2017

Cyber-harassment in higher education: a study of institutional policies and procedures

Victoria Ann Schaefer-Ramirez

Pepperdine University

Graduate School of Education and Psychology

CYBER-HARASSMENT IN HIGHER EDUCATION:

A STUDY OF INSTITUTIONAL POLICIES AND PROCEDURES

A dissertation submitted in partial satisfaction

of the requirements for the degree of

Doctor of Education in Organizational Leadership

by

Victoria Ann Schaefer-Ramirez

April, 2017

Farzin Madjidi, Ed.D. – Dissertation Chairperson

This dissertation, written by

Victoria Ann Schaefer-Ramirez

under the guidance of a Faculty Committee and approved by its members, has been submitted to and accepted by the Graduate Faculty in partial fulfillment of the requirements for the degree of

DOCTOR OF EDUCATION

Doctoral Committee:

Farzin Madjidi, Ed.D. Chairperson

Lani Simpao Fraizer, Ed.D.

Gabriella Miramontes, Ed.D.

TABLE OF CONTENTS

Page

LIST OF TABLES vi

LIST OF FIGURES vii

DEDICATION viii

ACKNOWLEDGEMENTS ix

VITA x

ABSTRACT xi

Chapter 1: Introduction to the Study 1

- Statement of the Problem 6
- Purpose of the Study 6
- Research Questions 7
- Significance of the Study 7
- Assumptions 8
- Limitations of the Study 8
- Definition of Terms 9
- Summary 11

Chapter 2: Literature Review 13

- Bullying and Harassment 13
- Cyberbullying and Cyber-harassment 15
- Federal and State law 26
- Title IX of the Department of Education and Office for Civil Rights 30
- Jeanne Clery Disclosure of Campus Security Policy and Crime Statistics Act 35
- Violence Against Women Act 39
- Case Law 43
- University Risk, Response, and Responsibility 44
- Summary 49

Chapter 3: Research Design and Methodology 52

- Restatement of Research Questions 53
- Research Methodology 53
- Research Design 54
- Interview Protocol 61
- Statement of Limitations and Personal Bias 66
- Data Analysis 69

Inter-rater Reliability 71
Summary 72

Chapter 4: Findings 73

Recruitment of Participants 74
Data Collection Process 76
Data Analysis 80
Data Display 81
Research Question One 81
Research Question Two 93
Research Question Three 103
Research Question Four 114
Summary 118

Chapter 5: Conclusions and Recommendations 121

Results and Discussion of Findings 122
Implications of the Study 131
Recommendations for Future Research 134
Broader Application and Final Thoughts 135

REFERENCES 144

APPENDIX A: Protecting Human Research Certificate of Completion 160

APPENDIX B: ACUPA Site Approval 162

APPENDIX C: Recruitment Letter 163

APPENDIX D: IRB Exemption Notice 164

APPENDIX E: Informed Consent 166

APPENDIX F: Letter of Intent 169

APPENDIX G: Nondisclosure and Review Form for Inter-Rater Reliability 170

APPENDIX H: Interview Questions 171

LIST OF TABLES

Page

Table 1. Cyberbullying Definitions 18

Table 2. Forms of Cyberbullying 24

Table 3. Research Questions and Corresponding Interview Questions 66

Table 4. Dates of the Participant Interviews 77

Table 5. Cyber-Harassment Policy Framework 139

Table 6. Analysis of Cyberbullying and Cyber-Harassment Definitions 142

LIST OF FIGURES

Figure 1. Participant responses 76

Figure 2. Student enrollment at participating institutions. 80

Figure 3. Themes and frequencies of responses associated with interview question 1. 82

Figure 4. Themes and frequencies of responses associated with interview question 2. 85

Figure 5. Themes and frequencies of responses associated with interview question 3. 87

Figure 6. Themes and frequencies of responses associated with interview question 4. 89

Figure 7. Themes and frequencies of responses associated with interview question 5. 94

Figure 8. Themes and frequencies of responses associated with interview question 6. 98

Figure 9. Themes and frequencies of responses associated with interview question 7. 99

Figure 10. Themes and frequencies of responses associated with interview question 9. 105

Figure 11. Themes and frequencies of responses associated with interview question 10. 107

Figure 12. Themes and frequencies of responses associated with interview question 11. 110

Figure 13. Themes and frequencies of responses associated with interview question 12. 112

Figure 14. Themes and frequencies of responses associated with interview question 13. 115

Figure 15. Themes and frequencies of responses associated with interview question 14. 117

DEDICATION

I dedicate this work to my daughter, Allison, whose presence in my life has brought me tremendous joy and purpose. May you progress and surpass me in every way.

With love, Mommy

ACKNOWLEDGEMENTS

As I reflect upon this journey, I am humbled by the support and encouragement shown to me throughout this process. I wish to acknowledge the love and kindness those have given.

To my wonderful dissertation committee. Dr. Farzin Madjidi, thank you for seeing in me, what I could not see in myself. I will forever be grateful for your encouragement and support. Dr. Gabriella Miramontes, thank you for challenging me and encouraging me to meet my full potential. Dr. Lani Fraizer, words cannot express my appreciation and gratitude for all that you have done. For your thoughtful guidance, dedication, and support – I am grateful for you.

To my GAP and EIP cohort at Pepperdine University. Thank you for giving me the opportunity to learn from you. I am especially grateful for my #EDOLbesties; Stephen Birch, Grey Hoff, Gene Coughlin, Samantha Kahoe, and Gabrielle Ellerbrock. You have supported me without reservation, accepted me for who I am, and have helped me become the person I should be. I am honored to call you my colleagues, and blessed to call you my friends.

I owe a considerable debt of gratitude to my family for their unconditional love and support. To my sisters, Liv and Tina, you are my "bestest" friends. Always have been, always will be. To my big brother, Glenn, thank you for your never-ending encouragement. To my beautiful baby girl Alli, thank you for your patience and understanding. You inspire me to love more, be more, and do more. To my husband, Angel, for your unselfish, loving, and encouraging support. Your unfailing belief in me gave me the confidence that I needed to complete this degree. Thank you for being my unconditional everything.

Finally, I would be remiss if I didn't take this opportunity to thank God, to whom I owe my very existence and whose blessings have made me the person I am today.

VITA

EDUCATION

Pepperdine University, Graduate School of Education and Psychology 2017
Doctor of Education in Organizational Leadership
Comprehensive Examination with honors
Dissertation title: Cyber-harassment in Higher Education: A Study of Institutional Policies and Procedures

University of Phoenix, School of Business 2007
Master of Business Administration in Technology Management

San Diego State University, College of Business Administration 2003
Bachelor of Science in Accounting

PROFESSIONAL EXPERIENCE

National University System, La Jolla, California October 2011 - Present
Title IX System Coordinator and Compliance Officer
Operations Analyst; Office of the Chancellor

Management and Operations Consultant [self-employed], San Diego, California May 2009 – October 2011
Principle Consultant

Encore Capital Group [NASDAQ: ECPG], San Diego, California March 2006 – May 2009
Process Manager II; Business Process Improvement and Strategic Initiatives
Process Manager II; Legal Outsourcing

Booz Allen Hamilton, San Diego, California August 2003 – March 2006
Senior Consultant
Consultant

COMMITTEE WORK

National University, La Jolla, CA
Research Council - Ex officio

National University System, La Jolla, CA
Enterprise Risk Committee - Chair

PRESENTATIONS

Schaefer-Ramirez, V. (2016) "Promoting a Culture of Safety: Legal Obligations in Higher Education to Mitigate Cyber Bullying" presented at the International Organization of Social Sciences and Behavioral Research (IOSSBR) Conference

PROFESSIONAL MEMBERSHIPS

Association of College and University Policy Administrators (ACUPA)
National Association of College and University Business Officers (NACUBO)
Association of Title IX Administrators (ATIXA)
Society of Corporate Compliance and Ethics (SCCE)

ABSTRACT

Cyberbullying is a growing phenomenon, causing concern among students, parents, and professionals in the educational community. Although no federal law specifically addresses cyber-harassment in higher education, institutions have a legal obligation to address all claims of harassment, regardless of the location or platform in which the harassing behavior occurs. Recent court cases are setting precedents for obligatory institutional response and potential penalties for lack thereof; conversely, institutions are left to their own devices to employ and develop policy statements and sanctions that prohibit or discourage cyber-harassment behaviors. As the legal and political environment regarding bullying and cyberbullying behaviors continues to evolve, universities are challenged to administer policies and procedures that address misconduct that occurs in physical and virtual environments.

Qualitative by design, this study examines the perspectives, insights, and understandings of those individuals responsible for developing and operationalizing policies in the areas of cyber-harassment. Accordingly, participants in this research study provided key insights regarding strategies, best practices, and challenges experienced by policy administrators when developing and implementing cyber-harassment, prevention and mitigation policies and programs. Participants' perspectives provided an insightful understanding of the complexities of interpreting legislation and the implications associated with higher education policy.

Keywords: higher education, cyber-harassment, harassment, policy, title ix

Chapter 1: Introduction to the Study

Institutions of higher education have an ethical and legal obligation to provide students with reasonable security and protection (U.S. Department of Education, 2014c). With over 21 million students enrolled at over 4,500 postsecondary degree granting institutions operating within the United States (U.S. Census Bureau, 2011), issues of campus safety are of great concern (Westat, Ward, & Mann, 2011). Higher education administrators are challenged with expanding protocol in their "commitment to ensure the safety and general welfare of those on their campuses and to provide appropriate policies, procedures, and strategies to maintain a safe campus" (U.S. Department of Education, 2010, p. 1).

Technology has increased the effectiveness and efficiency of communication. Despite the advantages technology provides, technology has fundamentally changed the way in which people communicate. Changes in technology have changed how education is facilitated, the manner and method in which students interface with other students, and the interaction between student and instructor (Rogers, 2000). Institutions of higher education have capitalized on technological advances, with over 86% of postsecondary institutions offering online courses in 2012 (Allen & Seaman, 2013). With advances in technology, higher education administrators are challenged with expanding protocol beyond the physical boundaries of a campus and into the virtual environment.

Despite the benefits, the introduction of such technologies provides for a format in which malicious behaviors can occur (Beran & Li, 2005; Francisco, Veiga Simão, Ferreira, & Martins, 2015). The development and expansion of information and communication technologies introduced several types of malevolent behaviors, including "deleterious social interactions such as cyberbullying" (Kubiszewski, Fontaine, Potard, & Auzoult, 2015; Willard, 2005).

Cyberbullying is summarized as "a bullying problem occurring in a new territory" (Li, 2006, p. 166).

Cyberbullying is a new and growing phenomenon, causing concern among students, parents, and professionals in the educational community. To understand the nature and extent of cyberbullying, researchers have conducted studies to explore the prevalence of this phenomenon (Li, 2006, 2007; Patchin & Hinduja, 2006). Scholarly research on cyberbullying behaviors performed on elementary, middle school, and high school aged populations range from 9% to 42% (Kowalski, Giumetti, Schroader, & Lattner, 2014). Additionally, cyberbullying research conducted by Kiriakidis and Kavoura (2010) showed that cyberbullying behaviors increase from middle school to high school. Given this trend, it is logical to conclude that college students experience cyberbullying as well (Crosslin & Golman, 2014; Schenk, Fremouw, & Keelan, 2013).

Research conducted by Schenk et al. (2013) reported victims show higher rates of depression, paranoia, and are more likely to consider suicide or attempt suicide. Cyberbullying has risen to the head of public agenda after unfortunate events broadcasted by the media (Tokunaga, 2010). Psychological and emotional impacts are not limited to victims of cyberbullying. Recent studies have shown repercussions to cyberbullying victims, bystanders, and bullies themselves (Schenk et al., 2013)

Higher education legal environment. Educational institutions are complex organizations that are governed by a diverse and multifaceted set of federal, state, and agency regulations. The Higher Education Compliance Alliance (n.d.) has compiled a list of over 250 regulations that govern the day-to-day operations of an institution. Legislators have clearly addressed campus safety and security risks by adopting the Jeanne Clery Disclosure of Campus

Security Policy and Crime Statistics Act (1998), more commonly referred to as the Clery Act; the Reauthorization of the Violence Against Women Act (2013); Title VII of the Civil Rights Act (1964); Section 504 of the Rehabilitation Act of 1973; the Age Discrimination Act of 1975; and 20 U.S.C. Section 1681 et seq., Title IX of the Education Amendments of 1972 and its implementing regulations.

As a strategy to promote a culture of safety on higher education campuses, the U.S. Department of Education has prescribed prevention and mitigation efforts, mandated educational programs, and enforced sanctions on those that fail to meet regulatory standards (Krebs, Lindquist, Warner, Fisher, & Martin, 2007; National Victim Center, 1992). Policies are enforced through the establishment of authoritative offices such as the Department of Education's Office for Civil Rights (OCR). Where Title VII of the Civil Rights Act prohibits sex based discrimination in the workplace, Title IX of the Education Amendments (1972) prohibits sex based discrimination in federally funded educational programs and activities (Townley & Schmieder-Ramirez, 2010; U.S. Department of Education, 2015; U.S. Department of Justice, 2001). Per Title 34 of the Code of Federal Regulation Part 106.8 (2000), regulations promulgated by the U.S. Department of Education requires institutions to designate an employee whose responsibility is to develop, implement, and monitor an institution's policies and procedures in compliance with Title IX (1972) regulation (U.S. Department of Justice, 2015b). Designated employees are referred to as Title IX Coordinators (Lhamon, 2015a; U.S. Department of Justice, 2015b).

In a study conducted by the U.S. Department of Justice (Baum & Klaus, 2005), researchers discovered that over 93% of campus crimes assessed between 1995 and 2002 occurred off-campus. Regardless of the location of the reported crime, higher education

institutions are required to provide victims with reasonable accommodations regardless if the alleged perpetrator is associated with the institution. Higher education institutions are legally responsible for addressing alleged violations of conduct at a standard of proof that is more conservative than that imposed through legal proceedings (U.S. Department of Justice, 2015a). Additionally, should the alleged be a student at that same institution, the alleged may be subject to disciplinary hearings and institutional sanctions in addition to any disciplinary actions allowed by federal and state legislation.

College and university campus operations are highly regulated through federal, state, and government agency legislation, although regulations that pertain specifically to virtual conduct remains limited. With insufficient regulatory guidance addressing online codes of conduct, institutions are faced with potential legal risk and unknown levels of vulnerability (Fisher, 1995). As the legal and political environment regarding bullying and cyberbullying behaviors continues to evolve, universities are challenged to administer policies and procedures that address misconduct that occurs in physical and virtual environments. Although no federal law specifically addresses cyber-harassment in higher education, institutions have a legal responsibility to address all claims of harassment regardless of the location or platform in which the harassing behavior occurs.

Cyberbullying and cyber-harassment. Cyberbullying is bullying that is facilitated through the use of technology, including cell phones, computers, digital communication tools and forums including text messages, email, and social media sites, to send or post messages with the intent of hurting or humiliating another individual (National Centre Against Bullying, n.d.; National Crime Prevention Council, n.d.; U.S. Department of Health and Human Services, 2013). While cyberbullying typically refers to bullying of children and teens, cyberbullying

adults is referred to as cyber-harassment (Gupta, 2008; Vance, 2010). When referring to bullying that occurs through technological platforms, cyberbullying and cyber-harassment are used interchangeably (Beran & Li, 2005; Vance, 2010).

There is an extensive amount of research regarding the prevalence and impact of bullying behaviors in pre-adolescent and adolescent groups. Bullying behaviors foster "a climate of fear and disrespect that can seriously impair the physical and psychological health of its victims and create conditions that negatively affect learning" (Ali, 2010, p. 1), undermining a student's ability to reach their full potential. However, cyberbullying behaviors among adults, specifically within the college-age student populations, are still being investigated and further defined.

A study conducted by Pew Research Center (Duggen, 2014) found that young adults between the ages of 18–29 are more likely to experience online harassment than those in other age groups, with young women between the ages of 18–24 experiencing "severe types of harassment at disproportionately higher levels" (p. 3), including behaviors such as stalking and online sexual harassment. A study conducted at a large, private, not-for-profit university found that students and faculty, 12% and 39% respectively, had been victims of cyber-harassment (Vance, 2010). Zalaquett and Chatters (2014) found that 19% of college and university students surveyed were victims of cyber-harassment, with 38% of those respondents specifically reporting harassment based on sexuality or gender. This phenomenon is not limited to K–12 students, and as additional research has shown, cyber-harassing behaviors continue to occur outside of adolescent populations.

Institutions are limited in their ability to influence federal, state, and legislative mandates. As a result, changes in legislation solicit a reactionary response, and institutions must face the challenge of interpreting and operationalizing legislation. Although no federal law specifically

addresses cyber-harassment, institutions have a legal obligation to address all harassment claims, regardless of the location or platform in which the harassing behavior occurs (Ali, 2010). While the landscape of responsibility required of post-secondary institutions continues to expand and evolve, institutions must not only respond to, comply with, and operationalize regulatory changes, but also create and implement policies that address appropriate student conduct. Federal regulations and recommended best practices from respected organizations provide detailed guidance on the implementation of policies and the execution of effective programs (Jozkowski, Henry, & Sturm, 2014; U.S. Department of Justice, 2000).

Statement of the Problem

Thus far, legislation has failed to specifically address higher education institution's responsibility in addressing cyberbullying. Recent court cases are setting precedents for obligatory institutional response and potential penalties for lack thereof. Conversely, institutions are left to their own devices to employ policies and procedures that prohibit, discourage, and respond to cyber-harassment behaviors. Given that institutions are legally responsible for the safety and general wellbeing of their students (Fisher, 1995; U.S. Department of Education, 2010), this study addresses policies and procedures regarding cyber-harassment.

Purpose of the Study

It is vital for institutions to prevent and mitigate unwelcome conduct and to respond appropriately and effectively should misconduct occur. Accordingly, the purpose of this qualitative study was to determine the strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. Additionally, this study sought to determine success measures and recommendations for future implementation for higher education institutions when preventing and mitigating cyber-harassment.

Research Questions

- What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment?
- What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment?
- How do higher education institutions measure the success of cyber-harassment policies and procedures?
- What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures?

Significance of the Study

The significance of this study has become increasingly important due to recent changes in legislation, case law, and media attention with regard to cyber-harassment in higher education. For institutions that encourage the use of technology and especially for those institutions that promote and facilitate online learning platforms, it is imperative to understand the risks and potential occurrences of unwelcome misconduct within virtual environments. College and university campus operations are highly regulated through federal, state, and government agency legislation, although regulations that pertain specifically to virtual conduct remains limited. As institutions become increasingly liable for the prevention and mitigation of, and appropriate response efforts to, cyberbullying, it is vital that institutions acknowledge potential implications and associated risks.

This study provides a contextual methodology for developing policies that address conduct in virtual environments. The results of this study may benefit current and future higher education policy administrators. By exploring the best practices of policy development, this

study can contribute to a more insightful understanding of the complexities of interpreting legislation in the areas of cyber-harassment in higher education. As such, there are implications for institutions of higher education. As legislatures continue enhancing existing regulation or approve additional legislation, institutions must be cognizant of these changes and respond accordingly. Results of this study may benefit current and future students in higher education. As students continue to embrace technological advances, it is important for students to recognize malevolent behaviors occurring in the virtual environment.

Assumptions

The researcher assumes that:

- Participants' responses are expressed in truth, and shared to the best of their ability.
- Participants have sufficient knowledge of the higher education legal environment.
- Participant responses will sufficiently address the research questions.

Limitations of the Study

Given the qualitative nature of the research, it is important to recognize limitations inherent to the design of the study. This research study required that participants provide an accurate account of their past experiences. As such, the methodology relies heavily on the assumption that participants' memories were shared accurately and honestly. It is also assumed that participants were able to effectively articulate recollections of their personal experiences and were willing to share in the depth and breadth of those experiences (Polkinghorne, 2005). Given that the participants were asked to reflect upon their experiences, it is possible that their recollection or account of those experiences may change in time.

Participants for this study were limited to policy administrators employed at post-secondary institutions of higher education. Other limitations of participation for this study include the following:

- Research with participants was limited to those who have responsibility to significantly influence policy change, specifically those that are authorized to develop or approve proposed policies.
- Research with participants was limited to the geographical boundaries of the continental United States of America.
- Research with participants was limited to individuals employed higher education institutions that offer educational courses in an online format.

Through qualitative inquiry, framed in the form of semi-structured interviews, the participants' experiences were collected. According to DeMarrais (2004), in interview is a "process in which a researcher and participant engage in a conversation focused on questions related to the research" (as cited in Merriam, 2014, p. 87). Finally, it is imperative to recognize researcher bias in the structure of the research and in the analysis of the accounts conveyed by the participants.

Definition of Terms

The following terms are referenced throughout the research, and are defined as follows for consistency and interpretation.

Bullying. Bullying refers to intentional, repeated behavior in which there is a power imbalance between the two parties (Olweus, 2013).

Harassment. Harassment refers to unwelcomed conduct that is based on a protected class including race, color, religion, national origin, age, disability, or sex (U.S. Equal

Employment Opportunity Commission, 2015), where conduct does not have to include "intent to harm, be directed at a specific target, or involve repeated incidents" (U.S. Department of Education, 2015, p. 2). Conduct may include "verbal acts and name-calling, as well as non-verbal behavior, such as graphic and written statements, or conduct that is physically threatening, harmful, or humiliating" (U.S. Department of Education, 2015, p. 15).

Verbal harassment. Verbal harassment refers to unwelcome conduct including name calling, offensive jokes, threats, insults, or mockery (U.S. Equal Employment Opportunity Commission, 2015), "encompassing all offensive speech with regarding sex, disability, race or other classifications" (Reynolds, 2003, p. 1).

Physical harassment. Physical harassment refers to acts "perpetrated against a person's will or where a person is incapable of giving consent" (U.S. Department of Education, 2015, p. 15). Acts may include hitting, spitting, making hand gestures, sexual abuse, and rape (U.S. Department of Education, 2015).

