input type="radio"/>	<input type="radio"/>
p. Volunteer/Community service check	<input type="radio"/>	<input type="radio"/>
q. Role-play assessment center	<input type="radio"/>	<input type="radio"/>
Physical attributes		
r. Drug test	<input type="radio"/>	<input type="radio"/>
s. Medical exam	<input type="radio"/>	<input type="radio"/>
t. Physical agility test	<input type="radio"/>	<input type="radio"/>

45. Excluding in-service training, how many hours of academy and field training are required for newly hired FULL-TIME **nonsworn** security officers for entry into service?

Mark here if not applicable -- no full-time NONSWORN officers. Go to Question 46.

For newly hired full-time NON-SWORN security officers	Total # hours	# Academy hours	# Field hours	No training of that type required
a. State-mandated training hours				<input type="radio"/>
b. Additional agency-required hours				<input type="radio"/>

46. Does your agency participate in the following types of "Active Shooter Training"? *Please select ONE response per row.*

	Yes	No
a. Workshop/Seminar/Lecture	<input type="radio"/>	<input type="radio"/>
b. Mock exercise/Scenario	<input type="radio"/>	<input type="radio"/>
c. Virtual reality	<input type="radio"/>	<input type="radio"/>
d. Other type	<input type="radio"/>	<input type="radio"/>

EQUIPMENT

47a. Which of the following types of **weapons/actions** are authorized for use by your agency's FULL-TIME **sworn** police officers? *Please select ONE response per row.*

Mark here if not applicable -- no full-time SWORN police officers. Go to Question 47b.

	Yes	No
a. Sidearm, semiautomatic	<input type="radio"/>	<input type="radio"/>
b. Sidearm, revolver	<input type="radio"/>	<input type="radio"/>
c. Rifle	<input type="radio"/>	<input type="radio"/>
d. Shotgun	<input type="radio"/>	<input type="radio"/>
e. Traditional baton	<input type="radio"/>	<input type="radio"/>
f. PR-24 baton	<input type="radio"/>	<input type="radio"/>
g. Collapsible baton	<input type="radio"/>	<input type="radio"/>
h. Chemical/pepper spray	<input type="radio"/>	<input type="radio"/>
i. Conducted energy device (e.g. Taser)	<input type="radio"/>	<input type="radio"/>
j. Bean bag rifle	<input type="radio"/>	<input type="radio"/>
k. Rubber bullets	<input type="radio"/>	<input type="radio"/>
l. Flash/bang grenade	<input type="radio"/>	<input type="radio"/>

EQUIPMENT (cont'd)

47b. Which of the following types of **weapons/actions** are authorized for use by your agency's FULL-TIME **nonsworn** security officers? Please select ONE response per row.

Mark here if not applicable -- no full-time NONSWORN security officers. Go to Question 48.

- | | Yes | No |
|---|-----------------------|-----------------------|
| a. Sidearm, semiautomatic | <input type="radio"/> | <input type="radio"/> |
| b. Sidearm, revolver | <input type="radio"/> | <input type="radio"/> |
| c. Rifle | <input type="radio"/> | <input type="radio"/> |
| d. Shotgun | <input type="radio"/> | <input type="radio"/> |
| e. Traditional baton | <input type="radio"/> | <input type="radio"/> |
| f. PR-24 baton | <input type="radio"/> | <input type="radio"/> |
| g. Collapsible baton | <input type="radio"/> | <input type="radio"/> |
| h. Chemical/pepper spray | <input type="radio"/> | <input type="radio"/> |
| i. Conducted energy device (e.g. Taser) | <input type="radio"/> | <input type="radio"/> |
| j. Bean bag rifle | <input type="radio"/> | <input type="radio"/> |
| k. Rubber bullets | <input type="radio"/> | <input type="radio"/> |
| l. Flash/bang grenade | <input type="radio"/> | <input type="radio"/> |

48. How many vehicles of each type below were used regularly by your agency in 2011? Of those vehicles, how many were electric or hybrid vehicles?

Vehicle Type	Total # of vehicles	# that are marked	# that are electric or hybrid
a. Cars			
b. Vans			
c. Trucks			
d. Sport-utility vehicles (SUVs)			
e. Golf carts			
f. Motorcycles			
g. Bicycles			
h. Boats			
i. Personal transporter (e.g., Segway)			
j. Other (please specify):			

49. Do patrol officers in your agency have **direct electronic access** to the following? Please select ONE response per row.