Social harassment. Social harassment refers to covert or social bullying, which includes embarrassment, rumors, and gossip (U.S. Department of Health and Human Services, n.d.).

Cyberbullying. Cyberbullying refers to "any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others" (Tokunaga, 2010, p. 278), that occurs through the use of technological devices, including cell phones and computers (U.S. Department of Health and Human Services, 2013). Conduct can occur through forums including email, text messages, websites, or social media sites (National Centre Against Bullying, n.d.; National Crime Prevention Council, n.d.; U.S. Department of Health and Human Services, 2013). Cyberbullying refers to overt or covert harassment of children or teens.

Cyber-harassment. Cyber-harassment refers to cyberbullying of adults (Gupta, 2008; Vance, 2010).

Cyberstalking. Cyberstalking refers to "the use of electronic communications to stalk another person through repetitive harassing or threatening communication" (Kowalski, Limber, & Agatston, 2012).

Sexual harassment. Sexual harassment refers to sex-based harassment that is "unwelcome conduct of a sexual nature, such as unwelcome sexual advances, requests for sexual favors, and other verbal, nonverbal, of physical conduct of a sexual nature" (U.S. Department of Education, 2015, p. 15).

Gender-based harassment. Gender-based harassment is a form of sex-based harassment and refers to "an individual's actual or perceived sex, including harassment based on gender identity or nonconformity with sex stereotypes, and not necessarily involving conduct of a sexual nature" (U.S. Department of Education, 2015, p. 15).

Sexual violence. Sexual violence is an overt form of sexual harassment that refers to "physical sexual acts perpetrated against a person's will or where a person is incapable of giving consent" (U.S. Department of Education, 2015, p. 15). Acts may include "rape, sexual assault, sexual battery, sexual abuse, and sexual coercion" (U.S. Department of Education, 2015, p. 15).

Title IX coordinator. Title IX coordinator is a designated employee at a post-secondary educational institution, whose responsibility is to develop, implement, and monitor an institution's compliance with Title IX (1972) regulation (U.S. Department of Justice, 2015b).

Summary

Every institution of higher education has a duty to disclose campus safety and security risks and to provide students with reasonable security and protection (Fisher, 1995). Issues of

campus safety are of great concern among University constituents (Westat, Ward, & Mann, 2011). As university operations expand beyond the physical boundaries of a campus and into the virtual environment, higher education administrators are challenged with expanding safety and security protocol. Although no federal law specifically addresses cyber-harassment, institutions have a legal obligation to address all harassment claims, regardless of the location or platform in which the harassing behavior occurs (Ali, 2010).

Institutions are left to their own devices to develop and employ policy statements and sanctions that prohibit or discourage cyber-harassment behaviors. Colleges and universities have addressed bullying within the context of harassment; however, few have included provisions that specifically address cyber-harassment. This qualitative study explored the strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. With the constant growth in online programs and course offerings (Allen & Seaman, 2011, 2013), institutions increasingly must promote a safe learning environment beyond the boundaries of the physical classroom and into the virtual classroom thus the findings of this study will help in furthering that dialogue so that more can be done to establish practices and strategies that will result in safer environments for students.

Chapter 2: Literature Review

Institutions of higher education have incorporated technological advances, with over 86% of postsecondary institutions offering online courses in 2012 (Allen & Seaman, 2013). As jurisdiction extends beyond the boundaries of a physical campuses and into the virtual environment, higher education administrators are challenged with expanding protocol. There are risks and opportunities associated with adopting modern technologies in schools (Beran & Li, 2005; Li, 2006). With the expansion of information and communication technologies, cyberbullying behaviors are causing great concern (Kubiszewski et al., 2015; Willard, 2005). Extensive research has been conducted on school bullying and workplace harassment, however little research has been conducted in the areas of cyber-harassment (Kiriakidis & Kavoura, 2010). Cyber-harassment victimization among college populations varies in range from 10% to 28.7% (Zalaquett & Chatters, 2014).

In the *Dear Colleague Letter* issued in October 2010, the U.S. Department of Education expressed full support toward efforts of individual State Education Authorities in reducing bullying in schools (Ali, 2010). However, legislation developed by State Education Authorities primarily addressed behaviors in K–12. When a student in the K–12 system becomes a legal adult and a student in higher education, the laws that apply vastly change. Most students attending higher education institutions, are over the age of 18, and are considered adults. Federal laws fail to address cyber-harassment, as students transition from adolescence in K–12 and onto adult learners at higher education institutions.

Bullying and Harassment

Bullying is a form of aggression (Kubiszewski et al., 2015) with “certain special characteristics” (Olweus, 2013, p. 756). Bullying can be defined as repeated behavior intended to

harm or disturb an individual, where there is an inequity of power between the offender and the victim (Kowalski & Limber, 2013; Olweus, 2013; Willard, 2005). Olweus (1993) identifies two critical components that differentiate bullying from aggression, where aggression can be described as single act between two individuals of equal power compared to bullying which is described as multiple or repetitive acts occurring between two individuals with an imbalance of power (as cited in Dooley, Pyzalski, & Cross, 2009; Olweus, 2013).

Traditional definitions of bullying have included physical or verbal unwelcomed behaviors (Kowalski & Limber, 2013). More specifically, physical harassment refers to overt physical acts perpetrated against an individual who cannot provide consent (U.S. Department of Education, 2015). Physical acts may include hitting, shoving, spitting, and making hand gestures (Kowalski & Limber, 2007; U.S. Department of Education, 2015; U.S. Department of Health and Human Services, n.d.). Sexual violence is an aggressive and explicit form of sexual harassment that refers to "physical sexual acts perpetrated against a person's will or where a person is incapable of giving consent" (U.S. Department of Education, 2015, p. 15). Acts may include rape, sexual exploitation, and sexual coercion (U.S. Department of Education, 2015).

Verbal harassment refers to unwelcome conduct including name calling, offensive jokes, threats, insults, or mockery (U.S. Equal Employment Opportunity Commission, 2015), "encompassing all offensive speech with regarding sex, disability, race or other classifications" (Reynolds, 2003, p. 1). Verbal harassment includes overt behavior such as taunting or name calling (Kowalski & Limber, 2007), and includes covert or social-bullying behaviors such as embarrassment, rumors, and gossip (U.S. Department of Health and Human Services, n.d.). Sexual harassment refers to sex-based harassment that is such as unsolicited sexual advances or requests for sexual favors (U.S. Department of Education, 2015). Behaviors experienced among

adolescents are typically described as bullying, whereas behaviors experienced by adults are described as harassment (Antoniadou & Kokkinos, 2015; Gupta, 2008; Vance, 2010).

Cyberbullying and Cyber-harassment

There are risks and opportunities associated with adopting modern technologies in schools (Beran & Li, 2005; Li, 2006). With more than 97% of United States adolescence linked to the Internet (Tokunaga, 2010), the use of information and communication technologies has increased in recent years (Li, 2006, 2007). Despite the benefits, the introduction of such technologies provides for a format in which malicious behaviors can occur (Beran & Li, 2005; Francisco et al., 2015). The development and expansion of information and communication technologies, introduced several types of malevolent behaviors (Kubiszewski et al., 2015; Willard, 2005), including "deleterious social interactions such as cyberbullying" (Kubiszewski et al., 2015, p. 49).

Cyberbullying is a new and growing phenomenon, causing concern among students, parents, and professionals in the educational community. Researches have conducted a plethora of studies exploring the prevalence of cyberbullying within educational establishments (Li, 2006, 2007; Patchin & Hinduja, 2006). Reports of cyberbullying among K–12 range from 9% to 42% (Kowalski et al., 2014). Research conducted by Kiriakidis and Kavoura (2010) showed that cyberbullying behaviors increase from middle school to high school. Given this trend, it is logical to conclude that college students experience cyberbullying as well (Crosslin & Golman, 2014; Schenk et al., 2013).

Some cynics conclude that cyber-harassment behaviors are limited to pre-adolescent and adolescent populations and that those types of behaviors cease upon maturity; however, unfortunately, the behavior transcends age (Bullying Statistics, n.d.; What is adult bullying?,

2014). Bridget Roberts-Pittman, assistant professor of counseling at Indiana State University, argued whether there is a distinction between an 18-year-old high school student and an 18-year-old freshman in college (Sicking, 2011). Higher education institutions are addressing this issue head-on by conducting surveys and assessments to assess the degree to which college students experience cyber-harassment. Studies of cyber-harassment among the college aged population range from 10% to 28.7% (Zalaquett & Chatters, 2014).

Studies have indicated that prevalence may be difficult to determine, as reports of cyber-harassment are not consistently reported (Gahagan, Vaterlaus, & Frost, 2015). Kiriakidis and Kavoura (2010) noted differences in reporting rates between age and between gender. Research conducted by Paullet and Pinchot (2014) found that participants reported cyberbullying to a friend, however failed to report to authorities (as cited in Gahagan et al., 2015). College students have expressed that cyberbullying is "childish and not something you communicate with others" (Crosslin & Golman, 2014, p. 16). One research study concluded that college students "underrated their involvement in acts of cyberbullying, whether it was from the perspective of the victim, or aggressor, or one of the observers" (Francisco et al., 2015, p. 178). And in a research study conducted by Crosslin and Golman (2014), 20.7% of participants did not believe that cyber-harassment was even an issue at their institution.

Recently conducted research studies have explored the distinction and degree to which there is overlap between bullying and cyberbullying (Antoniadou & Kokkinos, 2015; Kubiszewski et al., 2015). Those that propose similarity, express that cyberbullying is form of bullying, facilitated through the use of technology (Antoniadou & Kokkinos, 2015). To add to the complexity, cyberbullying definitions vary among researchers (Gahagan et al., 2015; Kubiszewski et al., 2015; Tokunaga, 2010). Definitions of cyberbullying, are fundamentally

derived from definitions of bullying, where conduct is defined as bullying behaviors that are facilitated by information and communication technologies (Kubiszewski et al., 2015). Crosslin and Golman (2014) defines cyberbullying as repeated, unwanted harassment or aggressive behavior conducted through the use of technologies. Besley (2009) defines cyberbullying as "the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others" (as cited by Tokunaga, 2010, p. 278). Patchin and Hinduja (2006) defines cyberbullying as inflicting repeated and intentional harm through text. Olweus (2013) defines cyberbullying as "bullying performed via electronic means such as mobile/cell phones or the internet" (p. 765).

Sacco, Silbaugh, Corredor, Casey, and Doherty (2012) noted that although most state laws provide definitions of bullying behaviors, the definitions vary greatly, and the definitions as outlined in policy do not reference research-based definitions of bullying. Stuart-Cassel, Bell, and Springer (2011) defined bullying as a "repeated pattern of aggressive behavior that involves an imbalance of power and that purposefully inflicts harm on the bullying victim" (p. 1). The research conducted highlights that only eight of the states that address bullying define behaviors similar to definitions used by the U.S. Department of Education; 16 states indicate that the behavior has an intent to harm, and only four states include provisions that address the imbalance of power (Ali, 2010). In all of the policies, the terms *bullying* and *harassment* are used interchangeably to describe the behavior (Stuart-Cassel et al., 2011). The interchangeable use of terminology may be attributed to the following:

> The legislative language used in crafting bullying laws often borrows directly from harassment statutes. This has frequently led to a conflation of terms used to define prohibited conduct, with bullying and harassment often used interchangeably in laws,

> despite their important legal distinctions. Harassment is distinguishable from more general forms of bullying in that it must be motivated by characteristics of the targeted victim. It is generally viewed as a subset of more broadly defined bullying behavior. Harassment also violates federal civil rights laws as a form of unlawful discrimination. (Sacco et al., 2012, p. 6)

In an effort toward identifying a more comprehensive definition of cyberbullying, research conducted by Tokunaga (2010) expressed the need for consistent and operational definitions. Tokunaga (2010) submits the following definition of cyberbullying for consideration: "Cyberbullying is any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others" (p. 278). The definitions are summarized in table 1.

Table 1

Cyberbullying Definitions

Study	Definition
Crosslin and Golman (2014)	Repeated, unwanted harassment or aggressive behavior conducted through the use of technologies
Besley (2009)	"The use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others" (as cited by Tokunaga, 2010, p. 278)
Patchin and Hinduja (2006)	"Willful and repeated harm inflicted through the medium of electronic text" (p. 152)
Olweus (2013)	"Bullying performed via electronic means such as mobile/cell phones or the internet" (p. 521)
Stuart-Cassel et al. (2011)	"Repeated pattern of aggressive behavior that involves an imbalance of power and that purposefully inflicts harm on the bullying victim" (p. 1)
Tokunaga (2010)	"Cyberbullying is any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others" (p. 278)

Where cyberbullying refers to harassment of adolescents and pre-adolescents, facilitated through technology (U.S. Department of Health and Human Services, 2013), cyber-harassment refers to technologically facilitated harassment of adults (Gupta, 2008; Vance, 2010). In a qualitative research study on college students conducted by Crosslin and Golman (2014), with regard to cyberbullying terminology, participants expressed that the term cyberbullying was a misleading term and suggests that "harassment or attack . . . better describe cyberbullying" (Crosslin & Golman, 2014, p. 17).

Like bullying, cyberbullying is characterized as repeated occurrences of behavior, intended to harm or disturb an individual, where there is a disproportionate level of power between the offender and the victim (Patchin & Hinduja, 2006; Sabella, Patchin, & Hinduja, 2013). Although there appears to be quite a number of similarities between bullying and cyberbullying, research indicates clear distinctions for consideration (Antoniadou & Kokkinos, 2015; Kubiszewski et al., 2015).

In traditional bullying, bullying behaviors "generally occur during school hours and cease once a victim returns home" (Tokunaga, 2010, p. 279), whereas cyberbullying transcends geographical restrictions and boundaries. Additionally, cyberbullying can continue online without the presence or participation of the victim (Crosslin & Golman, 2014). Advances in technology communication systems has provided users with mechanisms in which the perpetrator has the option to remain completely anonymous (Kokkinos, Antoniadou, & Markos, 2014). Ultimately, this provides for a situation in which a victim cannot identify their perpetrator. Those proposing divergences in victim profiles and variations of the emotional effects of cyberbullying on both the victim and bully support the theory that cyberbullying is a different phenomenon (Kubiszewski et al., 2015). Additionally, bullying through technologies is

easier and provides a greater return on investment for bullying efforts (Antoniadou & Kokkinos, 2015). Others highlight that cyberbullying provides a forum in which individuals can play the role of victim and bully (Antoniadou & Kokkinos, 2015).

Research conducted by Francisco et al., (2015) found that students "underrated their involvement" (p. 179) in cyberbullying acts. Crosslin and Golman (2014) found in their study of cyber-harassment in higher education, that 20% considered cyber-harassment as a rite-of-passage, undermining the impact that behaviors have on victims. Some dismiss the behavior all together, suggesting that bullying is an inevitable aspect of growing up (Patchin & Hinduja, 2006; Sabella, Patchin, & Hinduja, 2013). As a result of dismissive perspectives regarding cyber-harassing behaviors, studies found that students did not report incidents of cyber-harassment because they "felt helpless, ashamed, self-reliant, [and] worried about the reactions of adults" (Francisco et al., 2015).

Forms of cyberbullying. Willard (2005) identifies several forms of cyberbullying including flaming, harassment, stalking, denigration, impersonation, outing, trickery, and exclusion. These actions can be characterized as either direct or indirect forms of aggression (Francisco et al., 2015). Flaming is a form of aggression described as sending "a brief, heated exchange between two or more individuals" (p. 62) facilitated through information and communication technologies (Kowalski, Limber, & Agatston, 2012). Flaming typically occurs in online chat rooms and discussion boards and are comprised of angry, abusive, or vulgar messages (Kowalski et al., 2012, Tokunaga, 2010; Willard, 2005).

The U.S. Equal Employment Opportunity Commission (2015) specifies that harassment refers to unwelcome conduct that is based upon a protected class such as race, color, religion,

national origin, age, disability, or sex. The Equal Employment Opportunity Commission is responsible for

> enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit (U.S. Equal Employment Opportunity Commission, 2016a, para. 1)

The U.S. Department of Education (2015) expands upon this definition to specify that the conduct does not have to have intent, be repetitive or be directed towards a specific person or group of persons. The definition prescribed by the U.S. Department of Education in 2015, aligns more clearly with the definition of harassment and sexual harassment as defined by the U.S. Equal Employment Opportunity Commission (2016b). Similarly, the U.S. Department of education places the liability on institutions of higher education to respond to and take appropriate action, as the U.S. Equal Employment Opportunity Commission (2015) places the liability upon the employer.

Cyberstalking is the use of technology to “stalk another person through repetitive harassing or threatening communication” (Kowalski, Limber, & Agatston, 2012, p. 1074), which may include behaviors that exhibit excessive intimidation (Li, 2008) or create significant fear (Simmons & Bynum, 2014). A study conducted by Pew Research Center (Duggen, 2014) classifies online stalking as a severe type of harassment. Cyberstalking may be inconspicuousness to the victim in which the perpetrator uses a veil of anonymity to conceal their identity in an effort to spy on another person (Kowalski et al., 2014)

Kubiszewski, Fontaine, Potard, and Auzoult (2015) define denigration as posting "false information, gossip, or rumors . . . on a blog or online social network in order to damage his/her reputation or friendships" (p. 50). Denigration includes sending untrue information to other people (Li, 2008). Online slam books, where students can post harmful and cruel statements about other students on websites, is an example of denigration (Kowalski et al., 2012). Denigration is a form of covert or social-bullying behaviors.

Impersonation is an indirect form of bullying (Francisco et al., 2015). Impersonation includes identity theft (Kokkinos, Antoniadou, & Markos, 2014), where the perpetrator poses as the victim, and sends or posts harmful cruel statements (Kowalski et al., 2012). Impersonation includes breaking into an email account (Kiriakidis & Kavoura, 2010) and the "creation of a web page or blog in which the creator assumes the identity of another person or . . . the knowing impersonation of another person as the author of posted content or messages" (Stuart-Cassel et al., 2011, p. 151).

According to Siegle (2010) outing is described as disclosing someone's confidential information or sharing embarrassing information or photos on the Internet. Outing includes forwarding private information or images (Kowalski et al., 2012; Li, 2008). Trickery is described as "tricking someone into revealing personal information about themselves and then sharing the information with others" (Kowalski et al., 2012, p. 65). An additional indirect form of bullying is exclusion, where an individual or group intentionally excludes an individual from an online group (Siegle, 2010; Willard, 2005). Flaming, harassment, stalking, denigration, impersonation, outing, trickery, and exclusion are all forms of cyberbullying, outlined in Table 2 (Willard, 2005).

Cyberbullying is conducted through information and communication technologies by means of emails, text messages, instant messaging, online social networking sites, chat rooms, or blogs (Kowalski & Limber, 2007, 2013; Kubiszewski et al., 2015; Willard, 2005). Smith et al., (2008) has identified seven distinctive ways cyberbullying behaviors are conducted including "text messages, picture/video clips; phone calls; emails; chat rooms; instant messaging and via websites" (as cited in Francisco et al., 2015). Electronic mail, or more commonly referred to as emails, are a frequently leveraged technological platform for cyberbullying activities due to accessibility and ease of use (Kowalski et al., 2012). Ellison and Boyd (2013) indicate that most cyberbullying occurs through social networking sites including Facebook and Twitter (Francisco et al., 2015).

Defined by the Federal Bureau of Investigation (2006), social networking sites are "websites that encourage people to post profiles of themselves—complete with pictures, interests, and even journals—so they can meet like-minded friends" (as cited by Kowalski et al., 2012, p. 72). It is reported that over 89% of young adults in 2014 used social network sites (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015). Facebook is identified as the most commonly used social media site, with 87% among users aged 18 to 29 surveyed (Duggan et al., 2015). However, young adults also report using platforms such as Instagram and Twitter (Gahagan, Vaterlaus, & Frost, 2015). Through the use of technologies, cyberbullying surpasses "the boundaries of time, since it is infinitely present in virtual space . . . and goes beyond the boundaries of personal and physical space" (Francisco et al., 2015, p. 169).

Table 2

Forms of Cyberbullying

Bullying	Definition
Flaming	A "brief, heated exchange between two or more individuals" facilitated through information and communication technologies (Kowalski, Limber, & Agatston, 2012, p. 62).
Harassment	Harassment refers to unwelcome conduct that is based upon a protected class such as race, color, religion, national origin, age, disability, or sex (U.S. Equal Employment Opportunity Commission, 2015). Repeated, unwanted harassment or aggressive behavior conducted through the use of technologies (Crosslin & Golman, 2014).
Stalking	The use of technology to "stalk another person through repetitive harassing or threatening communication" (Kowalski, Limber, & Agatston, 2012, p. 1074).
Denigration	Posting "false information, gossip, or rumors . . . on a blog or online social network in order to damage his/her reputation or friendships" (Kubiszewski, Fontaine, Potard, & Auzoult, 2015, p. 50).
Impersonation	Impersonation includes identity theft (Kokkinos, Antoniadou, & Markos, 2014), where the perpetrator poses as the victim, and sends or posts harmful cruel statements (Kowalski et al., 2012).
Outing	"Sharing someone's secrets or embarrassing information or images online" (Siegle, 2010, p. 15), which includes forwarding private information or images (Kowalski et al., 2012; Li, 2008).
Trickery	"Tricking someone into revealing personal information about themselves and then sharing the information with others" (Kowalski et al., 2012, p. 65)
Exclusion	An individual or group intentionally excludes an individual from an online group (Siegle, 2010; Willard, 2005).

Note. Forms of cyberbullying (Willard, 2005)

Cyberbullying motivations. Rafferty and VanderVen (2014) identified that cyberbullies are motivated by cyber-sanctioning, power struggles, or for entertainment purposes (as cited in Gahagan et al., 2015). Cyber-sanctioning occurs when a victim reacts to bullying behaviors by replicating the same behaviors, with the intent of shaming the bully for their actions (Gahagan et al., 2015). In general, cyberbullies are individuals who intend to impose harm or cause distress (Tokunaga, 2010). Although it is reported that most cyberbullies intend to cause harm, not all acts classified as cyberbullying intend to cause harm (Antoniadou & Kokkinos, 2015). From the

perspective of cyberbullies, “38% said that cyberbullying was made for fun, 25% said retaliation, and 6% said they did it because they feel bad about themselves” (Kiriakidis & Kavoura, 2010, p. 91).

Psychological and emotional effects of cyberbullying. Cyberbullying victims reported feelings of “sadness, anger, fear and loss of hope—feelings that influence both concentration and academic achievement” (Francisco et al., 2015, p. 169) Additionally, victims may feel emotional distress, anxiety, and isolation (Crosslin & Golman, 2014). Research conducted by Schenk et al., (2013) reported victims of cyberbullying show higher rates of depression, paranoia, and were more likely to contemplate or attempt suicide. In response to cyber-bullying, victims resort to a variety of coping mechanisms. According to Smith et al., (2008) common mechanisms that students’ employ includes blocking contacts, informing officials, and asking someone for help (as cited by Francisco et al., 2015).

Psychological and emotional impacts are not limited to victims of cyberbullying. Recent studies have shown repercussions to cyberbullying victims, bystanders and the bullies themselves (Schenk et al., 2013). The effects go beyond the parties involved. Kiriakidis and Kavoura (2010) argue that “cyberbullying could be considered a threat to youth, schools, families, and communities, which has to be dealt with from a preventive public health approach” (p. 86). With cyberbullying occurring through social networking sites, the exposure to bystanders increases significantly (Francisco et al., 2015).

Recent studies have shown repercussions to cyberbullying victims, bystanders, and the bullies themselves (Schenk et al., 2013). Cyberbullying is a unique form of bullying in which bystanders have the option to “respond to bullying by remaining an outsider, assisting or reinforcing the bully, or supporting or defending the victim” (Gahagan, Vaterlaus, & Frost, 2015,

p. 1098). It is suggested that social media network sites that allow for anonymity, have increased rates of cyberbullying activity.

Cyberbullying has ascended to the forefront of the public agenda after unfortunate events broadcasted onto the media (Tokunaga, 2010). The unfortunate suicide of Tyler Clementi, an 18-year-old at Rutgers University in New Jersey, was the net effect of cyberbullying (Crosslin & Golman, 2014; Foderaro, 2010). Tyler's roommate live streamed the sexual encounter on the Internet and invited others to view it. Tyler learned of this after viewing his roommate's social media feed, and subsequently decided to end his life by jumping off of the George Washington Bridge (Foderaro, 2010; The Tyler Clementi Foundation, n.d.). Psychological and emotional impacts are not limited to victims of cyberbullying. Recent studies have shown repercussions to cyberbullying victims, bystanders and the bullies themselves (Schenk et al., 2013).

Federal and State law

The U.S. Department of Education encouraged State Education Authorities to develop policies in an effort to reduce bullying behaviors in schools (Ali, 2010). To help understand the current state of bullying laws, the U.S. Department of Education (Stuart-Cassel et al., 2011) conducted an analysis of state bullying legislation and policies enforced by State Education Authorities. This study reviewed State Education Authorities' bullying policies and legislation, state definitions of harassment and bullying, as well as sanctions for prohibited behavior. Although the study focused primarily on youth bullying in the K–12 school systems, many of the key findings and recommendations are applicable to institutions of higher education. The report cited that only 46 states had bullying laws, of which 36 states included provisions that address bullying through technological means (Stuart-Cassel et al., 2011).

Despite the fact that there are currently few laws addressing virtual conduct, regulations are quickly changing and advancing in their response. State legislation continues to expand and evolve, and as of July 2013, all but one state, Montana, has enacted bullying laws (Patchin & Hinduja, 2013). Of the 49 states that have bullying laws, 48 include provisions that address bullying through technological platforms, of which 20 specifically state *cyberbullying* within the legislation (Hauck, 2014). State legislation regarding bullying and cyberbullying behaviors in schools are limited in that they apply primarily to K–12 education systems. These policies do not automatically apply to colleges and universities operating in that particular state.

When a student in the K–12 system becomes a legal adult and a student in higher education, the laws that apply change vastly. State legislative laws govern the behaviors of adults, in which states vary in definition and application of said laws, where some states include specific language addressing cyber-harassment, while others have adopted stand-alone cyber-harassment statutes. Of the 50 states, only 38 have enacted legislation that is specific to cyber-stalking, and 41 have legislation that specifically addresses cyber-harassment (National Conference of State Legislatures, 2015).

One of the unique variations in state policies is that some policies clearly address regional jurisdiction. Sacco et al.'s (2012) research report acknowledges that there are variances in whether the behavior occurs off-campus. Of the states that have bullying provisions, an alarming 14 of them limit their jurisdiction to behaviors that transpire on campus or at off campus school-related functions, and seven states extend their jurisdiction to include behaviors that occur on school-owned technology. The varying standards and vagueness with which State Education Authorities define behaviors and jurisdictions result in inconsistent standards, and ultimately, penalties, as educational institutions struggle to operationalize legislation.

The processes and procedures as dictated by State Education Authorities differ vastly in expectation and level of responsibility from state to state. Only 32 states require that the institution perform an investigation, while only three states highly encourage it (Sacco et al., 2012). The remaining states neglect to address the institution's responsibility in investigating claims of harassment and bullying. In 34 of the states, the policy outlines the disciplinary consequence as a requirement, while two of the states encourage remediation efforts (Stuart-Cassel et al., 2011). The disciplinary actions as described in the policies vary between the states; however, some states specify the sanctions to include suspension and expulsion for those students that participate in bullying and harassing behaviors.

When addressing if harassment and bullying behaviors constitute a criminal act, only nine states require that school administrators report the incident to law enforcement (Stuart-Cassel et al., 2011). Stuart-Cassel et al. (2011) stated that:

> Recent state legislation and policy addressing school bullying has emphasized an expanded role for law enforcement and the criminal justice system in managing bullying on school campuses. Though historically, authority over youth bullying has fallen almost exclusively under the purview of school systems, legislation governing the consequences for bullying behavior reflects a recent trend toward treating the most serious forms of bullying as criminal conduct that should be handled through the criminal justice system. . . . An increasing number of states also have introduced bullying provisions into their criminal and juvenile justice codes. (p. 19)

As the discussion regarding bullying in America's education system continues to draw national attention, legislatures are making strides to address bullying behaviors. States are continuously

enhancing state legislation and are motivated as social interest groups, media, and school education systems encourage change.

Criminal justice system. State bullying policies are limited in their applicability to K–12 institutions, as authorized by individual State Education Authorities, which vary from state to state. An institution has a responsibility to "take immediate and appropriate steps to investigate or otherwise determine what occurred" (U.S. Department of Education, 2014d, p. 2). Regardless of whether the event triggers a criminal investigation, institutions have the responsibility to investigate independently of the criminal justice process (Ali, 2011), thus requiring institutions of higher education to conduct due process proceedings in parallel with a criminal investigation.

The criminal system may vary depending on the city, county, state, or federal jurisdiction; however, there are two main systems. The state criminal justice system serves crimes that occur within state boundaries (Hill, 2007), whereas the federal criminal justice system addresses crimes that are committed on federal property or in the event a crime occurs in two or more states (National Center for Victims of Crime, 2012). The California Criminal Justice System has four major components: (a) the crime, which may include a felony, misdemeanor, or infraction; (b) the arrest made by law enforcement; (c) the prosecution of the case; and (d) the detention and supervision of offenders (Hill, 2007).

The criminal justice system is primarily based on criminal sentencing law, which defines three major types of offenses for which a person may be prosecuted: infractions, misdemeanors, and felonies (Hill, 2007; San Diego County District Attorney, n.d.; Shouse Law Group, n.d.). Legislative bodies dictate definitions of crime, including state legislation such as the California Penal Code; through local ordinance; or through California Vehicle Code. A felony is the most serious crime classification, in which a convicted individual may be sentenced to state prison. A

misdemeanor is a less serious offense that may include crimes such as shoplifting, assault, and driving under the influence.

Although a misdemeanor is less serious than a felony, these criminal acts may result in incarceration in a county jail, probation, and fines. It is important to note that misdemeanors may be removed from an individual's record after serving jail time or through probationary processes. An infraction is the least serious of all of the offenses and is generally punishable by a fine. Examples of infractions include traffic violations or speeding tickets (Hill, 2007; San Diego County District Attorney, n.d.).

Title IX of the Department of Education and Office for Civil Rights

The U.S. Department of Education (n.d.) plays an important role in providing leadership and oversight to ensure that U.S. school systems are effective. In addition to governing the quality of education that is provided by institutions of learning, the U.S. Department of Education provides clear direction on the administrative responsibility of the institutions by broadening their jurisdiction to include: establishing policies regarding educational funding, distributing funds, and oversight for appropriate use; collecting data and overseeing research efforts; identifying major issues in education and focusing national efforts; and enforcing federal laws prohibiting discrimination for educational programs that utilize federal funding. Title IX of the Education Amendments of 1972 protects college and university students and employees from "all forms of sex discrimination, including discrimination based on gender identity or failure to conform to stereotypical notions of masculinity or femininity" (U.S. Department of Education, 2015, p. 1).

The U.S. Department of Education's OCR "prohibits discrimination on the basis of sex in any federally funded education program or activity" (U.S. Department of Justice, 2015a, para. 1).

Sexual assault, harassment, and bullying behaviors fall under the purview of Title IX guidance. In the 2010 *Dear Colleague Letter* by Russlynn Ali, Assistant Secretary for Civil Rights, the Department of Education expressed full support toward efforts of individual State Education Authorities in reducing bullying in schools. Title IX has issued guidance regarding sexual harassment and sexual violence. However, this guidance is limited in its ability to specifically address cyberbullying. Laws that address cyberbullying-type behaviors are applied in the context of harassment, stalking, libel, campus sexual violence, or workplace sexual harassment. The letter, however, serves as a reminder that, "some student misconduct that falls under a school's anti-bullying policy also may trigger responsibilities under one or more of the federal antidiscrimination laws enforced by the Department's Office for Civil Rights" (p. 1).

A *Dear Colleague Letter* is a letter issued by a legislative body that addresses an administrative matter. The U.S. Department of Education (2011) "has determined that this *Dear Colleague Letter* is a significant guidance document under the Office of Management and Budget's Final Bulletin for Agency Good Guidance Practices" (as cited in Ali, 2011, p. 1). The *Dear Colleague Letter* of April 2011 provides guidance with regard to an educational institution's role and responsibility in the event of sexual violence (Ali, 2011). The *Letter* outlines an institution's responsibility in supporting criminal investigations and investigating sexual harassment and sexual assault, also describing proactive measures an institution must employ in an effort to prevent and mitigate behaviors. Most importantly, the *Letter* provides clarity regarding the relationship between Title IX and the Clery Act (1998) as it relates to institutional responsibility regarding complainants' and perpetrators' rights, and potential sanctions a perpetrator may face. Institutions are obligated to take immediate action and respond accordingly (Ali, 2010). If it has been determined that a discriminatory act has occurred, the

institution must take "prompt and effective steps reasonably calculated to end the harassment, eliminate the hostile environment, prevent the harassment from recurring, and, as appropriate, remedy its effects" (U.S. Department of Education, 2015, p. 15). Additionally, institutions must take appropriate measures to ensure the protection of the complainant (Ali, 2011). Although many of the processes and procedures specifically address extreme cases of sexual violence, the processes and procedures outlined apply to all cases with regard to gender discrimination, including harassment and bullying.

An institution has a responsibility to take appropriate steps to investigate regardless if the event has triggered a criminal (U.S. Department of Education, 2014d). During an investigation, to be consistent with OCR guidelines, the institution must use the preponderance of evidence standard in its administrative hearings (Ali, 2011). The *preponderance evidence standard of proof* has been met if the event was more likely to be true than not (Cornell University Law School, n.d.-a), which is less stringent than the *clear and convincing standard* or the *beyond a reasonable doubt standard* typically used in state or federal proceedings. As a result, there may be a situation in which the alleged may be found guilty of harassment in a college or university investigation under Title IX, but may not be found guilty through the federal or state judicial system.

In 2014, the U.S. Department of Education came to a resolution agreement with Princeton University, which under the OCR, found Princeton in violation of Title IX legislation (U.S. Department of Education, 2014b). The U.S. Department of Education OCR (n.d.) highlighted that Princeton violated the rights of rape victims by using a standard of proof that was higher than what was prescribed under Title IX regulation, which requires a preponderance of evidence standard of proof. In meeting compliance standards, Catherine E. Lhamon, Assistant

Secretary for Civil Rights, commented, "I applaud Princeton University for its commitment to ensuring a community-wide culture of prevention, support, and safety, for its students, staff, and community . . . We look forward to continuing to work cooperatively with Princeton to implement this agreement" (U.S. Department of Education, 2014b, para. 1).

The OCR does not provide a single solution for addressing bullying behaviors, but rather offers guidance for institutions to ensure they employ efforts that prevent and address bullying. In the August 20, 2013, *Dear Colleague Letter*, Musgrove and Yudin (2013) stated that bullying cannot be tolerated in our educational institutions and that "every effort should be made to structure environments and provide supports to students and staff so that bullying does not occur" (p. 1). Although no federal law specifically addresses cyber-harassment, institutions have a legal obligation to address all harassment claims, regardless of the location or forum in which the harassing behavior occurs. Although the Clery Act (1998) specifies what is reportable, it does not include harassing behaviors as a reportable category. This does not negate the obligation that institutions may have in providing appropriate responses, accommodations, or notifications as mandated by Clery Act policy provisions.

The U.S. Department of Education has the authority to suspend an institution from participating in Federal Student Financial Aid programs (U.S. Department of Education, 2015). Legislative changes made to the Code of Federal Regulation increased Clery Act violations from $27,500 to $35,500 per infraction (2012). In 2013, the U.S. Department of Education imposed eight fines, totaling $1,455,000 (Lacher & Ramos, 2014), including $165,000 to Yale University (Sander, 2012), and $275,000 to Lincoln University of Missouri (Lipka, 2013). The goal of the OCR Title IX investigations is to "ensure that the campus is in compliance with federal law, which demands that students are not denied the ability to participate fully in educational and

other opportunities due to sex" (U.S. Department of Education, 2014a, para. 4) . As of October 2014, 85 colleges and universities were under Title IX sexual violence violation investigations (U.S. Department of Education, 2014a).

Despite the volatile legal environment governing gender discrimination and harassment, institutions have responded favorably by expanding upon federal, state, and agency regulation mandates. Institutions have opted to eliminate the statute of limitations for reporting sexual offenses at their respective institution, and increased student and employee training requirements beyond legislative guidance in the areas of sexual harassment and assault (Grasgreen, 2012). The government is not alone in expressing the need to address campus safety and security; many active nonprofit organizations are focused on increasing awareness, providing resources, and supporting the effort to decrease campus crime and violence. Organizations such as Students Active for Ending Rape (SAFER), Promoting Awareness Victim Empowerment (PAVE), Sexual Harassment & Assault Prevention Education (SHAPE), and the Clery Center for Security on Campus have supported these efforts through education, awareness, and research.

In an effort to reiterate institutional obligations under Title IX, the U.S. Department of Education issued a *Dear Colleague Letter* on April 24, 2015, reminding institutions participating in Federal financial assistance programs, that they must "designate at least one employee to coordinate their efforts to comply with and carry out their responsibilities under Title IX of the Education Amendments of 1972 . . . These designated employees are generally referred to as Title IX Coordinators" (Lhamon, 2015a, p. 1). Title IX coordinator is a designated employee at a post-secondary educational institution, whose responsibility is to develop, implement, and monitor an institution's compliance with Title IX (1972) regulation. The *Letter* expands upon the institutions' responsibility to "provide Title IX Coordinators with the appropriate authority and

support necessary for them to carry out their duties . . . to help their institutions comply with Title IX" (p. 1). To express the importance of the Title IX Coordinator position, the *Dear Colleague Letter* referenced a *Dear Coordinator letter* specifically directed to Title IX Coordinators (Lhamon, 2015b). In that letter, the Assistant Secretary of Civil Rights expressed gratitude and support towards Title IX Coordinators, further noting that they are essential to upholding the law. Institutions that fail to comply with regulatory guidance face consequences that may include loss of participation in Federal Financial Aid programs, fines and sanctions, loss of accreditation, and potential impact to reputation and enrollment.

Jeanne Clery Disclosure of Campus Security Policy and Crime Statistics Act

After their daughter was raped and murdered in her residence hall at Lehigh University in Pennsylvania in 1986, Howard and Connie Clery advocated relentlessly for institutional responsibility for student safety (Carter, 2014; Patterson, 2011). Jeanne Clery's parents advocated for laws requiring the disclosure of campus crime, ultimately fueling the national debate stressing the need for colleges and universities to expand upon their role and responsibility for students. State legislators in Pennsylvania responded, and as a result enacted the College and Security Information Act of (1988), requiring colleges and universities to provide students and employees with information related to crime statistics and security measures, granting powers to the State Board of Education, and providing for penalties.

Two years later, the Federal government enacted the Student Right-to-know and Campus Security Act (1990). Signed into law by President George H.W. Bush as part of the Higher Education Act of 1965, the Student Right-to-know and Campus Security Act (1990) required all higher education institutions to prioritize student welfare and address campus safety (Carter, 2014; Patterson, 2011). The Jeanne Clery disclosure of Campus Security Policy and Campus

Crime Statistics Act (1998), named in memory of Jeanne Clery, requires public and private institutions that participate in Federal Financial Aid programs to disclose crime statistics and safety policies annually (Carter, 2014; Clery Center for Security On Campus, 2012; Stuart-Cassel et al., 2011).

20 U.S.C. Section 1092(f)(8) of the Student Right-to-know and Campus Security Act of 1990, more commonly referred to as the Clery Act (American Council on Education, 2012), requires compliance from higher education in a variety of areas. Requirements include (a) annual disclosure of crime statistics, (b) issuance of timely warnings to the campus community regarding Clery Act crimes, (c) assurance that all campuses have emergency response notification plans and testing policies, and (d) maintain and uphold policies and procedures addressing missing students, harassment, and sexual misconduct (Clery Center for Security On Campus, 2012). State and federal legislators clearly addressed the significance of campus safety and security risks by adopting a series of laws expanding the provisions of the Clery Act. These provisions include a variety of amendments and additional legislation altering the original Act, including the Victims of Trafficking Protection Act (2000), the Campus Sex Crimes Prevention Act (2000), and the Final Regulations of the Violence Against Women Act (2014).

In 1992 and again amended in 1998, the Campus Sexual Assault Victims' Bill of Rights was introduced, amending the Clery Act (1998), requiring schools to develop prevention policies and provide certain guarantees to victims. The Campus Sexual Assault Victims' Bill of Rights (1998) required institutions to provide information to students, including where to report an offense, the right to notify law enforcement, information regarding counseling and mental health support, options for changing academic and living situations, options for having support during disciplinary proceedings, and the right to be informed of proceeding outcomes (Carter, 2014).

Institutions vary to the degree in which they comply with Clery Act mandates (National Institute of Justice, 2010).

After filing a suit against Lehigh University the family applied the settlement to launch the advocacy and education group Security on Campus, commonly known as the Clery Center for Security on Campus (Patterson, 2011). The Clery Center provides trainings for colleges and universities, advocates for victims' rights, and campaigns for policy initiatives (Clery Center for Security On Campus, 2012). The Clerys decided to send Jeanne to Lehigh University rather than Tulane University, thinking that Lehigh was a safer alternative in light of a recent murder on Tulane's campus. Ironically, it was later discovered that there had been 38 violent crimes on Lehigh University's campus in the three years prior to Jeanne Clery's death (Patterson, 2011).

Provisions of the Clery Act (1998) require that institutions disclose crime statistics on an Annual Security Report (ASR), which outlines Clery reportable crimes, maintains a public crime log, provides timely warnings to the campus community regarding immediate or ongoing threats, and outlines institutional response requirements for victims and the alleged perpetrator (Stuart-Cassel et al., 2011). Clery Act reportable crimes can be classified into seven major categories as follows:

1. Criminal homicide including murder, non-negligent manslaughter, and negligent manslaughter
2. Sex offenses including forcible and non-forcible offenses
3. Robbery
4. Aggravated assault
5. Burglary, where: (a) there is evidence of unlawful entry (trespass), which may be either forcible or not involve force, (b) unlawful entry must be of a structure—having

four walls, a roof, and a door; or (c) there is evidence that the entry was made in order to commit a felony or theft.

6. Motor vehicle theft
7. Arson

Universities are also required to report statistics for arrests or referrals for campus disciplinary action for liquor law violations, drug law violations, and illegal weapons possession. Additionally, hate crimes involving larceny or theft; simple assault; intimidation; or destruction, damage, or vandalism of property must be reported. (Clery Center for Security on Campus, 2012; Stuart-Cassel et al., 2011).

The Clery Act requires that an institution must disclose statistics for reportable Clery crimes that occur: (a) on campus, (b) on public property neighboring the campus, and (c) on non-campus property that the institution wholly owns or controls (Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, 1998). The U.S. Department of Education developed the *Handbook for Campus Safety and Security Reporting*, which "takes you step-by-step along the path to compliance and explains what the regulations mean and what they require of your institution" (Westat, Ward, & Mann, 2011, p. 3). In addition to reportable crimes, Clery regulations (1998) require that institutions ensure that all campuses have emergency response notification plans and testing policies, and have policies and procedures that address missing students, harassment, and sexual misconduct (Clery Center for Security On Campus, 2012).

Although the Clery Act (1998) specifically outlines which crimes to report on the annual security report based on a specified geographical location as defined in the *Handbook for Campus Safety and Security Reporting* (Westat et al., 2011), this does not negate the institutional

obligatory response of the institution should a crime be committed against a student beyond the boundaries of the school's physical jurisdiction. Higher education institutions are required to provide victims with reasonable accommodations, which may include changing of housing arrangements or academic schedules. Should the accused be a student at that same institution, the accused may be subject to disciplinary hearings and institutional sanctions in addition to any disciplinary actions allowed by federal and state legislation.