	No direct electronic access	Yes, both mobile and fixed-site access	Yes, fixed-site access only	Yes, mobile access only
--	-----------------------------	--	-----------------------------	-------------------------

- | | | | | |
|------------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| a. Calls-for-service records | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| b. Criminal history records | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| c. Driving records | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| d. Linked files for crime analysis | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| e. Motor vehicle records | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| f. Student information | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| g. Employee information | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

50. Do any of the officers in your agency use the following types of **electronic devices** while on patrol? Please select ONE response per row.

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Vehicle-mounted computer/terminal | <input type="radio"/> | <input type="radio"/> |
| b. Portable computer/terminal (not vehicle-mounted) | <input type="radio"/> | <input type="radio"/> |
| c. Other electronic device (PDA, smart phones, etc.) | <input type="radio"/> | <input type="radio"/> |

51. Does your agency use **computers or electronic devices** for any of the following functions? Please select ONE response per row.

- | | Yes | No |
|-------------------------------------|-----------------------|-----------------------|
| a. Crime mapping | <input type="radio"/> | <input type="radio"/> |
| b. Dispatch (CAD) | <input type="radio"/> | <input type="radio"/> |
| c. Inter-agency information sharing | <input type="radio"/> | <input type="radio"/> |
| d. In-field reporting | <input type="radio"/> | <input type="radio"/> |

PROBLEM MANAGEMENT

52. In 2011, did your agency meet regularly with the following to discuss **crime-related problems**? Please select ONE response per row.

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Advocacy groups | <input type="radio"/> | <input type="radio"/> |
| b. Business groups | <input type="radio"/> | <input type="radio"/> |
| c. Campus administrators/officials | <input type="radio"/> | <input type="radio"/> |
| d. Domestic violence prevention groups | <input type="radio"/> | <input type="radio"/> |
| e. Faculty/Staff organizations | <input type="radio"/> | <input type="radio"/> |
| f. Fraternity/Sorority groups | <input type="radio"/> | <input type="radio"/> |
| g. Student Government Association | <input type="radio"/> | <input type="radio"/> |
| h. Local public officials | <input type="radio"/> | <input type="radio"/> |
| i. Neighborhood associations | <input type="radio"/> | <input type="radio"/> |
| j. Other law enforcement agencies | <input type="radio"/> | <input type="radio"/> |
| k. Religious groups | <input type="radio"/> | <input type="radio"/> |
| l. Sexual violence prevention programs | <input type="radio"/> | <input type="radio"/> |
| m. Student housing groups | <input type="radio"/> | <input type="radio"/> |
| n. Student organizations | <input type="radio"/> | <input type="radio"/> |

53. In 2011, did your agency engage in any of the following activities? *Please select ONE response per row.*

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Actively encouraged officers to engage in SARA-type problem-solving projects on campus | <input type="radio"/> | <input type="radio"/> |
| b. Conducted an on-campus citizen police academy | <input type="radio"/> | <input type="radio"/> |
| c. Maintained or created a formal, written community policing plan | <input type="radio"/> | <input type="radio"/> |
| d. Incorporated community policing elements into campus security policy | <input type="radio"/> | <input type="radio"/> |
| e. Gave officers responsibility for specific geographic areas on campus | <input type="radio"/> | <input type="radio"/> |
| f. Included collaborative problem-solving projects in the evaluation criteria of patrol officers ... | <input type="radio"/> | <input type="radio"/> |
| g. Upgraded technology to support the analysis of campus community problems | <input type="radio"/> | <input type="radio"/> |
| h. Partnered with citizen groups and included their feedback in the development of community policing strategies | <input type="radio"/> | <input type="radio"/> |
| i. Conducted a ride-along program | <input type="radio"/> | <input type="radio"/> |
| j. Conducted Environmental Analysis (CPTED) to assess precursors to crime | <input type="radio"/> | <input type="radio"/> |
| k. Conducted intelligence-led policing | <input type="radio"/> | <input type="radio"/> |
| l. Conducted joint patrols with local law enforcement | <input type="radio"/> | <input type="radio"/> |