In a study conducted by Karjane, Fisher, and Cullen (2005), 37% of higher education institutions surveyed fully complied with the provisions of the Clery Act (1998). Despite federal mandates, there is still much confusion in the interpretation and compliance with the provisions outlined in the legislation. Although most institutions submit the annual security report to the U.S. Department of Education, as required by the Clery Act, over 32% of institutions do not comply with all of the required written policy provisions that address the preservation of evidence and victim and alleged rights and responsibilities (Students Active for Ending Rape & V-Day, 2013).

Violence Against Women Act

Federal, state, and agency legislation express the need to educate about and prevent sexual violence against women, more specifically focusing on sexual violence against college women (American Council on Education, 2012; National Institute of Justice, 2010; Obama, 2014; U.S. Department of Justice, 2000). As a strategy to educate the high risk population of college women, the government has mandated educational programs, enforced regulations through audit and sanctions, and invested funding into addressing sex crimes on campus (Krebs et al., 2007; National Victim Center, 1992). In 1994, the United States Congress passed the Violence Against Women Act (VAWA), as part of the Violent Crime Control and Law

Enforcement Act (1994). VAWA (1994) was designed to decrease violence against women and address factors related to sexual violence including domestic violence, stalking, sexual assault, and victim services. Additionally, the VAWA allocated significant financial and technical support to state and local governments, nonprofits, and universities (U.S. Department of Justice, 2015a). The Campus Sexual Violence Elimination Act (2011), more commonly referred to as the SaVE Act, was introduced to the 112th Congress by U.S. Senator Robert Casey and House Representative Caroline Maloney.

The proposed act expanded the role that higher education played in the prevention of and education about sexual violence on college campuses. The SaVE Act sought to address the sexual violence women face on college and university campuses, where it was reported that approximately 20–25% of female students experienced rape or attempted rape (Clery Center for Security On Campus, 2012). When it was not adopted, the provisions outlined in the SaVE Act were included as a component that would enhance the Reauthorization of the Violence Against Women Act (2013). Section 304 of VAWA (2014), titled the Campus Sexual Violence Elimination Act, includes the provisions proposed in the Campus SaVE Act. Adoption of section 304 (Violence Against Women Reauthorization Act, 2013) amended the Higher Education Act of 1965 and the Campus Security Act of 1990, enhanced Title IX guidance as issued by the U.S. Department of Education ORC, and codified aspects of the *Dear Colleague Letter* of April 2011 (Ali, 2011).

Although the Violence Against Women Reauthorization Act (2013) was signed into law by President Barack Obama on March 7, 2013, through the negotiated rulemaking process, higher education institutions would not be responsible for compliance with the provisions outlined in section 304 until July 1, 2015. The Negotiated Rulemaking Act (1990) provides for a

framework that offers agencies an alternative procedure that moves the rule from proposal and into law (Langbein & Kerwin, 2000). Langbein and Kerwin (2000) described the rulemaking process in that negotiated rulemaking "uses an advisory committee, comprising representatives from the rule-making agency and affected entities—including relevant industries and professional associations, public interest groups, and state and local officials—to draft the rule that is to be proposed by the agency" (p. 599). This advisory committee was essential in understanding the implications that section 304 had on institutions of higher education. Until the legislation goes into effect, institutions are expected to make a good-faith effort to comply (U.S. Department of Education, 2014d). Section 304 of the Violence Against Women Reauthorization Act (2013) changed existing regulatory requirements and imposed new obligations with respect to reporting requirements, institutional procedural responses to complainants, and educational programs for students and employees.

Section 304 of the Violence Against Women Act Reauthorization (2014), as endorsed by the U.S. Department of Education, expanded upon the Clery crime statistics categories that institutions must publish in their annual security report, clearly addressed institutions' obligations in implementing provisions for victims' rights, required institutions to disclose policies that outline conduct proceedings, and mandated institutions provide educational programs that specifically address violence against women (United Educators, 2014). Under Section 304 of the Violence Against Women Act Reauthorization, colleges and universities must provide victims with information on obtaining protection orders; information regarding confidentiality when reporting; written notification for available services including mental health professionals, victim advocacy, and legal assistance; and written notification regarding victims' rights to change academic or living situations.

In addition to Clery Act (1998) crimes, the Section 304 of the Violence Against Women Reauthorization Act (2013) expanded upon the Clery crime categories to include dating violence, domestic violence, and stalking. Additionally, new categories of bias were expanded for Clery reportable crimes to include gender identification and national origin under hate crimes. The new requirements imposed by Section 304 require a training for all new students and new employees that includes definitions of consent, definition of offenses within applicable jurisdiction, bystander intervention options, and recognition of signs of abusive behavior. Additionally, the regulation requires that institutions provide an ongoing prevention and awareness program for students and employees (Violence Against Women Act; Final Rule, 2014). The new requirements imposed by the Section 304 also require the following modifications to be made to each institution's Annual Safety and Security Report:

- Statistics on domestic violence, dating violence, and stalking
- Include national origin and gender identity as hate crime categories
- Policy statement indicating that the institution will use a preponderance of the evidence standard as the standard of proof for Title IX violations (Ali, 2011)
- Policy statement that outlines a "victim's option to, or not too, notify and seek assistance from law enforcement and campus authorities and victims' rights and institutional responsibilities regarding judicial no-contact, restraining, or protective orders" (American Council on Education, 2013, p. 1)
- Policy statement describing student discipline proceedings
- Policy statement addressing victim confidentiality

CampusClarity (2013), a division of LawRoom, a compliance training organization, has expressed their interpretation of the legislation to address the requirements for students strictly

enrolled in online learning environments. A narrow exemption to the Clery Act reporting requirements exists for schools that only offer distance education programs, whereas any school whose students go to a physical location, whether to enroll, seek guidance, study, work, or intern, must comply with the Campus SaVE Act (2014) as part of their annual Clery Act reporting (Westat et al., 2011). CampusClarity elaborates this interpretation of the legislation, stating that if any segment of the student population goes to a physical location for services, such as enrollment or to study, the exception to this requirement will not apply to the students that are 100% distance learners, and that all enrolled students are required to comply. The intent of campus safety and security legislation is to address conduct happening on traditional brick and mortar campuses; however, those that operate strictly distance education programs, hybrid programs, or service primarily part-time students may find themselves challenged with applying the intent of the legislation.

Case Law

In addition to fines, institutions may be forced to deal with lawsuits brought about by victims of sexual assault (Kingkade, 2013). Recent court cases are setting precedents for obligatory institutional response and potential penalties for lack thereof; conversely, institutions are left to their own devices to employ and develop policy statements and sanctions that prohibit or discourage cyber-harassment behaviors. With bullying harassment regulation continuously evolving, it is vital for higher educational institutions to mitigate unwelcome conduct proactively, and to respond appropriately and effectively should misconduct occur. As the legal and political environment regarding bullying and cyberbullying behaviors continues to evolve, colleges and universities are challenged with administering policies and procedures that address misconduct in both physical and virtual environments.

Recent lawsuits are setting precedents for what is required of higher education administration in areas where legislation has failed to specifically address virtual conduct. Higher education institutions are legally responsible for addressing alleged violations of conduct at a standard of proof that is more conservative than that imposed through legal proceedings (U.S. Department of Justice, 2015a). In a recent court case, Carolyn Luby et al. versus the University of Connecticut, Luby, a student at the University, reported that she was harassed online as a result of making public statements regarding the university. The courts determined that the university failed to respond appropriately as required by Title IX. As a result, Luby was awarded a settlement in the amount of $25,000 (Luby et al. v. University of Connecticut, 2013). Although no federal law specifically addresses cyber-harassment, institutions have a legal obligation to address all harassment claims, regardless of the location or platform in which the harassing behavior occurs.

Victims from both sides of the process are seeking refuge in the legal system. As institutions are required to conduct internal investigations and adjudicate at a *preponderance of the evidence* standard, which may result in sanctioning, alleged offenders are filing suit against the institution in the event of mishandled adjudication processes and fair sanctioning. In a recent court case, John Doe versus the University of Colorado, a male student was suspended in connection with a campus sexual assault case. John Doe's attorneys argued that the university's administrators denied him due process, and that he was presumed guilty. John Doe settled in the amount of $15,000 dollars (DeSantis, 2015).

University Risk, Response, and Responsibility

Institutions are limited in their ability to influence federal, state, and legislative mandates. As a result, changes in legislation solicit a reactionary response, and institutions must face the

challenge of interpreting the legislation, with the responsibility for developing appropriate plans for effective and efficient implementation. As awareness of bullying increases, legislatures have responded accordingly. In a White House Memorandum, President Barack Obama (2014) stated that "although schools have made progress in addressing rape and sexual assault, more needs to be done to ensure safe, secure environments for students of higher education" (para. 1).

Policy. In a research study conducted by Crossline and Golman, the findings suggest that institutions develop guidelines for handling reports of cyber-harassment (2014). A variety of organizations provide supplemental guidance on the implementation and execution of prevention and mitigation programs; however, the effects of such programs are not meeting satisfactory expectations (Black et al., 2011; Jozkowski, Henry, & Sturm, 2014; Karjane et al., 2005; Krebs et al., 2007; U.S. Department of Justice, 2000).

Institutions should incorporate control mechanisms that actively monitor the effectiveness of such programs (Jozkowski et al., 2014). In a study conducted by Kokkinos, Antoniadou, and Markos (2014), it is recommended that universities "aim at the prevention of the incidents through proper ICT [information communication technologies] use, by the inclusion of proper online social conduct . . . and the thorough expression of the institution's expectations" (p. 212).

Willard (2005) proposes a clear and well communicated policy. A clearly written policy describes an institution's program objectives and addresses "knowledge (cognitive), skill (behavioral), and attitude (affective)" (Lawson, 2008, p. 234)—key foundational aspects of effective learning outcomes. In the referenced enclosure of the August 2013 *Dear Colleague Letter*, Musgrove and Yudin (2013) recommended that for effective practices for the prevention of bullying, behavior:

> efforts to prevent and address bullying behavior should be embedded within a comprehensive, multi-tiered behavioral framework used to establish a positive school environment, set high academic and behavioral expectations for all students, and guide delivery of evidence-based instruction and interventions that address the needs of students. (p. 1)

Given the limited research regarding cyberbullying, it is important for post-secondary institutions to understand the risks and possible implications associated with the lack of policy in addressing student codes of conduct. Stuart-Cassel et al. (2011) identified 11 key components among cyberbullying state laws:

1. Purpose statement
2. Statement of scope
3. Specification of prohibited conduct
4. Enumeration of specific characteristics
5. Development and implementation of local educational agency policies
6. Components of local educational agency policies
7. Review of local policies
8. Communication plan
9. Training and prevention education
10. Transparency and monitoring
11. Statements of rights to other legal recourse

SAFER recommends guidelines for an effective policy that includes crucial elements such as accessibility, due process, fairness, prevention and education, crisis intervention, and counseling (Burczak, 2007). In a study conducted by SAFER and V-Day (2013) reviewing the

effectiveness of policies from 299 4-year institutions of higher education, the authors revealed that, on average, institutions received a grade of a D+, and only 15.6% of institutions received a grade of B or higher, with no institutions receiving a grade of A. Despite Clery Act compliance requirements, 32.6% did not fully comply with the legislative requirement for public disclosure of policy that address specific factors—including the preservation of evidence, and victim and alleged rights and responsibilities.

Prevention program and training. Cyber-harassment policies should include a prevention program framework that includes an annual assessment (Sabella, Patchin, & Hinduja, 2013). According to Kiriakidis and Kavoura, institutions can address bullying and cyberbullying within a similar program (2010). Regulations clearly indicate that institutions of higher education should implement prevention programs that address harassment behaviors; however, they do not prescribe the form in which these programs must be executed. Some institutions have embraced the simple pedagogical model in which the institution plays the role of teacher, determining what, when, and how the information will be communicated. In these circumstances, students' educational programs become limited to the distribution of educational pamphlets regarding information and policy.

In a study conducted by Crosslin and Golman (2014), the researchers propose a socio-ecological approach for the reduction of cyberbullying in higher education. The research found that training was necessary component, as many students stated that they were embarrassed or ashamed to report cyber-harassment (Crosslin & Golman, 2014). Furthermore, Crosslin and Golman (2014) propose organizational interventions as an "awareness curriculum for RAs and student life personnel" to increase awareness among univerity personnel (p. 19). Simmons and Bynum (2014) reiterate those sentiments and suggesst that institions train university peronnel

regarding the effects of cyber-harassment and how appropriately respond to reports of cyber-harassment. It is also recommend that institutions have a group of individuals dedicated in meeting the needs of the students(Sabella, Patchin, & Hinduja, 2013). Simmons and Bynum (2014) propose the following prevention strategies:

- Update the technology policy, and ensure that cyber-harassment is specifically addressed;
- Integrate cyber-harassment in training;
- Establish an institution wide task force or committee;
- Foster relationships with local law enforcement;
- Cultivate a culture of safety;
- In the event of cyber-harassment, follow established policies and procedures.

If a learner is not given the foundational knowledge required as a baseline for the expected change, it is unreasonable to believe that he or she will change a behavior or attitude. Additionally, if the educational program lacks evaluation, the program's effectiveness remains unknown and any changes to behaviors or attitudes cannot be directly attributed to the training itself. A 2005 study sponsored by the U.S. Department of Justice found that 64% of institutions do not provide new students with sexual assault training (Karjane et al., 2005). The lack of such training offers an explanation of the stagnant statistics showing that sexual violence against women remains relatively unchanged. For the 36% of administrators who elect to educate their students, they face the difficult decision of selecting from a plethora of existing training programs or developing a program internally.

Training and education programs range in the content and cost, and a major discussion point for administrators is to balance the financial implications with the incremental benefits of

the program. Sabella, Patchin, and Hinduja (2013) recommend that student training "should be provided to confront cyberbullying by including student competencies which help youth recognize legal and personal consequences of cyberbullying, improve social problem-solving. . . and increase the ability to empathize with victims" (p. 2708). Program characteristics such as format (i.e., face to face, video), length of program, program content, program audience (students, employees), and effectiveness all must be taken into consideration. Given the small number of institutions that offer these educational programs, there is a deficiency in the amount of research available on the effectiveness of these programs (Cortina, Swan, Fitzgerald, & Waldo, 1998; Rothman & Silverman, 2007).

Summary

College and university campus operations are highly regulated through federal, state, and government agency legislation, although regulations that pertain specifically to virtual conduct remain limited. With insufficient regulatory guidance addressing online codes of conduct, institutions face potential legal risk and unknown levels of vulnerability (Fisher, 1995). Institutions that fail to comply with regulatory guidance face consequences that may include loss of participation in Federal Financial Aid programs, fines and sanctions, loss of accreditation, and potential impact to reputation and enrollment.

Although there have been great advances in research, most cyberbullying research has been focused on adolescence (Crosslin & Golman, 2014; Gahagan et al., 2015). However, this phenomenon is not limited to K–12 students. As additional research has shown, cyber-harassing behaviors continue to occur outside of adolescent populations (Crosslin & Golman, 2014). Despite this high level of concern, there still remains an inadequate amount of research regarding cyber-harassment in higher education.

Legislators have clearly addressed discriminatory conduct at colleges and universities by adopting Title IX. In addition to Title IX, the U.S. Department of Education's OCR enforces federal civil rights laws—including Title VI of the Civil Rights Act of 1964, discrimination on the basis of disability as outlined by Section 504 of the Rehabilitation Act of 1973, and age discrimination as outlined by the Age Discrimination Act of 1975. Policies are enforced through the establishment of authoritative offices such as the Department of Education's Office for Civil Rights (OCR). Conduct that violates Title IX, as enforced by the OCR, includes sexual harassment, gender-based harassment, and sexual violence. Institutions that fail to comply with regulatory guidance face consequences that may include loss of participation in Federal Financial Aid programs under Title IV of the Higher Education Act of 1965, fines and sanctions, loss of accreditation, and potential impact to reputation and enrollment. Federal legislation has made significant progress in the areas of gender discrimination in higher education. The U.S. Department of Education's OCR states, "No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance" (U.S. Department of Education, 2015, para. 2).

Sexual assault, harassment, and bullying behaviors fall under the purview of Title IX guidance (Ali, 2010). However, legislation has failed to specifically address higher education institution's responsibility in addressing cyberbullying. With greater advances in technology and increased communication methods, harassment has taken a new shape in the form of cyber-harassment.

Educational institutions are complex organizations that are governed by a diverse and multi-faceted set of federal, state, and agency regulations. Legislation ultimately impacts

organizations through policy, process, and procedure—all of which require organizations to respond and change. When legislation is vague and inconsistent, institutions face the challenge of interpreting policy and implementing compliance measures in an effort to meet regulatory compliance requirements.

Although the U.S. Department of Education, as described in the 2011 *Dear Colleague Letter*, expressed full support towards efforts of individual State Education Authorities in reducing bullying in schools, they have issued no guidance for post-secondary institutions (Ali, 2011). It is recognized that states have an opportunity to expand upon their policies. However, State Education Authorities have limited their purview to adolescent and pre-adolescent students in K–12. Recent court proceedings are setting the standard by which institutions must comply under Title IX, and have left colleges and universities in a vulnerable position. As the justice system and legislation regarding higher education student safety and security continue to evolve, institutions are faced with complying appropriately and operationalizing their compliance efforts.

Given the limited research regarding cyberbullying, it is important for post-secondary institutions to understand the risks and possible implications associated with the lack of policy in addressing student codes of conduct. Willard (2005) proposes institutions employ a clear and well communicated policy. Cyber-harassment policies should include a prevention program framework that includes an annual assessment (Sabella, Patchin, & Hinduja, 2013). It is also recommended that institutions train university personnel (Simmons & Bynum, 2014), and dedicate university reources (Sabella, Patchin, & Hinduja, 2013).

Chapter 3: Research Design and Methodology

In compliance with the provisions outlined in Title IX of the Education Amendments (1972), the Clery Act (1998), and the Violence Against Women Reauthorization Act (2014), institutions of higher education must publish and disclose policy statements pertaining to campus safety and security protocol. That being said, institutions are charged with the responsibility of interpreting legislative guidelines and implementing policies and procedures to ensure compliance with federal, state, and agency legislation. The purpose of this qualitative study is to determine the strategies, best practices, and challenges in policy development towards the prevention and mitigation of cyber-harassment at post-secondary institutions.

Qualitative by design, this study examines the perspectives, insights, and understandings of those that are responsible for developing and operationalizing policies in the areas of cyber-harassment. Creswell (2013) defines qualitative research as an "approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem" (2013, p. 4). This study utilized qualitative data collection methods, to gain "explanation from the data instead of from (or in addition to) prior knowledge or theory" (Richards & Morse, 2013, p. 1).

In an effort to seek further understanding, this study employed a phenomenological method to explore insights and experiences. Through phenomenology, the researcher sought to understand the basic structure of an experience (Merriam, 2014). Phenomenology is the study of people's lived experiences (Merriam, 2014). Phenomenological research is described as a "qualitative strategy in which the researcher identifies the essence of human experiences about a phenomenon as described by participants in this study" (Creswell, 2013, p. 245). Van Manen (1990) expresses that in order to seek *essences*, the researcher must go through a process of "reflection, writing, and rewriting, and thematic analysis" (as cited in Richards & Morse, 2013,

p. 201). A phenomenological approach provided a framework that allowed the researcher to examine higher education policy administrators' in-depth description and perception of the experience of policy development.

This chapter describes the research methodology, including the process for selecting data sources, instrumentation, qualitative data collection procedures, and human subject consideration. Additionally, this study determined success measures and recommendations for future implementation for higher education institutions, when preventing and mitigating cyber-harassment.

Restatement of Research Questions

As described in Chapter 1, this study examined the extent to which institutions have implemented policies regarding cyber-harassment. This study sought to provide more understanding regarding the following:

- What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment?
- What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment?
- How do higher education institutions measure the success of cyber-harassment policies and procedures?
- What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures?

Research Methodology

Richards and Morse (2013) describe five distinctly different qualitative research methodologies: phenomenological research, grounded theory, ethnography, discourse analysis,

and case studies. To address the aforementioned research questions, a phenomenological approach was used to explore strategies, best practices, and challenges experienced by higher education institutions in preventing and mitigating cyber-harassment. As a phenomenological study, this review is designed to understand the experiences of college and university policy administrators (Creswell, 2013).

Phenomenology provides for a framework in which "descriptive, reflective, interpretive, and engaging mode of inquiry from which the essence of an experience may be elicited" (Richards & Morse, 2013, p. 67). The rationale for this study is to further understand the policy administrators' experience and perception of policy development with regard to cyber-harassment in higher education. Qualitative interviews with participants helped to explore policy development and provided participants with a forum to share their unique experiences and perspectives (Creswell, 2013).

Research Design

This research seeks to understand the strategies, best practices, and challenges employed by higher education institutions to prevent and mitigate cyber-harassment. Guided by the literature, interview questions were developed to elicit and explore participants' experiences. To gain the essence of the participants' experiences, the researcher will employ phenomenological interview (Merriam, 2014). The procedures for participant selection, human subjects' consideration, and data collection methods are described in the following sections.

Participant selection. The population studied was policy administrators at post-secondary education institutions. Policy administrators are defined as individuals who are charged by their respective institutions with the responsibility of managing or facilitating the institutional policy process, which may include working with policy developers and policy

approvers. As a qualitative study, the most appropriate sampling method is purposive or purposeful (Merriam, 2014). Purposeful sampling is used when a researcher wants to "discover, understand, and gain insight and therefore must select a sample from which the most can be learned" (Merriam, 2014, p. 77). Through the use of purposive selection sampling, the researcher can learn about the main issues (Polkinghorne, 2005).

In selecting an appropriate sample size, the recommendations vary and are not as succinct or prescribed compared to quantitative research. Merriam (2014), states that sample size depends largely on the research problem itself, where Lincoln and Guba (1985) recommend sampling to the point in which adding additional samples yield redundancy (as cited in Merriam, 2014). Polkinghorne (1989), recommends between 5 and 25 participants for phenomenological studies (as cited in Creswell, Hanson, Plano Clark, & Morales, 2007). For this particular study, a unit of analysis was based on a single participant representing a single, post-secondary institution of higher education. Through purposive selection sampling, the researcher will purposefully selected participants "that [*sic*] will best help the researcher understand the problem and the research question" (Creswell, 2013, p. 189). The selection process began with identifying member institutions of the Association of College and University Policy Administrators (ACUPA). ACUPA membership is comprised of higher education professionals in the United States who are responsible for the oversight of institutional policy.

Consideration was given to the 170 active member institutions publicly available on the Association of College and University Administrators (2015a) website. Member institutions listed on the ACUPA website provide direct links to the institution's primary website. As a member of ACUPA, membership includes access to a master list of individual participant representatives of the listed institution. Individual identifying information for active members is

limited by individual privacy settings established by each individual user. All members are granted the same levels of rights and responsibilities, as detailed in the Association's membership terms and conditions. ACUPA (2015b), acceptable use guidelines, as published on the website, allows ACUPA members to send or announce surveys approved by ACUPA through E-list and to post survey invitations on the ACUPA Bulletin Board. ACUPA board members reviewed the request to contact membership through E-list and the ACUPA Bulletin Board, and provided permission as requested. A copy of the ACUPA Site approval can be found in Appendix B.

Criteria for inclusion. Participation criteria was limited to one individual representative, representing a single higher education institution. The inclusion criteria required that:

- Participants are over the age of 18;
- Participants are members of the Association of College and University Policy Administrators;
- Participants have responsibility to significantly influence policy change and/or are authorized to develop or approve proposed policies;
- Participants represent institutions that are Title IV (1965) federal financial aid eligible institutions; and
- Participants represent institutions that are located on the continental United States.

Criteria for exclusion. Institutions located outside of the continental United States are not included in the sample. Given the strict inclusion criteria outlined, the potential pool of qualified participants is further constricted to 195 potential candidates representing 170 unique institutions of higher education. Upon receipt of approval from the Institutional Review Board,

the researcher posted an invitation to participate on the ACUPA Bulletin Board, and contacted membership via email through E-list, as permitted by ACUPA.

Criteria for maximum variation. To ensure maximum variation, participants were selected from a variety of geographic regions, and represent public, private, and not-for-profit entities. Additionally, institutions ranged in providing varying degrees of post-secondary degree levels and program designations. Invitations to eligible participants were made on a rolling basis, starting with the first 12 identified participants, and then contacting additional participants as needed, until the researcher identified 12 participants that met the inclusion criteria and were willing to participate in the study. Invitations to participate in the research study used the approved IRB recruitment script, found in Appendix C. Efforts to recruit participants was terminated upon the identification of 12 eligible participants. Participant invitations included a declaration expressing that participation is voluntary; participation and responses to the study are confidential; a statement indicating that the participant willingly participates in the study; and the results of the study will be used to increase the body of knowledge with regard to cyber-harassment policy development and implementation.

Human subjects consideration. Qualitative studies, by nature, require data. As such, this study utilized qualitative data collection methods, which seek to discover understanding (Polkinghorne, 2005; Richards & Morse, 2013). The data necessary to further understand strategies, challenges, and best practices for policy development are in the form of experiences of the participants; therefore, the research methodology required the approval of the Institutional Review Board (IRB).

In accordance with the United States Department of Health and Human Services, Title 45 of the Code of Federal Regulations, section 46.101 (45 C.F.R. 46.101), Protection of Human

Research Subjects (2009), the research study required the approval of the Institutional Review Board (IRB) of Pepperdine University's Graduate School of Education and Psychology. Under 45 C.F.R. 46.101, subpart A, Basic HHS Policy for Protection of Human Research subjects, section (b)(2), states as follows:

> (b) Unless otherwise required by department or agency heads, research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy:
>
> (2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless: (i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside of the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation. (p. 3)

In compliance with the federal regulations and Pepperdine University's Federalwide Assurance (FWA), as issued by the Office of Human Research Protections under subpart E (2009), the research as designed in this study meets the requirements for *exemption* under the federal guidelines. A copy of the IRB Exemption Notice can be found in Appendix D. Terms and conditions of participation were communicated to participants. Section 46.116 (2009) of the federal guidelines outline the general requirements for an informed consent. A modified Informed Consent was provided to policy administrators that agreed to participate in the study. According to the guidelines found in the Protection of Human Subjects (2009), informed consent forms contain the following basic elements:

- A statement that the study "involves research, an explanation of the purpose of the research, and the expected duration of the subjects' participation," and research procedures (p. 7);
- A description of any foreseeable risks and potential benefits associated with participation;
- A statement addressing the degree to which confidentiality is maintained;
- A statement indicating that participation is voluntary, and that a participant may refuse to participate at any point in time during the duration of the study; and
- Results will be available to participants upon completion of the study.

All participants who elected to participate in the study were asked to review the modified Informed Consent, prior to participating in the study. A sample of the modified Informed Consent, can be found in Appendix E. Participants who agreed to participate in the study were provided a Letter of Intent. The Letter of Intent, found in Appendix F, provides the participant with the following information regarding the study: (a) a statement indicating that the study is in partial fulfillment of the requirements of a dissertation, (b) a statement reiterating the purpose of the study, (c) a summary of the research methodology used in conducting the study, (d) an approximate amount of time participants would commit to the study, (e) a statement reiterating commitment to confidentiality, (f) an overview of the interview process, (g) a statement disclosing the terms in which the researcher will maintain and destroy the collected data, and (h) a statement ensuring that participants may refuse to participate and withdraw from the process at any point and time during the study.

Data collection methods. Prospective participants received an email requesting participation in the study regarding cyber-harassment policy development and implementation at

post-secondary institutions. Those who responded expressing willingness, ability, and eligibility to participate were provided a letter of intent to participate. The Letter of Intent provided general information regarding the nature of the study, and any risks and benefits for participating. Potential risks subjects may be exposed to include fatigue, boredom, or feeling uncomfortable with certain questions. Other risks may include disclosures of internal policies and procedures in reference to participant's role at their relative place of employment that may impact one's relationship with one's employer.

Interviews with participants were scheduled on days and times in February and March 2016 for a duration of approximately 60 contiguous minutes. Data collection was limited to 12 participants. Where possible, interviews were conducted face-to-face with participants. Given the national population of participants, interviews were also facilitated virtually through a recordable format such as Adobe Connect. At the time of the interview, participants were provided additional information regarding the terms and conditions of their participation, including the option to record sessions as well as options to use specific content as part of the study. In the event a participant refrained from providing consent to record interviews, as an alternative, the researcher took notes during the interview. In the event a participant refrained from providing consent to use specific, or identifying, information, the investigator destroyed identifying information. Identification of the participant's identity would be known only by the investigator, and only pseudonyms were used to reference the participant and his or her respective organization.

For interviews that were conducted in person, the researcher arrived at least 20 minutes prior to the scheduled interview time. For those that provided permission to record interview sessions, the researcher brought two recording devices to mitigate risk of technological failure.

Where a phone or video conference interview was scheduled, the researcher utilized the method preferred by the participant. All interviews were confirmed at least 24 hours prior to the scheduled time and date. The confirmation included the researcher contact information, the scope of the interview, the time and date of the interview, the interview location if applicable, and a copy of the modified Informed Consent.

All recorded interviews were stored on a computer hard drive. Interview content was transcribed by the researcher immediately following the interview to ensure that inadvertent references made using individual names or institutions were redacted. Audio records were immediately destroyed after interviews were transcribed. All records, handwritten and electronic, were stored in a secure file cabinet in a locked office in the principal researcher's home. Records will be stored for a minimum of three years, after which the data will be destroyed. Reporting of the data was done in aggregate.

To further ensure confidentiality, participants' personal information will be subject to confidentiality, and only themes will be disclosed as part of the research study. Participants were not provided incentives for participation in the study. After completing the interview, participants received letters of acknowledgment from the principal researcher expressing gratitude for investing their time and sharing their experience in support of the study. Additionally, each participant was provided the option to receive a copy of the formal report upon completion.

Interview Protocol

Guided by the literature and the research questions, interview questions were developed. According to Potter (1996), interviewing is a "technique of gathering data from humans by asking them questions and getting them to react verbally" (as cited in Polkinghorne, 2005,

p.142). Interviewing is necessary, when the researcher "cannot observe behavior, feelings, or how people interpret the world around them" (Merriam, 2014, p. 88). Interviewing is the most effective technique when conducting research from few selected participants (Merriam, 2014; Polkinghorne, 2005). The following sections outline the framework for the interview, including techniques used during the interviews with participants, interview instrument, and the validity and reliability of the instrument used to collect the qualitative data.

Interview techniques. Prior to the interview, the researcher sent a reminder confirmation to the participant one week prior to the prearranged appointment time. The reminder was sent electronically, via email, with a secondary courtesy call expressing gratitude for participation. The confirmation included the researcher contact information, the scope of the interview, the time and date of the interview, the interview location if applicable, and a copy of the modified Informed Consent. For meetings in which the researcher or the participant was not available to meet in person, video conferencing or telephonic communication tools were used to facilitate for the discussion. Where a phone or video conference interview was scheduled, the researcher utilized the method preferred by the participant.

For interviews that were conducted in person, the researcher arrived at least 20 minutes prior to the scheduled interview time to allow the researcher ample time to account for logistics and any unforeseeable circumstances associated with traveling to an unfamiliar destination. For participants that provided permission to record interview sessions, the researcher brought two recording devices to mitigate any potential technological failure. Prior to beginning the interview process, the researcher reviewed the provisions outlined in the modified Informed Consent with the participant. The modified informed consent form provides for a detailed outline of discussion points including: (a) the purpose of the study, (b) the expected duration of the meeting, (c) a

reminder of any foreseeable risks and potential benefits with participating, (d) the degree to which the researcher will maintain confidentiality, (e) a reminder that participation is voluntary and that the participant may elect to refrain from answering any of the questions without penalty, and (f) a reminder that upon completion of the study, the results will be available for the participant to review.

The researcher outlined the semi-structured nature of the interview, which allows the researcher the opportunity to follow up and ask for elaboration and clarification (Creswell, 2013; Merriam, 2014). Participants were encouraged to answer the questions thoughtfully and honestly, and were provided the opportunity to elaborate on previously asked questions. In turn, participants were informed that the researcher may ask follow-up questions. The participant was provided a full understanding of the intent and use of the participants' interview responses (Creswell, 2013). Prior to commencing participant interviews, this study used consensual validation that seeks the opinions of others (Creswell, 2013).

The researcher began the discussion with one or two icebreaker questions to gain a better understanding of the participant's applicable professional and academic experiences. During the interview, the researcher employed active listening techniques to encourage participation. Upon commencement of the interview, the researcher provided a final thank-you statement, acknowledging the time the participant invested into the research study (Creswell, 2013).

Interview questions. Participants were asked to participate in a semi-structured interview. Semi-structured interviews are "appropriate when the researcher knows enough about the study topic to frame the needed discussion in advance" (Richards & Morse, 2013, p. 127). Each participant in this research study was asked a series of 14 pre-structured questions

pertaining to cyber-harassment policies at post-secondary institutions, intended to elicit the participants perspectives (Creswell, 2013). The list of interview questions were as follows:

1. How do you define “cyber-harassment”?
2. What are your best practices for the prevention and mitigation of cyber-harassment?
3. What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment?
4. What policy implementation process techniques and methods have worked in your development of prevention and mitigation programs for cyber-harassment?
5. What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to prevention and mitigation of cyber-harassment?
6. What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment?
7. How did you deal with and/or overcome those challenges?
8. How does your institution measure the success of cyber-harassment policies and procedures?
9. What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment?
10. How do you assess your interim success through the policy development and implementation process? For instance, how did you know things were going according to plan?
11. How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure?

12. How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program?
13. What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program?
14. Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study?

Validity and reliability. To ensure that the interview questions adequately addressed the research questions, a multi-step validation process was developed. In the first step, guided by the research questions and the literature review, interview questions were developed by the researcher. In the second step, the interview questions were reviewed by peers. In the final step of the process, the interview questions were reviewed by an expert panel of faculty members.

Prima facie validity is an established presumption that the evidence is "sufficient to establish fact" (Cornell University Law School, n.d.-b, para 1). The researcher crafted interview questions that encouraged and solicited thoughtful and comprehensive responses from the participants. The questions were developed to engage the participant in sharing their experiences, challenges, and recommendations. The researcher establishes prima facie validity, by independently designing questions with knowledge obtained through research of the subject and review of the literature. To ensure that the interview questions appropriately addressed the constructs of the research questions, interview questions were reviewed by a preliminary committee of two doctoral students enrolled in the Organizational Leadership program at Pepperdine University. The proposed interview questions along with associated research questions were emailed to the peer reviewers for consideration. The doctoral committee was asked to review the questions for adequacy and validity as they aligned to the research questions.

After review, the peer reviewers returned the table with thoughtful comments and recommendations. Through peer review validity, doctoral students contributed both professional and academic experiences, to which they were able to ascertain the validity of the proposed questions. After which, the feedback was incorporated, and provided to the dissertation committee for review.

Finally, the interview questions and associated research questions were provided to the doctoral committee for further refinements and recommendations. The questions were submitted to the committee comprised of three faculty members at Pepperdine University's, Graduate School of Education and Psychology through an online learning platform. In the event that committee members disagreed, the dissertation chairperson would make the final recommendation. Below, Table 3 reflects the approved interview questions as validated through the three-step process.

Table 3

Research Questions and Corresponding Interview Questions

Research Questions	Interview Questions
RQ1: What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment?	IQ1: How do you define "cyber-harassment"? IQ2: What are your best practices for the prevention and mitigation of cyber-harassment? IQ3: What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment? IQ4: What policy implementation process techniques and methods have worked in your deployment of prevention and mitigation programs for cyber harassment?

(continued)

Research Questions	Interview Questions
RQ2: What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment?	IQ5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to the prevention and mitigation of cyber-harassment? IQ6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment? IQ7: How did you deal with and/or overcome those challenges?
RQ3: How do higher education institutions measure the success of cyber-harassment policies and procedures?	IQ8: How does your institution measure the success of cyber-harassment policies and procedures? IQ9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment? IQ10: How do you assess your interim success through the policy development and implementation process? For instance, how did you know things are going according to plan? IQ11: How would you personally describe the elements of a successful prevention and mitigation of cyber-harassment policy and procedure? IQ12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program?
RQ4: What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures?	IQ13: What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program? IQ14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study?

Statement of Limitations and Personal Bias

The design of the study is inherent with limitations. This research study required that participants provide an accurate account of their past experiences. As such, the methodology relies heavily on the assumption that participants' memories were shared accurately and honestly. It is also assumed that participants were able to effectively articulate recollections of their personal experiences and willing to share in the depth and breadth of those experiences (Polkinghorne, 2005).Given that the participants were asked to reflect upon their experiences, it is possible that their recollection or account of those experiences may change in time.

Accordingly, a purposive sample is one in which the participant is purposefully selected to help understand the phenomenon of higher education policies and procedures as they pertain to cyber-harassment (Creswell, 2013). Only policy administrators employed at post-secondary institutions of higher education were chosen as participants of this study. Additionally, the participant selection was limited to individuals employed at institutions that offer educational courses on online formats. The research was limited to individuals who have responsibility to significantly influence policy change, specifically those that are authorized to develop or approve proposed policies. The participant selection was limited to individuals employed at institutions located within the geographical boundaries of the continental United States of America. As such, participants from countries outside of the United States of America may reflect upon different perceptions and experiences.

Participants for this study were purposefully selected, and were not selected randomly. As such, the respondents may not represent the broader population of college and university policy administrators. Given the national population of participants, interviews were facilitated through phone and video-conference in scenarios where in-person meetings were unlikely. Although the participant responses were no less qualitative in nature, it is important to note the implications that the physical presence, or lack thereof, of the researcher may inadvertently modify the respondents' responses to the questions. Data was solicited from the participants through semi-structured interviews. According to DeMarrais (2004), an interview is a "process in which a researcher and participant engage in a conversation focused on questions related to the research" (as cited in Merriam, 2014, p. 87).

It is imperative to recognize researcher bias in research design and analysis. The researcher understands that personal bias may influence the interpretation of the data collected.

The researcher has spent over 15 years as a business operations professional, specializing in compliance, risk, and regulatory operations. More recently, the researcher has spent the past five years working in higher education. It is important to note that the researcher had personal bias while conducting the research for this study (Creswell, 2013). As such, the researcher acknowledges this biasness, and has identified and reflected upon these experiences.

According to Richards and Morse (2013), the research must bracket previous knowledge gained through personal knowledge and knowledge gained from the literature. According to Giorgi, bracketing previous knowledge is necessary to allow the researcher to encounter the phenomenon "freshly and describe it precisely as it is perceived" (as cited in Richards & Morse, 2013, p. 199). Epoche is a process by which the researcher becomes aware of personal prejudices and assumptions regarding his or her research (Merriam, 2014). The following outlines the strategies the investigator employed to put personal knowledge aside. Before embarking on the data gathering, personal assumptions of anticipated findings were documented in a journal. This provides a forum in which assumptions are brought to the forefront, where the implicit becomes clear and unambiguous. A second strategy used to conduct the research was the practice of "building an argument" (Richards & Morse, 2013, p. 218). As knowledge continues to grow, the argument is referenced and challenged throughout the data analysis process.

Data Analysis

The objective of data analysis is to "make sense of the data" (Merriam, 2014, p. 175) requiring the researcher to consolidate, synthesize, and interpret the information obtained from the interviews conducted. The study followed Creswell's (2013) six step iterative approach to data analysis and interpretation, whereas research data was collected, organized, analyzed, and then coded for themes. The first of the six distinctive steps began with the organization and

preparation of the data (Creswell, 2013). Step two of Creswell's (2013) six steps is to "read or look at the data" (p. 197). Step two is distinctly different from step one in that step two serves as an opportunity to reflect upon the overall meanings and ideas the participants expressed during the interview process.

The analysis and coding processes are described in steps three and four, where coding is defined as organizing the data by bracketing it into chunks (Creswell, 2013). Richards and Morse (2013) describes coding as a process of abstracting themes from the data; a theme is defined by "a common thread that runs throughout the data" (p. 151). Step five of the process translates the themes identified from the coding porcess, and advances how these themes will be represented in conveying the findings of the analysis (Creswell, 2013). Interpretation of the qualitative research is the final step of the data analysis process, where interpretation can take on a variety of forms (Creswell, 2013). Giorgi (1997) proposes a similar method consisting of five basic steps to include collection of data, reading the data, coding the data, expression of the data, and synthesis and summary of the data (as cited in Richards & Morse, 2013).

1. Collection of the verbal data will occur while conducting the semi-structured interviews with the participants. Through the research framework previously discussed, data as represented by the experiences shared by the participants is collected.
2. Reading the data allows the researcher to scope the depth and breadth of the experiences reported through the interviews, and provides the researcher an opportunity to reflect upon its meaning (Creswell, 2013).
3. Themes are extracted through the coding process. Merriam (2014) introduces the notion of open coding, in which the researcher is *open* to that data.

4. From the key words identified, patterns will begin to emerge and form themes. The codes are organized in a fashion in which key themes are identified.
5. In the final stage, the coded information is synthesized and summarized.

Inter-rater Reliability

Strauss (1987) expresses the importance of coding in that the "excellence of research rests in large part on the excellence of coding" (as cited in Richards & Morse, 2013, p. 149). To ensure that the coding process establishes consistency in researcher findings (Armstrong, Gosling, Weinman, & Marteau, 1997), a multi-step coding process was employed. In the first step, the data was coded by the researcher. In the second step, the results were discussed with peer reviewers. In the final step, the results were reviewed by an expert panel of faculty members. Peer reviewers were asked to complete a Peer Reviewer Nondisclosure form, to further protect the information and research related to participant interview data. A sample of the Peer Reviewer Nondisclosure can be found in Appendix G.

Step 1: initial coding. In the initial step, the researcher reviewed the participant responses and identified a key word or phrase that summarized the statement. The researcher created a table in which the statement has a corresponding key word or phrase. The segments of data and associated keywords help to organize the information (Merriam, 2014). The codes extracted from the data were categorized into themes. Overarching themes were used as column headings to organize the coding into categories and patterns.

Step 2: peer review. Upon construction of the table, the coding and themes were reviewed by a preliminary committee of two doctoral students enrolled in the Organizational Leadership program at Pepperdine University. The co-reviewers discussed the themes,

triangulated (Armstrong et al., 1997) the findings, and reviewed the recommended changes with the researcher.

Step 3: expert review. Upon completion of the peer review, the researcher and a member of the dissertation committee met to review the coding and the respective recommendations of the co-reviewers. In the event that the co-reviewers expressed conflicting recommendations, the faculty provided final guidance and concurrence. The themes are discussed in detail in chapter four.

Summary

Qualitative by design, this study examined the perspectives, insights, and understandings of policy development in the areas of cyber-harassment. This study employed a phenomenological research method to explore insights and experiences, and to seek further knowledge and understanding. In an effort to explore further understanding, participants were purposefully selected to participate in semi-structured interviews. As the researcher had enough knowledge about the domain, the use of semi-structured interviews was appropriate and did not limit the discovery of significant concepts expressed (Richards & Morse, 2013). Interview questions were designed to elicit views and opinions from the participants (Creswell, 2013, p. 190). Upon completion of the interviews, the researcher transcribed, analyzed, and then coded the information into themes.

Chapter 4: Findings

Technology has increased the effectiveness and efficiency of communication in higher education. The development and expansion of information and communication technologies introduced several types of malevolent behaviors such as cyber-harassment (Kubiszewski, Fontaine, Potard, & Auzoult, 2015; Willard, 2005). With advances in technology, higher education administrators are challenged with expanding protocol beyond the physical boundaries of a campus and into the virtual environment. Although no federal law specifically addresses cyber-harassment in higher education, institutions have a legal obligation to address all claims of harassment, regardless of the location or platform in which the harassing behavior occurs.