54. Did your agency engage in any of the following **preparedness activities** in 2011? *Please select ONE response per row.*

- | | Yes | No |
|---|-----------------------|-----------------------|
| a. Disseminated information to increase citizen preparedness | <input type="radio"/> | <input type="radio"/> |
| b. Formal intelligence-sharing agreements with other law enforcement agencies | <input type="radio"/> | <input type="radio"/> |
| c. Participated in meetings with campus administrators/staff regarding emergency preparedness plans | <input type="radio"/> | <input type="radio"/> |
| d. Designed or revised a preparedness plan for a school shooting | <input type="radio"/> | <input type="radio"/> |
| e. Designed or revised a preparedness plan for an emergency evacuation of campus .. | <input type="radio"/> | <input type="radio"/> |

55. Were **student patrols** used on your campus in 2011?

- Yes No -- Go to Question 56.

55a. If student patrols were used on your campus, did these student patrols perform any of the following functions? *Please select ONE response per row.*

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Special event security | <input type="radio"/> | <input type="radio"/> |
| b. Auxiliary patrol during normal patrol hours | <input type="radio"/> | <input type="radio"/> |
| c. Building lock-up | <input type="radio"/> | <input type="radio"/> |
| d. Emergency response | <input type="radio"/> | <input type="radio"/> |
| e. Recruitment tool for agency | <input type="radio"/> | <input type="radio"/> |
| f. Residence hall security | <input type="radio"/> | <input type="radio"/> |
| g. Safety escorts | <input type="radio"/> | <input type="radio"/> |

56. In 2011, for each issue listed below, did your agency have a special unit with FULL-TIME personnel, use designated personnel as needed, have policies and procedures only, or not officially address the issue? *Please select ONE response per row.*

- | | Not officially addressed | Policies and procedures only | Designated personnel used as needed | Unit with personnel assigned full time |
|--|--------------------------|------------------------------|-------------------------------------|--|
| a. Alcohol education | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| b. Bicycle/Pedestrian safety | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| c. Date rape prevention | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| d. Drug education | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| e. General crime prevention | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| f. General rape prevention | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| g. Self-defense training | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| h. Suicide prevention | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| i. Bias/Hate crime | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| j. Community policing | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| k. Cybercrime | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| l. Identity theft | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| m. Intimate partner violence | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| n. Research and planning | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| o. Social network abuse (including online stalking, intimidation, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| p. Stalking | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| q. Student security patrol | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| r. Victim assistance | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| s. White collar crime | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

57. Did **sworn** police officers (full time or part time) from your agency participate in the following events in 2011? *Please select ONE response per row.*

- Mark here if not applicable -- no SWORN officers. Go to Question 58.

- | | Yes | No |
|---|-----------------------|-----------------------|
| a. Crime prevention programs at orientation .. | <input type="radio"/> | <input type="radio"/> |
| b. Drug/Alcohol programs at orientation | <input type="radio"/> | <input type="radio"/> |
| c. Crime prevention programs during the academic year | <input type="radio"/> | <input type="radio"/> |
| d. Drug/Alcohol programs during the academic year | <input type="radio"/> | <input type="radio"/> |

PROBLEM MANAGEMENT

58. Did **nonsworn** security officers (full time or part time) from your agency participate in the following events in 2011? *Please select ONE response per row.*

Mark here if not applicable -- no NONSWORN officers. Go to Question 59.

- | | Yes | No |
|---|-----------------------|-----------------------|
| a. Crime prevention programs at orientation | <input type="radio"/> | <input type="radio"/> |
| b. Drug/Alcohol programs at orientation | <input type="radio"/> | <input type="radio"/> |
| c. Crime prevention programs during the academic year | <input type="radio"/> | <input type="radio"/> |
| d. Drug/Alcohol programs during the academic year | <input type="radio"/> | <input type="radio"/> |

59. Did your agency have a **campus safety escort service** in 2011?

Yes No -- Go to Question 60.