Researchers have conducted studies to explore the prevalence of cyberbullying (Li, 2006, 2007; Patchin & Hinduja, 2006). Scholarly research on cyberbullying behaviors performed on elementary, middle school, and high school aged populations range from 9% to 42% (Kowalski et al., 2014) with cyber-harassment victimization among college populations ranging from 10% to 28.7% (Zalaquett & Chatters, 2014). Given the prevalence of cyber-harassment behaviors, it is vital for institutions to prevent and mitigate unwelcome conduct and to respond appropriately and effectively should misconduct occur. Accordingly, participants in this research study provided key insights regarding strategies, best practices, and challenges experienced by policy administrators when developing and implementing prevention and mitigation policies and programs. Additionally, participants' perspectives provided an insightful understanding of the complexities of interpreting legislation and the implications associated with operationalizing higher education policy. In an effort to seek further understanding, this study employed a phenomenological method in addressing the following research questions:

- What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment?
- What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment?
- How do higher education institutions measure the success of cyber-harassment policies and procedures?
- What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures?

Recruitment of Participants

Participants in this study included representative members of the Association of College and University Policy Administrators (ACUPA). ACUPA (2015a) membership is comprised of professionals who provide oversight and management of institutional policy at higher education institutions. Participation criteria was limited to one individual, representing a single higher education institution. The inclusion criteria require that:

- Participants are over the age of 18;
- Participants are members of the Association of College and University Policy Administrators;
- Participants have responsibility to significantly influence policy change and/or are authorized to develop or approve proposed policies;
- Participants represent institutions that are Title IV (1965) federal financial aid eligible; and
- Participants represent institutions that are located on the continental United States.

Summary of recruited participants. Consideration was given to the 711 active members publicly available on the ACUPA website (2015a). In selecting an appropriate sample size, the recommendations vary and are not as succinct or prescribed compared to quantitative research. Polkinghorne (1989), recommends between 5 and 25 participants for phenomenological studies (as cited in Creswell, Hanson, Plano Clark, & Morales, 2007, p. 254). Given the inclusion criteria outlined, the potential pool of qualified participants is further constricted to 195 prospective participants. All 195 prospective participants, representing 170 institutions, received invitations to participate in the study. Invitations to eligible participants were made on a rolling basis, starting with the first 12 identified participants, and then contacting additional participants as needed, until the researcher identified 12 participants that met the inclusion criteria and were willing to participate in the study. Efforts to recruit participants were terminated upon the identification of 12 eligible participants.

Prospective participants received an email requesting participation in the study regarding cyber-harassment policy development and implementation at post-secondary institutions. Of the 195 ACUPA members invited to participate in the study, 78% did not respond and an additional 10% were further categorized as ineligible. The researcher categorized participants as ineligible upon receipt of an automatic email response from potential participants indicating that they were no longer employed at the institution or that their role at the respective institution had changed; therefore, making those individuals ineligible to participate.

Eleven (6%) participants responded to the invitation declining to participate in the study. Reasons included (a) unavailability due to personal obligations, (b) participant was new in their respective role, (c) their responsibility relative to policy development did not meet the inclusion criteria, (d) given the specific subject of cyber-harassment participants were not able to

adequately or appropriately address the topic and/or interview questions, and (e) given their role at their respective institution, participating would potentially breach attorney-client privilege. Those who responded expressing willingness, ability, and eligibility to participate, were provided a letter of intent to participate. The Letter of Intent (Appendix F) provided general information regarding the nature of the study and any risks and benefits for participating. Additionally, each participant was provided a copy of the modified Informed Consent (Appendix E).

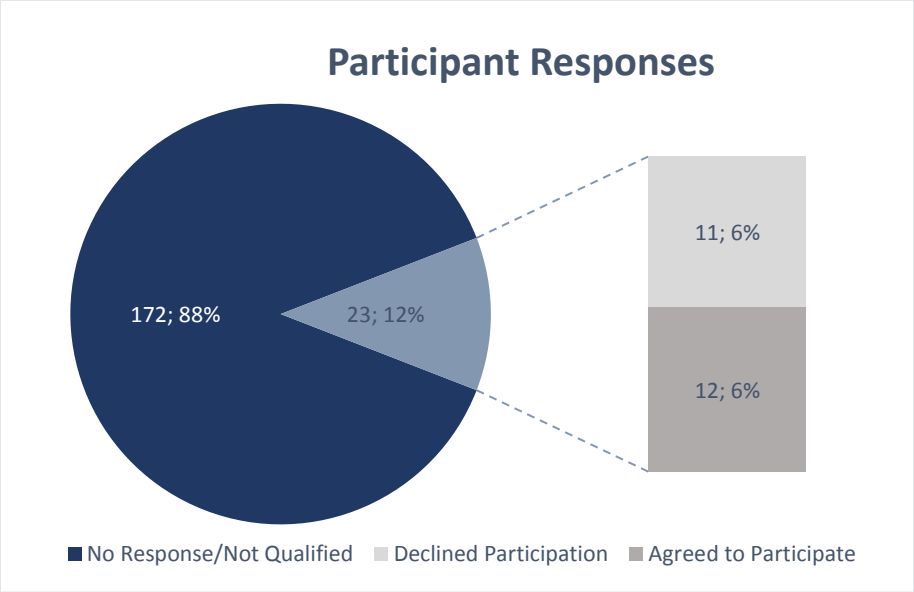

Figure 1. Participant responses

Data Collection Process

The data for this study was collected from the participants throughout the month of March 2016. Given the geographical distribution of the participants, all interviews were conducted through telephonic communication tools. At the time of the interview, participants were provided additional information regarding the terms and conditions of their participation, including the option to record sessions. All participants agreed to have their interviews recorded, as outlined in the Informed Consent. Table 4 summaries the dates in which the 12 participants for this study were interviewed.

Table 4

Dates of the Participant Interviews

Participant	Interview Date
P1	March 1, 2016
P2	March 2, 2016
P3	March 3, 2016
P4	March 8, 2016
P5	March 8, 2016
P6	March 8, 2016
P7	March 10, 2016
P8	March 14, 2016
P9	March 17, 2016
P10	March 17, 2016
P11	March 21, 2016
P12	March 29, 2016

Relationship between research and interview questions. Prior to the start of the interview, the researcher reviewed with the participant the provisions outlined in the Informed Consent. Data collection was facilitated through semi-structured interviews that lasted up to one hour. Each participant in the research study was asked a series of 14 research-based interview questions pertaining to cyber-harassment policies. Research question one asked: What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment? To address this question, the participants were asked the following four interview questions:

IQ 1: How do you define “cyber-harassment”?

IQ 2: What are your best practices for the prevention and mitigation of cyber-harassment?

IQ 3: What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment?

IQ 4: What policy implementation process techniques and methods have worked in your development of prevention and mitigation programs for cyber-harassment?

Research question two asked: What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment? To address this question, the participants were asked the following four interview questions:

IQ 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to prevention and mitigation of cyber-harassment?

IQ 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment?

IQ 7: How did you deal with and/or overcome those challenges?

The third research question asked: How do higher education institutions measure the success of cyber-harassment policies and procedures? To address this question, the participants were asked the following four interview questions:

IQ 8: How does your institution measure the success of cyber-harassment policies and procedures?

IQ 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment?

IQ 10: How do you assess your interim success through the policy development and implementation process? For instance, how did you know things were going according to plan?

IQ 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure?

IQ 12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program?

The fourth research question asked: What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures? To address this question, the participants were asked the following four interview questions:

IQ 13: What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program?

IQ 14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study?

During the interview, the researcher employed active listening techniques to encourage participation. The researcher paraphrased and rephrased questions as necessary and provided clarification as requested by the participant. At the completion of the interview, the researcher provided a final thank-you statement acknowledging the time the participant invested into the research study (Creswell, 2013). As outlined in the Informed Consent, all recorded interviews were transcribed into a Microsoft Word document. All identifying information or any reference made to individuals or the participants' respective institution were redacted from the transcripts, ensuring transcripts were deemed anonymous by nature. The 12 identified eligible participants fully represented the diverse requirements of the selection criteria, having varying levels of education, levels of experience in higher education, and having varying ranges in positions at their respective institutions. Each participant was employed at a public or private institution of higher education. There were nine female participants and three male participants in the study.

The 12 participants represented 12 distinctly different private and public institutions of higher education, geographically disbursed throughout the continental United States. Two institutions were located in the State of New York, two institutions were located in the State of Texas, and the remaining eight institutions located in the following states; Florida, Pennsylvania,

Minnesota, Ohio, Illinois, Kentucky, Colorado, and Virginia. Represented institutions reflect nine public institutions and three private institutions of higher education, of which two of the three private institutions were religiously affiliated. Active student enrollment in these participating institutions ranged from 2,300 to 61,600 (U.S. Department of Education, 2016).

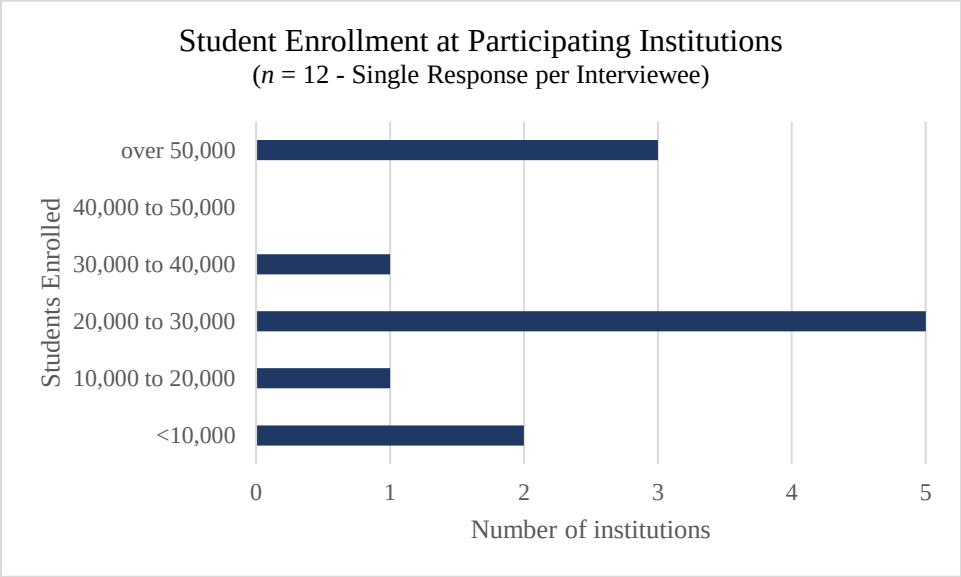

Figure 2. Student enrollment at participating institutions.

Data Analysis

The transcribed data was reviewed and analyzed following Giorgi's (1997) five-step approach to data analysis and interpretation, in which data was collected, read, coded, themed, and summarized. After the data was transcribed, the researcher read and reviewed the transcripts to understand the depth and breadth of the participant experiences (Creswell, 2013). The transcripts were printed, organized, and reviewed. The transcribed data was reviewed, and all key words and phrases were highlighted. A table was created to organize segments of data provided in participant responses. The highlighted key words and phrases were entered into the table accordingly, where overarching themes were identified.

Inter-rater reliability. A multi-step coding process helped to establish consistency in researcher findings (Armstrong et al., 1997). Participant responses were reviewed, and key words and phrases that summarized the statement were identified. The results of the analysis were presented to a preliminary committee of two doctoral students enrolled in the Organizational Leadership program at Pepperdine University. The co-reviewers discussed the themes, triangulated (Armstrong et al., 1997) the findings, and provided the researcher with the recommended changes. Recommended changes included recategorization of identified key words and phrases, and refinement of thematic naming conventions. Their insights and suggestions were appreciated and invaluable in assessing the data and presenting the findings. The recommended changes were incorporated into the analysis accordingly.

Data Display

Interview questions were designed to elicit participant experiences (Creswell, 2013). Participant responses were reflective of these views and opinions, and provided context in adequately addressing the research questions outlined within this study. Overarching themes which emerged from the data, are discussed as follow:

Research Question One

Research question one asked: What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment? To address this question, the participants were asked the following four interview questions:

IQ 1: How do you define “cyber-harassment”?

IQ 2: What are your best practices for the prevention and mitigation of cyber-harassment?

IQ 3: What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment?

IQ 4: What policy implementation process techniques and methods have worked in your development of prevention and mitigation programs for cyber-harassment?

Interview question 1. Illustrated in figure 3, participants expressed three major themes in response to the first interview question. IQ 1: How do you define "cyber-harassment"? Participant responses were categorized as follows: (a) their institution did not have a specific policy that addressed cyber-harassment, (b) application of existing policies, and (c) expressed their personal definition.

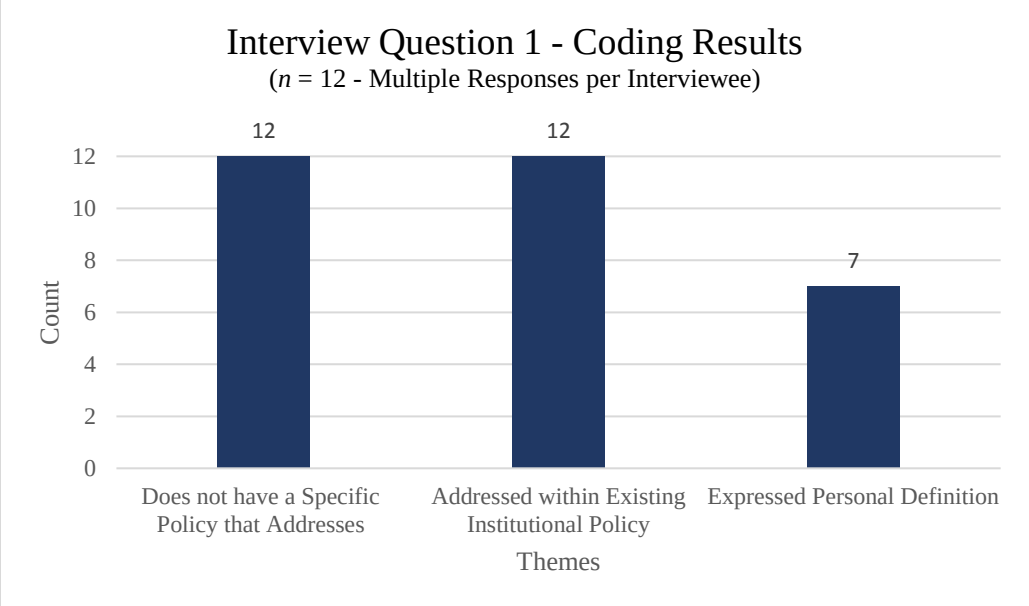

Figure 3. Themes and frequencies of responses associated with interview question 1.

Does not have a specific policy that addresses. Of the 12 participants, 100% indicated that their institution lacked a specific policy that addressed cyber-harassment. Additionally, all participants indicated that cyber-harassing behaviors would be addressed within the context of the institution's battery of existing policies. Eight of the 12 respondents; P1, P3, P4, P6, P8, P9, P10, and P12 indicated that their policies were broad enough to apply to virtual environments. P8

clarifies that their policies "govern the behavior itself, in all of the forms that it can manifest" (personal communication, March 14, 2016). Although some confidently referenced existing policies, and their application to cyber-harassment, P1 stated "I'm not so sure we address cyber-harassment or cyberbullying . . . I'm not saying it couldn't qualify, I'm just saying it's not called out" (personal communication, March 1, 2016).

Addressed within existing institutional policy. When clarifying which policy or policies would apply to cyber-harassing behaviors, participants cited a range of policies including the Harassment Policy, Sexual Harassment Policy, Sexual Misconduct Policy, Acceptable Use and Network Security Policy, Responsible Use Policy, Discrimination and Harassment Policy, Title IX Policy, Violence Policy, Social Media Policy, and Student Code of Conduct Policy. Additionally, many of the participants cited multiple policies that would apply in the event of cyber-harassment, as illustrated by P4:

> There is a Board policy on Harassment. We have Sexual Harassment . . . we have the responsibilities spelled out, which is also on our board policies. And then we link back to any related information . . . we link back to Code of Conduct, Sexual Harassment, and Student Code of Conduct . . . There is another administrative policy, called Sexual Assault, Relationship Violence, and Stalking.

Expressed personal definition. Seven participants (58%) provided definitions of cyber-harassment based on their professional and educational experiences. P3 describes cyber-harassment as "unsolicited or unwelcomed messages from identified or unidentified individuals in which there are threatening or unwelcomed comments," and P5 elaborates upon this definition to specify activity that is conducted "using technology to post inappropriate pictures or things that would be viewed inappropriate." P11 specified technological platforms including

"Facebook, Twitter, and Yik Yak" in addition to communication technologies such as email and texting.

Interview question 1 summary. Illustrated in figure 3, participants expressed three major themes in response to the first interview question. IQ 1: How do you define "cyber-harassment"? Participant responses were categorized as follows: (a) their respective institution did not have a specific policy that addressed cyber-harassment, (b) institutions could apply or leverage existing policies in the event of cyber-harassment, and (c) participants expressed their personal definition. 100% of participants indicated that their institution lacked a specific policy that addressed cyber-harassment. Additionally, all participants indicated that cyber-harassing behaviors would be addressed within the context of the institutions existing policies including the Harassment Policy, Title IX Policy, and Violence Policy. Although seven participants (58%) provided definitions of cyber-harassment based on their professional and educational experiences. Definitions provided varied among participants.

Interview question 2. When participants were asked IQ 2: What are your best practices for the prevention and mitigation of cyber-harassment? participants leveraged their experiences and shared best practices obtained from the development and implementation of similar policies. For example, P10 referenced a robust Title IX policy (personal communication, March 17, 2016), whereas P4 stated that "cyber-harassment . . . it's harassment in general, but it would be the same thing, it would be whatever mechanism one would have for harassment" (personal communication, March 8, 2016). Illustrated in figure 4, participants expressed three major themes in response to the second interview question regarding best practices for prevention and mitigation: (a) education and training, (b) active oversight and management, and (c) policy.

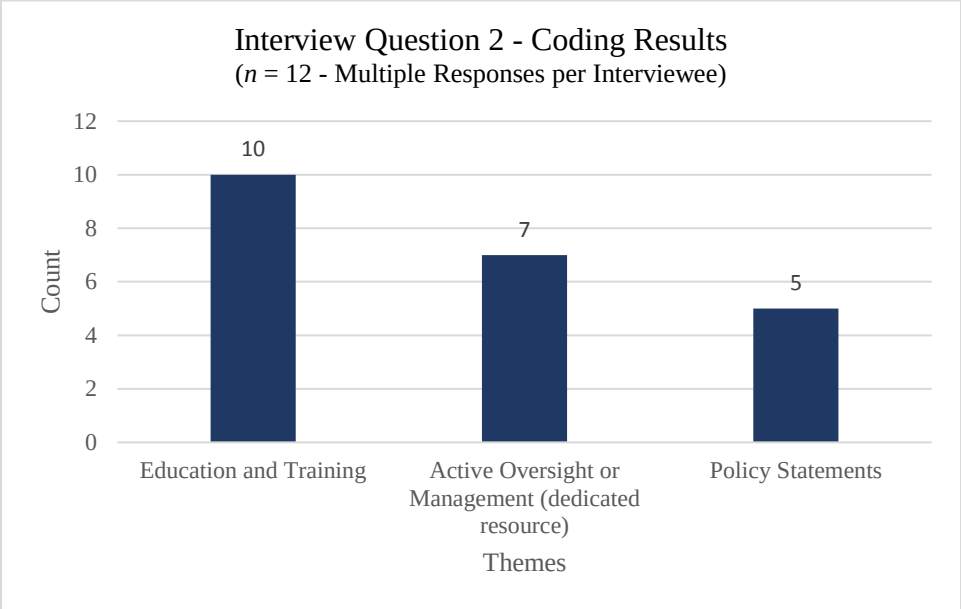

Figure 4. Themes and frequencies of responses associated with interview question 2.

Education and training. Ten out of the 12 participants expressed the use of education and training as a best practice for the prevention and mitigation of cyber-harassment. Participants described a variety of forums and methods in which institutions could extend education and training. P7 discussed a new student orientation as a forum in which cyber-harassing behaviors were discussed. P8 described an online training course for sexual misconduct, which included provisions that addressed cyber-harassing behaviors, while P5 indicated that cyber-harassment is briefly mentioned in their annual "Management Standards Training."

Active oversight and management. Seven (58%) of the 12 policy administrators, P1, P3, P4, P5, P7, P8, and P10 expressed that having dedicated resources and personnel were an essential component of prevention and mitigation programs. However, it is important to note that each participant provided varying examples of resources that potentially could support a cyber-harassment claim. Resources included a marketing and communications department that managed the institutional brand including the management of social media, an Office of

Diversity, a member of the Human Resources department dedicated to employee training, a Crisis Action Team (CAT), and Title IX Coordinators.

Policy statements. Five participants' responses identified written policies as a best practice for the prevention and mitigation of cyber-harassment. Participants expressed the importance of having clearly written policy statements or written disclosures to clarify the institution's expectations of university constituents. With regard to policy violations, policies should specify what the ramifications are for non-compliance, in that it

> would be the right way to educate first and not only be punitive . . . you'll see that our policies have a three-tiered approach to behavioral issues . . . if you look at most of our policies in general, they are progressive. Even on the staff side, there is a progression. (P9, personal communication, March 17, 2016)

***Interview question 2 summary*.** When participants were asked IQ 2: What are your best practices for the prevention and mitigation of cyber-harassment? participants leveraged their experiences and shared best practices obtained from the development and implementation of similar policies. Participants expressed three major themes in response to the second interview question: (a) education and training, (b) active oversight and management, and (c) policy. Ten out of the 12 participants expressed the use of education and training as a best practice for the prevention and mitigation of cyber-harassment. Seven (58%) of the 12 policy administrators, expressed that having dedicated resources and personnel were an essential component for prevention and mitigation programs. Five participants' responses identified written policies as a best practice for the prevention and mitigation of cyber-harassment.

Interview question 3. Participants expressed three major themes in response to the third interview question 3: What resources (e.g., training, education, etc.) do you think are most

helpful in implementing a successful prevention and mitigation program for cyber-harassment? All participants provided similar responses to the second interview question, but highlighted additional specifics. As illustrated in figure 4, participants attributed (a) education and training, (b) active oversight and management, and (c) policy as general themes to be the most helpful resources. As all participants previously stated in IQ1, their institutions lacked policy programs to reference, so participants reflected upon resources that were helpful in similar programs at their respective institutions. P1 exemplifies this point by responding to IQ4, "as I said, we don't have a prevention or mitigation program for bullying or cyberbullying . . . hopefully, somebody knows it when they see it."

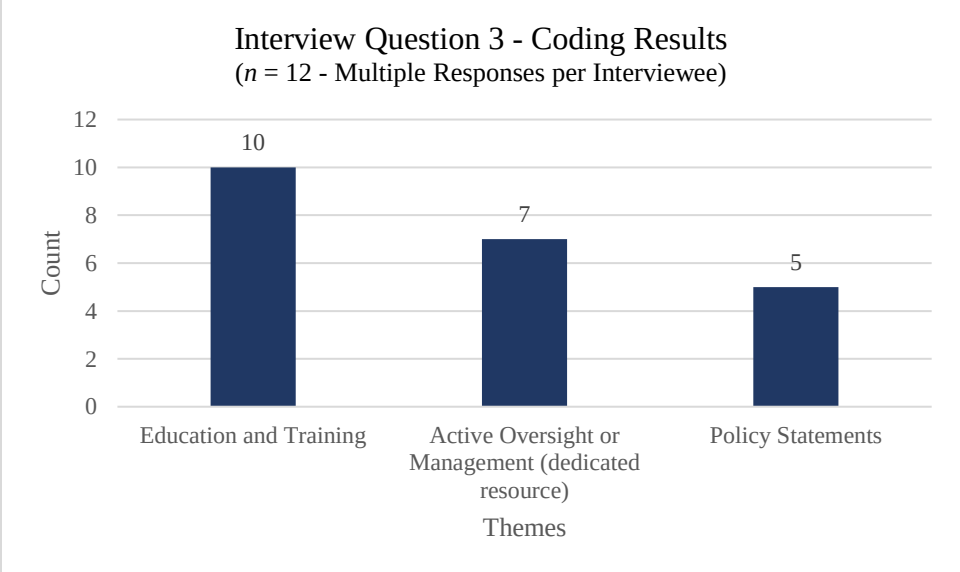

Figure 5. Themes and frequencies of responses associated with interview question 3.

Education and training. Education and training were identified as most helpful in the prevention and mitigation of cyber-harassment. P3 specified that all students, staff, and faculty must take state-mandated trainings, including Security Awareness Training and Technological Security Awareness Training. Within those trainings, specific modules that reinforce the notion that "certain behaviors are not going to be tolerated." P3 indicated that cyber-harassment is a

training component incorporated within technology training topics; P5 indicated that cyber-harassment is addressed within the context of sexual misconduct training. P9 discusses student workshops in which appropriate and inappropriate behaviors are discussed, and P5 indicates that cyber-harassment would be discussed as part of new employee orientation.

Active oversight and management. Active oversight or management were noted as helpful in implementing a successful prevention and mitigation program for cyber-harassment. As originally mentioned in IQ 2, participants elaborated on the role that resources played in executing the provisions within an existing policy.

Policy statements. Five (41%) of the 12 participants indicated that a stated policy that outlines all of the standards and expectations of an institution were most helpful in implementing a successful prevention and mitigation program. P5 begins their response to IQ3 with, "I think first and foremost, obviously there has to be a clearly established policy either directly called cyber-harassment or cyberbullying . . . once that's been established, you can attack it a couple of different ways." To ensure that employees have understood the policies, P5 describes the annual certification process employees must endure to attest to having read and understood the policies.

Interview question 3 summary. Participants expressed three major themes in response to the third interview question 3: What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment? Participants attributed (a) education and training, (b) active oversight and management, and (c) policy as general themes to be the most helpful resources. All participants provided similar responses to the second interview question, but highlighted additional specifics.

Interview question 4. The fourth interview question in the series, IQ4, what policy implementation process techniques and methods have worked in your development of prevention

and mitigation programs for cyber-harassment? explores the role that policy plays as a strategy and best practice. Given that the institutions of all participants in this study lacked a cyber-harassment policy, participants were unable to describe implementation process techniques and methods from firsthand experience. Responses provided were based on the participants' experiences from implementing policies of a similar nature. Responses were categorized in three major themes as illustrated in figure 6: (a) formalized process, (b) outreach, and (c) education and training.

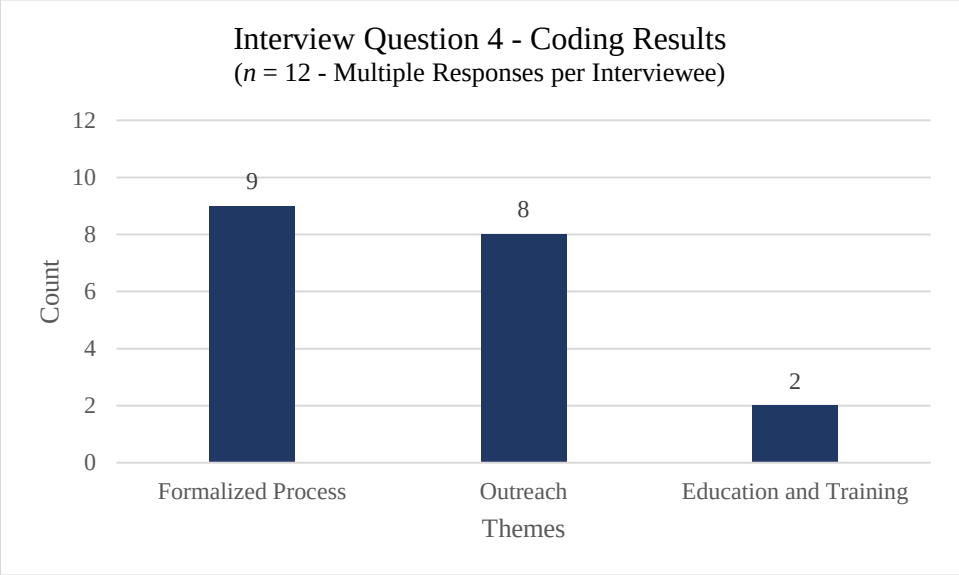

Figure 6. Themes and frequencies of responses associated with interview question 4.

Formalized process. Of the 12 participants interviewed, nine (75%) described a formalized process for policy development, citing that the process of developing the policy was crucial for successful implementation. P4 described the process of creating a new policy in which a policy owner must complete a Policy Plan. Within the framework of the Policy Plan, a policy owner must address a variety of strategic and operational implications:

> Why is it being created, does it overlap with any other policies, what are the risks that are being addressed by this policy, so it will be reputational, financial, health and safety,

managerial, whatever those might happen to be. They have to say how they are going to communicate or train on a brand new policy that goes out.

Policy development processes ranged in complexity, inclusive of formal and informal policy development procedures. P5 describes a formal approval process, requiring endorsement for proposed policies from the Staff Council president, Faculty Council president, and Student Council president. In the event that a Council President expresses concerns on behalf of a constituent group, the Council President would extend an invitation to the policy owner for further discussion. As an informal process, P9 described a fast track procedure in situations where the institution must respond to and comply with changes in the regulatory environment. In a fast track process, the policy "would go right out to our cabinet level, and be approved and communicated out" to the university community."

Seven of the nine participants who identified a formalized process as a key implementation technique, also identified the importance of communicating the policy to university constitutions. In total, eight of the 12 participants described communication and outreach efforts as a fundamental component throughout the development process. Upon the receipt of an Impact Statement and accompanying approval from the Cabinet to begin policy development, P1 composed a working group of "subject matter experts in the area of policy, including, of course, the department that will be the policy owner, and anybody that represents a major stakeholder group." P6 described a semi-public viewing process in which draft policies are posted on a restricted access website for 30 days for key stakeholders to review. Invitations are sent to a broad range of university stakeholders, including the Student Government President, the speaker of the Faculty Senate, and the head of the Employee Advisory Committee, to participate in the comment period. P4 described a process that provides for a 30-day, university community

review period, where policy proposals are posted directly on the institution's website for review and public commentary.

Outreach. Participants not only described the process or duration of communication, they also described the method by which communication should be conducted. P8 stressed the importance of face to face discussions, focus groups, and socialization of a policy. As a way to socialize a policy into the university's culture, "even before we draft, we will go out and do outreach and a lot of listening with the community . . . listen, explain, and listen some more." P2 described the process as "a fairly simple, yet comprehensive policy process . . . that creates an environment that encourages participation."

Education and training. Two participants, P4 and P12, specifically addressed education and training as a fundamental aspect of policy implementation. As a policy is approved and implemented, P4 stressed the importance of public disclosures, fully informing the campus community of the new or revised policy. Although not a common theme widely addressed by participants, P10 noted the importance the organizational structure has in facilitating for policy implementation. As expressed, the "Policy Office [is] well positioned to have a good overview of the institution . . . we put in place a process."

Interview question 4 summary. The fourth interview question in the series, IQ4, what policy implementation process techniques and methods have worked in your development of prevention and mitigation programs for cyber-harassment? explores the role that policy plays as a strategy and best practice. Responses provided were based on the participants' experiences from implementing policies of a similar nature. Responses were categorized in three major themes: (a) formalized process, (b) outreach, and (c) education and training.

Nine (75%) of the 12 participants described a formalized process for policy development, citing that the process of developing the policy was crucial for successful implementation. Eight of the 12 participants described communication and outreach efforts as a fundamental component throughout the development process. Two participants specifically addressed education and training as a fundamental aspect of policy implementation.

Research question 1 summary. Scholarly research has determined the prevalence of cyber-harassing behaviors in higher education (Zalaquett & Chatters, 2014). The first four interview questions helped to explore the first research question: What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment? Participants were asked to define cyber-harassment. All participants indicated that their institutions lacked policies that addressed cyber-harassment; therefore, they were unable to reference an exact definition. Furthermore, participants expressed that should cyber-harassment behaviors occur, the institutional response would be guided by a range of other policies inclusive of behavioral conduct policies, information technology policies, and discrimination and harassment policies.

Participants identified education and training, active oversight and management, and a clearly written policies as best practices for the prevention and mitigation of cyber-harassment behaviors. Similarly, when asked what resources are most helpful, participants expanded upon their responses from the previous question and provided additional examples of methods and forums in which institutions have conducted training. Education and training were recommendations made as a resource for faculty, staff, and student constituents. In all of the examples provided, all responses were based on experiences learned from implementing other types of prevention and mitigation programs.

To round out the final interview question asked of participants with regard to policy implementation process techniques and methods that have shown effective, responses were categorized to include a formalized process for policy development; outreach and communication to the university community; and education and training. As with previous questions, participants could only speak from experiences from policies of a similar nature, as the institutions of all the participants lack a cyber-harassment policy.

Research Question Two

Research question two asked: What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment? To address this question, participants were asked the following three interview questions:

> IQ 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to prevention and mitigation of cyber-harassment?
>
> IQ 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment?
>
> IQ 7: How did you deal with and/or overcome those challenges?

Interview questions explored challenges, obstacles, or surprises in the development and implementation of the policy and process related to the prevention and mitigation of cyber-harassment. Additionally, participants shared methods and techniques used to overcome those identified challenges.

Interview question 5. Illustrated in figure 7, participants expressed four major themes in response to IQ 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing a policy related to the prevention and mitigation of cyber-

harassment? Participant responses were themed as follows: (a) organizational culture, (b) policy and the policy development process, (c) social and political environment, and (d) resources.

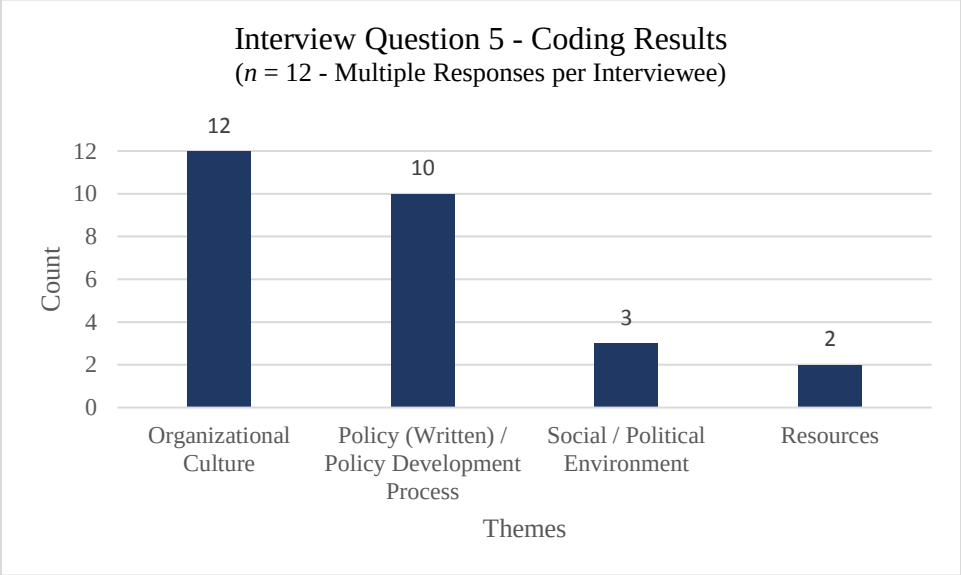

Figure 7. Themes and frequencies of responses associated with interview question 5.

Organizational culture. Of the 12 participants, 100% referenced the effect and impact that organizational culture had on developing and implementing a policy. It is important to acknowledge the organizational culture, taking into consideration the "connectedness that makes up the social community of the organization" (Schmieder-Ramirez & Mallette, 2007, p. 7). Participants clearly exploited the opportunity to discuss challenges between individuals and among departments. P3 provided a disclosure prior to providing appropriate response indicating that "this is my personal opinion, not to be shared by [*sic*] the university" (personal communication, March 3, 2016). After which, the participant candidly revealed personal disapproval of the leadership at the institution's diversity office.

P2 acknowledged the dichotomy between the "academic side versus the administrative side" (personal communication, March 2, 2016). P11 described the challenge in working with faculty, in that "if there is no bigger challenge, that is one of them [*sic*]" continuing to state that

"there is no comparison in the way that the two groups are treated" (personal communication, March 21, 2016). In reference to the opinions of a small group of faculty, P1 stated that "not everybody gets what they want" (personal communication, March 1, 2016).

Contributors to the process may exhibit "more passion or interest than others . . . depends on the policy and their relation to the person" (P7, personal communication, March 10, 2016). P6 acknowledged the role that personalities and personal agendas play in the policy development process. Although all conflict is not entirely avoidable, P3 described how some have reacted to the conflict, in that "people are reluctant to speak up because they feel like their opinions, or what they have to say, or how they say it, may be misconstrued by the other side" (personal communication, March 3, 2016). P4 addressed the challenge of developing and implementing policy at a larger institution. One's attempt to ensure inclusion with all of the appropriate audiences may come at the expense of having an expeditious process. P6 addressed the challenge of appeasing the varying constituent groups:

> We are constantly trying to balance things like, how do you make a policy that is successful to students and to faculty, that lets them know what their options are, with a policy that is complete and thorough, and gives you all the information that you need in one place. (personal communication, March 8, 2016)

Policies and policy development. P9 provided a realistic and insightful look into the extent to which institutions are motivated to create a behavioral policy.

> Yes, if we wanted to go down the path, and identify that we needed a separate, distinct policy on cyber-harassment, this would be a campus wide issue. This would invoke a full governance process. I bet this would require a year or more in the making on our campus, because there would be extensive consultation with students, employees, administrators.

> It's such a sensitive issue, where do you draw the line? Which is why we've always punted and said, "we'll treat it like any other behavior". We've already given our blood, sweat, and tears to develop the behavioral policies we have in place (personal communication, March 17, 2016)

Ten of the participants (83%) indicated that writing the policy and the policy process in itself was a challenge. P1 was challenged with ensuring that the policy was written thoroughly enough, and P6 expressed the need to ensure that the policy written clearly. P8 was challenged with identifying language that "people are comfortable with [*sic*]" (personal communication, March 14, 2016), while P12 was concerned with ensuring that the policy language expresses "the depth and breadth" (personal communication, March 29, 2016) of the institution's intent. In reference to the policy process, P4 balances the opportunity to consult with the appropriate groups while still being able to implement the policy in a timely manner. P9 described the tedious process of extensive consultation with a multitude of stakeholders, while P6 summarized the process as time consuming. P12 described a policy development process at the institution as "quite elegant" (personal communication, March 29, 2016). However, the challenge remains that the institution does not follow the established process, despite good intentions.

Social and political climate. Although not a common theme, three of the 12 participants noted the manifestation of challenges resulting from the social and political environment. P2 acknowledged the role that a charged political climate may have on a policy topic, and the impact that such a climate may have in creating a sense of urgency, or "generating dissension among your administration" (personal communication, March 2, 2016).

Resources. Although only two of the 12 participants identified resources as a challenge, P5 provided a thorough discussion around developing policies without adequate resources

necessary to meet the provisions outlined in the policy, stating, “If you’re going to do trainings, you have to make sure you have a budget for materials, [and] you have the space available to do trainings” (personal communication, March 8, 2016).

***Interview question 5 summary*.** Participants expressed four major themes in response to IQ 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing a policy related to the prevention and mitigation of cyber-harassment? Participant responses were themed as follows: (a) organizational culture, (b) policy and the policy development process, (c) social and political environment, and (d) resources. All of participants referenced the effect and impact that organizational culture had on developing and implementing a policy. Ten of the participants (83%) indicated that writing the policy and the policy process in itself was a challenge. Three of the 12 participants noted the manifestation of challenges resulting from the social and political environment. Two of the 12 participants identified resources as a challenge.

Interview question 6. Participants expressed two themes in response to the sixth interview question, IQ 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment? As illustrated in figure 8, participants identified (a) policy impact and change on the organization, and (b) policy communication as themes.

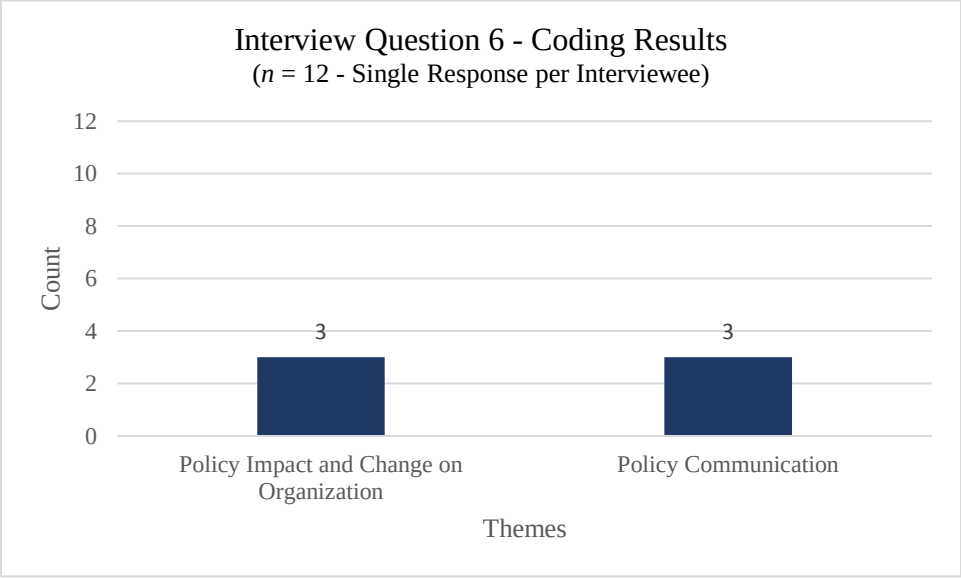

Figure 8. Themes and frequencies of responses associated with interview question 6.

Policy impact and change on organization. Once a policy has been developed through the established institutional process and approved through the appropriate committees or leadership groups, P12 acknowledged the variance between the intention of the policy as opposed to how the policy was interpreted by the university community. Additionally, once the policy has been implemented, concerns with regard to consistent application were expressed. Despite the existence of a well-thought-out policy, P1 identified the biggest challenge as "not letting the policy go on the shelf and doing nothing" (personal communication, March 1, 2016). In P3's assertive opinion, policy does not change culture.

Policy Communication. Equally reported, three of the 12 participants expressed the challenge with communicating new or updated policies. P12 expressed the frustration with encouraging the campus community to read new or updated policies. P10 shared this sentiment: "Making people understand that there has been a change and they need to attend to it—that is a constant issue" (personal communication, March 17, 2016).

Interview question 6 summary. Participants expressed two themes in response to the sixth interview question, IQ 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment? Participants identified (a) policy impact and change on the organization, and (b) policy communication as themes. Once a policy has been developed participants acknowledged the variance between the intention of the policy as opposed to how the policy was interpreted by the university community. Additionally, once the policy has been implemented, concerns with regard to consistent application were expressed. Equally reported, three of the 12 participants expressed the challenge with communicating new or updated policies and frustration with encouraging the campus community to read new or updated policies.

Interview question 7. Participants expressed four themes in response to the seventh interview question, IQ 7: How did you deal with and/or overcome those challenges? As illustrated in figure 9, participants identified (a) communication and collaboration, (b) leadership and interpersonal skills, (c) clearly defined processes, and (d) supportive organizational structure.