59a. Did your campus safety escort service include any of the following characteristics in 2011? *Please select ONE response per row.*

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Staffed by sworn police officers | <input type="radio"/> | <input type="radio"/> |
| b. Staffed by nonsworn security officers | <input type="radio"/> | <input type="radio"/> |
| c. Staffed by students | <input type="radio"/> | <input type="radio"/> |
| d. Walking escort service | <input type="radio"/> | <input type="radio"/> |
| e. Vehicle escort service | <input type="radio"/> | <input type="radio"/> |

60. Does your agency use any of the following methods for receiving **citizen complaints**? *Please select ONE response per row.*

- | | Yes | No |
|---|-----------------------|-----------------------|
| a. Complaints may be filed in person at agency | <input type="radio"/> | <input type="radio"/> |
| b. Complaints may be filed anonymously at agency | <input type="radio"/> | <input type="radio"/> |
| c. Complaints may be filed online at department website | <input type="radio"/> | <input type="radio"/> |
| d. Complaints may be filed online at another website | <input type="radio"/> | <input type="radio"/> |
| e. Complaints may be filed by telephone | <input type="radio"/> | <input type="radio"/> |
| f. Other form of filing available - please specify below: | <input type="radio"/> | <input type="radio"/> |

JURISDICTION AND JOINT EFFORTS

61. Do **FULL-TIME sworn** officers in your agency have **arrest** jurisdiction for any of the following? *Please select ONE response per row.*

Mark here if not applicable -- no full-time SWORN officers. Go to Question 62.

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Properties adjacent to campus | <input type="radio"/> | <input type="radio"/> |
| b. Properties outside the area surrounding the campus | <input type="radio"/> | <input type="radio"/> |
| c. Off-campus jurisdiction defined and carried out through a Memorandum of Understanding (MOU) or Mutual Aid Agreement | <input type="radio"/> | <input type="radio"/> |
| d. State-wide jurisdiction | <input type="radio"/> | <input type="radio"/> |

62. Do any **FULL-TIME** officers in your agency have **patrol** jurisdiction for any of the following? *Please select ONE response per row.*

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. Campus property | <input type="radio"/> | <input type="radio"/> |
| b. Properties adjacent to campus | <input type="radio"/> | <input type="radio"/> |
| c. Properties outside the area surrounding the campus | <input type="radio"/> | <input type="radio"/> |
| d. Off-campus jurisdiction defined and carried out through a Memorandum of Understanding (MOU) or Mutual Aid Agreement | <input type="radio"/> | <input type="radio"/> |

63. Does your agency currently have a Memorandum of Understanding (MOU) or Mutual Aid Agreement with the following types of agencies? *Please select ONE response per row.*

- | | Yes | No |
|--|-----------------------|-----------------------|
| a. State law enforcement agency (non-campus) | <input type="radio"/> | <input type="radio"/> |
| b. Local police department | <input type="radio"/> | <input type="radio"/> |
| c. Sheriff's office/department | <input type="radio"/> | <input type="radio"/> |
| d. Other campus law enforcement agency | <input type="radio"/> | <input type="radio"/> |
| e. Other campus agency (non-law enforcement) | <input type="radio"/> | <input type="radio"/> |
| f. State or local courts | <input type="radio"/> | <input type="radio"/> |
| g. Other agency not listed above - please specify below: | <input type="radio"/> | <input type="radio"/> |

JURISDICTION AND JOINT EFFORTS (cont'd)

64. What was your agency's accreditation status with CALEA* and IACLEA** as of September 30, 2011?
Please select ONE response per row.

	Accredited	Commission review phase	On-site assessment phase	Self-assessment phase	Application phase	None
a. Status with CALEA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Status with IACLEA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Commission on Accreditation for Law Enforcement Agencies (CALEA)

** International Association of Campus Law Enforcement Administrators (IACLEA)

ProQuest Number: 29211417

INFORMATION TO ALL USERS

The quality and completeness of this reproduction is dependent on the quality and completeness of the copy made available to ProQuest.



Distributed by ProQuest LLC (2022).

Copyright of the Dissertation is held by the Author unless otherwise noted.

This work may be used in accordance with the terms of the Creative Commons license or other rights statement, as indicated in the copyright statement or in the metadata associated with this work. Unless otherwise specified in the copyright statement or the metadata, all rights are reserved by the copyright holder.

This work is protected against unauthorized copying under Title 17, United States Code and other applicable copyright laws.

Microform Edition where available © ProQuest LLC. No reproduction or digitization of the Microform Edition is authorized without permission of ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346 USA