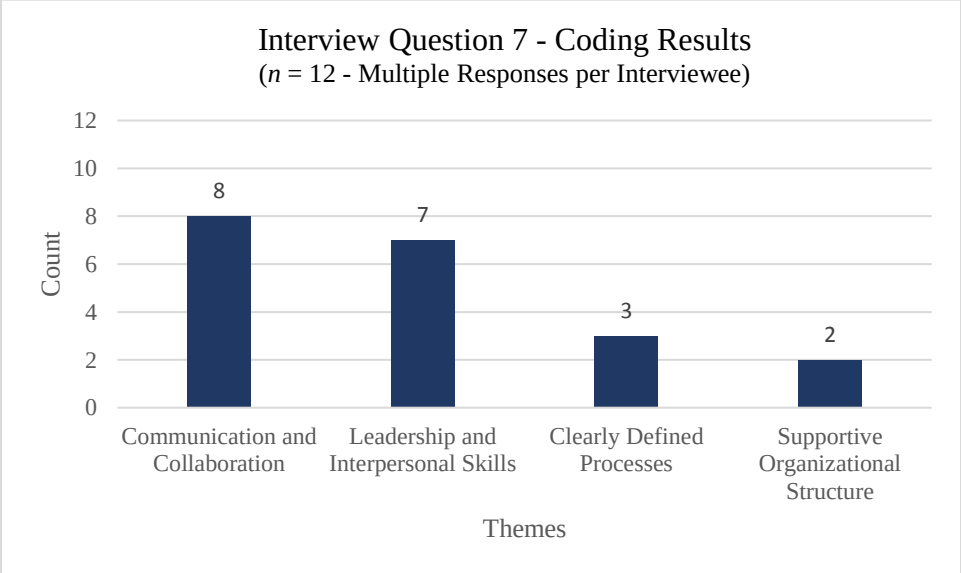

Figure 9. Themes and frequencies of responses associated with interview question 7.

Communication and collaboration. As the most common theme expressed by policy administrators, sentiments regarding communication and collaboration were described by eight of the 12 participants. Seven of the eight participants indicated that communicating in-person was key to overcoming the challenges expressed in the previous interview questions. As an alternative to communicating via email, P12 recommends that the university community should engage in conversation. Although the policy committee meets formally once a month, P6 admittedly meets with policy stakeholders informally, up to twice a week as a method to "soften the ground, prior to formally introducing the policy" (personal communication, March 8, 2016).

Leadership and interpersonal skills. Seven of the 12 participants (58%) described leadership skills and interpersonal skills as necessary for overcoming challenges. P9 provides an introspective look into policy development and simply states,

> It requires a lot of patience . . . you've got to talk to people, and talk to them, and talk to them, and talk to them again and listen to their fears and let them vent, and then let them talk to you and give you all their anecdotes, and every which way they think it could go wrong. (personal communication, March 17, 2016)

P11 expressed that maintaining transparency is an important aspect, while P12 shared an important reminder that policy administrators should be "open minded about how we are dealing with things." P10 and P12 discussed the significance of due diligence throughout the process, and that rectifying an approved policy is much more difficult.

Clearly defined processes and supportive organizational structure. Although only three of the policy administrators identified a clearly-defined policy development process as a method for overcoming challenges, P4 describes the institution's process as one that is designed to negate surprises. Two of the 12 participants credited a supportive organizational structure as a

method for overcoming challenges. Under P5's organizational structure, having a direct line to the board of trustees helps to alleviate many of the political challenges associated with policy conflict or controversy.

Interview question 7 summary. Participants expressed four themes in response to the seventh interview question, IQ 7: How did you deal with and/or overcome those challenges? Participants identified (a) communication and collaboration, (b) leadership and interpersonal skills, (c) clearly defined processes, and (d) supportive organizational structure. Eight of the 12 participants described communication and collaboration as the most common theme expressed by policy administrators. Seven of the 12 participants (58%) described leadership skills and interpersonal skills as necessary for overcoming challenges. Three of the policy administrators identified a clearly-defined policy development process as a method for overcoming challenges and two of the 12 participants credited a supportive organizational structure as a method for overcoming challenges.

Research question 2 summary. Three interview questions helped to explore the second research question: What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment? To explore this further, participants were asked the following questions:

> IQ 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to prevention and mitigation of cyber-harassment?
>
> IQ 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment?
>
> IQ 7: How did you deal with and/or overcome those challenges?

Participants expressed four major themes in response to IQ 5: (a) organizational culture, (b) policy and the policy development process, (c) social and political environment, and (d) resources. All the participants referenced the effect and impact that organizational culture had on developing and implementing a policy. In discussing challenges and obstacles, participants were candid in sharing observed conflict between departments. Some participants offered their personal sentiments and frustrations with other people. Ten of the 12 participants expressed frustration with writing the actual policy or with the policy process itself, illustrating the personal challenge of having to draft a comprehensive and impactful policy within a constrained amount of time. It is worthwhile mentioning two additional themes that surfaced: the impact that the social and political environment has on policy development, and the challenge of identifying the resources necessary to operationalize or execute the provisions outlined in the policy.

In response to interview question 6, what were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment? participants provided examples that were categorized into two themes: (a) the policy impact and change on the organization, and (b) policy communication. Once a policy has been developed and approved through the appropriate committees or leadership groups, participants acknowledged the variance between the intention of the policy versus how the policy was interpreted by the university community. Additionally, once the policy has been implemented, concerns with regard to consistent application were expressed. Equally expressed, participants noted the challenge with regard to communicating approved policies to the university community.

Interview question 7 asked participants to help explore challenges they are faced as policy administrators. The following four themes were identified: (a) communication and

collaboration, (b) leadership and interpersonal skills, (c) clearly defined processes, and (d) supportive organizational structure. As the most common theme expressed by policy administrators, sentiments regarding communication and collaboration were described by eight of the 12 participants. Seven of the 12 participants described leadership skills and interpersonal skills as necessary for overcoming challenges.

Research Question Three

Research question three asked: How do higher education institutions measure the success of cyber-harassment policies and procedures? To address this question, participants were asked the following five interview questions:

IQ 8: How does your institution measure the success of cyber-harassment policies and procedures?

IQ 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment?

IQ 10: How do you assess your interim success through the policy development and implementation process? For instance, how did you know things were going according to plan?

IQ 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure?

IQ 12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program?

Interview question 8. Given that all participants reported the absence of a cyber-harassment policy at their respective institutions, when participants were asked IQ 8, how does

your institution measure the success of cyber-harassment policies and procedures? participants would not or could not provide a thorough response. P1 simply responded with “no” while P11 politely responded with “I don’t think we do. P7 was generous enough to provide potential recommendations, but began the response with “I don’t know.” P7 continued with the following recommendation:

> One thought would be if there is an office, say it’s in Student Life, or maybe Equity, Diversity, Inclusion, if they’ve been receiving a lot of complaints, concerns, or calls from people about that topic after the policy was implemented . . . if the calls were reduced, or if there are more calls, is the policy addressing the issues that the calls are coming in about?

Interview question 9. Illustrated in figure 10, participants expressed three major themes in response to the ninth interview question, IQ 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment? Given that no cyber-harassment policy existed, participants referenced other behavioral policies. Responses were in alignment with those behavioral policies. Participant responses were categorized as follows: (a) no formalized evaluation method, (b) evaluation metrics, and (c) review process.

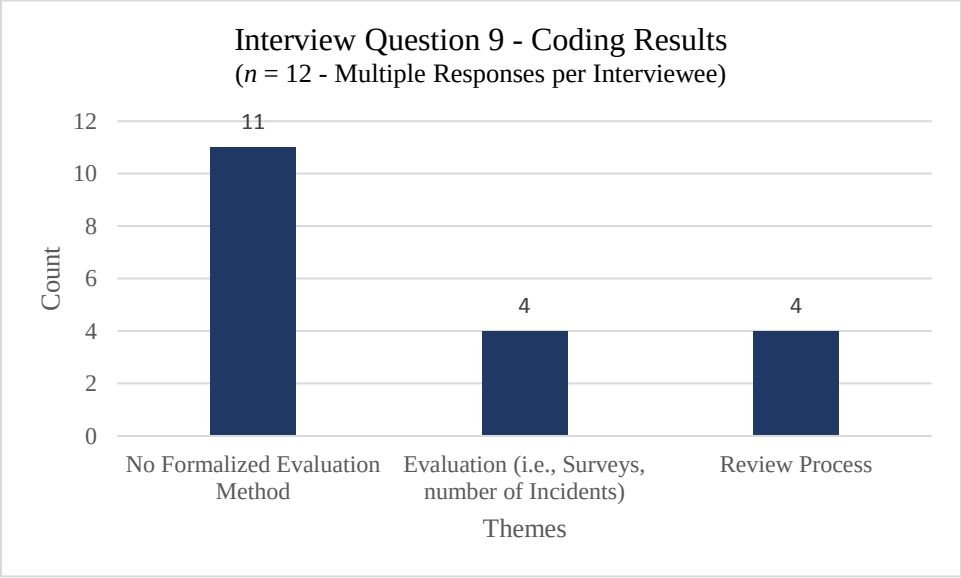

Figure 10. Themes and frequencies of responses associated with interview question 9.

No formalized evaluation method. Eleven of the 12 participants (92%) expressed that their institution did not have a formalized evaluation method to measure the success of a cyber-harassment policy. P1 expressed the desire: "I wish I could say we do something, but to be honest with you, we really don't" (personal communication, March 1, 2016). P5 indicated that "there is not a requirement for that to be in place" stating further that "if a policy owner is serious about what they are compelling folks to do, then I feel like they should have the strategic foresight to put something in place" (personal communication, March 8, 2016). P7 suggested that evaluation would be done on a unit or department basis. P6 acknowledged that the institution was known for their assessment and measurement capabilities, but hesitantly admitted that "this is an embarrassing response. We don't do a terrific job of assessing our policies" (personal communication, March 8, 2016).

Evaluation (i.e., surveys, number of incidents). P8 was the only participant who provided a thoughtful discussion with regard to evaluation methods. Over the past five or ten years, the institution has placed more emphasis on compliance and risk tolerance, and as a result,

initiated a "process to identify measures of success, metrics for policies, and training related to risk" (personal communication, March 14, 2016). P8 expands upon this discussion:

> Although it seems counter intuitive, success is getting more reports about cyber-harassment. Not sure how you measure this, but having people not afraid to report, so having some trust of the people who investigate or provide support for the person who is receiving it [*sic*] (personal communication, March 14, 2016)

Four participants provided a method in which some form of assessment was conducted. However, all neglected to provide an evaluation method that would specifically measure the success of a cyber-harassment program. P1 indicated that the institution distributes campus climate surveys. P4 began by indicating that the evaluation method would depend upon the nature of the policy; however, P4 continued to suggest that behavioral policies are more difficult to assess, and that an institution is limited to quantifying the claims reported. P12 indicated that an evaluation method is the "next frontier for the compliance unit;" however, P12 clarified by stating that the compliance unit is limited to "me, myself, and I" (personal communication, March 29, 2016).

Review process. P1, P4, P5, and P6 noted that what they do have in place is a set time period for which policies are reviewed for updates, modifications, or enhancements. P1 indicated that the review period varies, and is dependent on what is most appropriate for that policy, whereas P4 has a comprehensive review scheduled for every four years. P6 has regularly scheduled reviews as frequently as every 18 months.

Interview question 9 summary. participants expressed three major themes in response to the ninth interview question, IQ 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and

mitigation of cyber-harassment? Participant responses were categorized as follows: (a) no formalized evaluation method, (b) evaluation metrics, and (c) review process. Eleven of the 12 participants (92%) expressed that their institution did not have a formalized evaluation method to measure the success of a cyber-harassment policy. Four participants provided a method in which some form of assessment was conducted. However, all neglected to provide an evaluation method that would specifically measure the success of a cyber-harassment program. Four participants noted that what they do have in place is a set time period for which policies are reviewed for updates, modifications, or enhancements.

Interview question 10. Illustrated in figure 11, participants expressed three major themes in response to IQ 10: How do you assess your interim success through the policy development and implementation process? For instance, how did you know things were going according to plan? Participant responses were themed as follows: (a) defined processes and procedures, (b) meeting the milestones with the process, and (c) no formalized evaluation method.

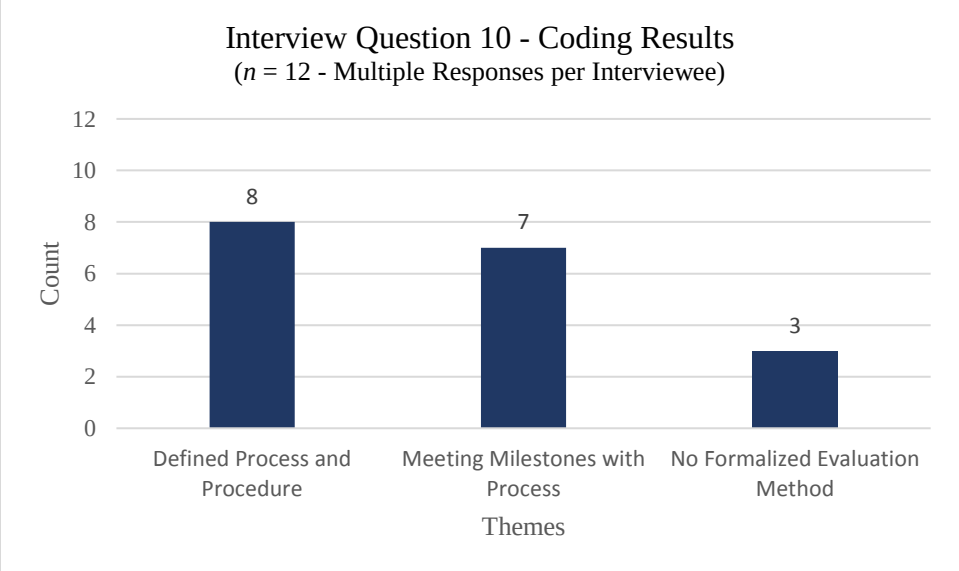

Figure 11. Themes and frequencies of responses associated with interview question 10.

Defined process and procedure. Of the 12 participants, eight (66%) identified a defined process and procedure as the most common theme. Participants indicated that policy development was a "linear progression" and that policies could be "rejected if not aligned, go back and start again and turned back entirely" (personal communication, March 17, 2016). P1's process is initiated by a proposal to create or revise an existing policy. Although a linear progression through time is seen as successful progress by some, time in itself cannot be a measurement as in the case of P3, where it was reported that one policy took as long as five years to get published. Given the complexity of the discussion, review, and multi-approval process, "by the time university risk and compliance got back to me, it was already outdated" (personal communication, March 3, 2016).

Meeting milestones with process. The second theme that emerged from participant responses indicated that meeting milestones within the process was an indicator of interim success. For P1, attaining an executive level sponsor to support the policy was a measure of interim success. Similar to P6, clearly identifying a chair or department sponsor is seen as an indicator of progress. Although P7 acknowledged that some policies may go through the process more quickly than others, consensus among the policy review group was an indicator of progress. From P8's perspective, meeting with each responsible office and communicating is considered interim success, whereas from the perspective of P3, "Success is exemplified by the fact that, excuse my language, we got the dang thing published" (personal communication, March 3, 2016).

No formalized evaluation method. For the final theme identified, three participants indicated that they lacked a formalized evaluation method to identify interim success. P11 indicated uncertainty as to how success could be measured. P6 provided an insightful perspective

in that receiving no feedback or response from the university community may be seen as interim success in certain scenarios, suggesting that either the proposed policy was well-thought out, or the policy itself contributed to the greater good.

***Interview question 10 summary*.** Participants expressed three major themes in response to IQ 10: How do you assess your interim success through the policy development and implementation process? Participant responses were themed as follows: (a) defined processes and procedures, (b) meeting the milestones with the process, and (c) no formalized evaluation method. Eight (66%) of the 12 participants identified a defined process and procedure as the most common theme. The second theme that emerged from participant responses indicated that meeting milestones within the process was an indicator of interim success. For the final theme identified, three participants indicated that they lacked a formalized evaluation method to identify interim success.

Interview question 11. Participants expressed four themes in response to the eleventh interview question, IQ 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure? As illustrated in figure 12, participants identified (a) written policy elements, (b) resources, (c) organizational culture, and (d) communication and dissemination.

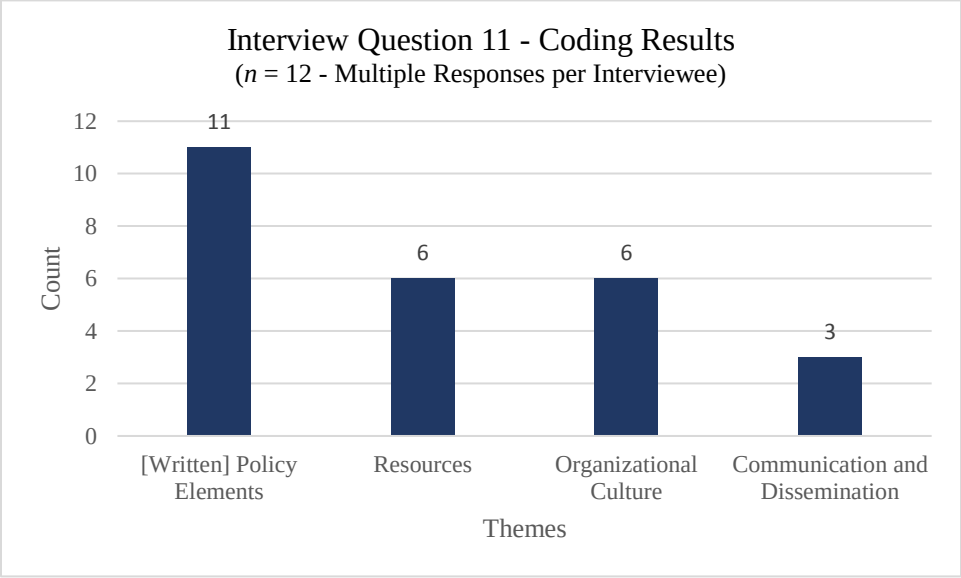

Figure 12. Themes and frequencies of responses associated with interview question 11.

Written policy elements. Of the 12 participants interviewed, 11 participants described specific provisions that they recommended be included in support of a successful prevention and mitigation cyber-harassment policy and program. Based on their experience, participants suggested that policy statements include (a) the definition of cyber-harassment, (b) a clearly written policy statement emphasizing the institution's position regarding this behavior, (c) who this policy applies to, (d) what an individual should do if they witness the behavior, (e) who to report the behavior to, (f) what the institution must do in response to receiving a report, (g) disciplinary measures or sanctions for non-compliance, and (h) any laws governing this behavior. Important pieces of information to include are (a) the effective date of the policy, (b) responsible officer or office, and (c) contact information for where to get assistance or support.

Additionally, participants provided specific guidance as to how the policy statements should be written. P2 recommended that the policies be specific, while P3 recommended that policies be written broadly, yet informative. P11 indicated that policies should be written in a

manner that those who do not have law degrees can understand, and P12 suggested that policies should be "readable to the layperson" (personal communication, March 29, 2016).

Resources. Fifty percent, or six of the participants, identified resources as a necessity for a successful prevention and mitigation policy and procedure. Resources including counseling services, victim advocacy, provisions for anonymity or a hotline for reporting, education, and training.

Organizational culture. Additionally, 50% of participants recognized the role that the organizational culture played on the success of a prevention and mitigation program. P8 expressed the importance of the institution's commitment to proactive prevention efforts. P5 expressed that the policies' effectiveness is increased when the policy is in alignment with the institution's mission. P3 noted the role that executive leadership played in influencing a behavioral policy.

Communication and dissemination. Three of the 12 participants stressed the importance of operationalizing a policy and program. They emphasized that active communication and increasing awareness were vital to introducing policies and programs across the various institutional constituencies.

Interview question 11 summary. Participants expressed four themes in response to the eleventh interview question, IQ 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure? Participants named (a) written policy elements, (b) resources, (c) organizational culture, and (d) communication and dissemination. Of the 12 participants interviewed, 11 participants described specific provisions that they recommended be included in support of a successful prevention and mitigation cyber-harassment policy and program. Fifty percent, or six of the participants,

identified resources as a necessity for a successful prevention and mitigation policy and procedure. Additionally, 50% of participants recognized the role that the organizational culture played on the success of a prevention and mitigation program and three participants stressed the importance of operationalizing a policy and program.

Interview question 12. Illustrated in figure 13, participants expressed two themes in response to IQ 12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program? Given that all participants reported the absence of a cyber-harassment policy at their respective institution, all but one participant would not or could not provide a thorough response.

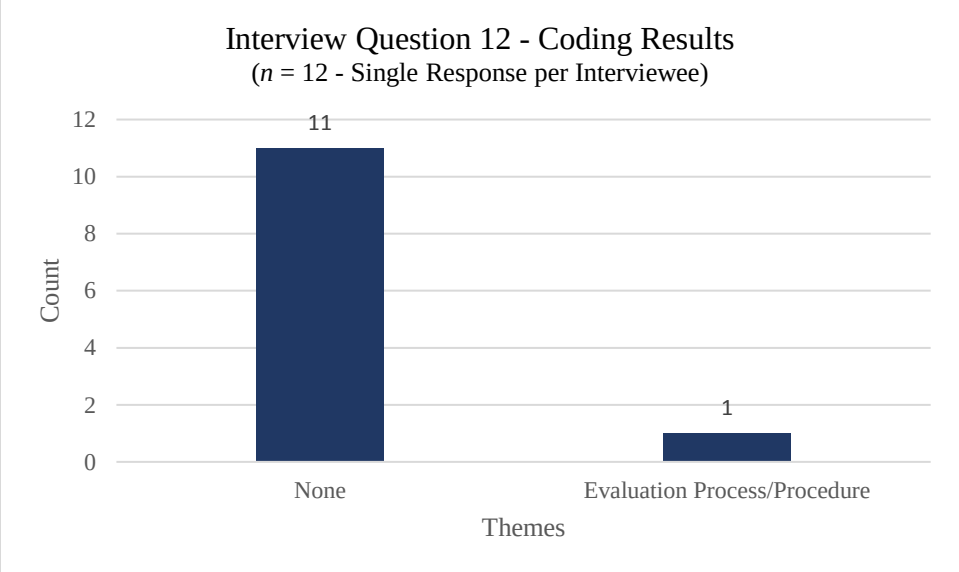

Figure 13. Themes and frequencies of responses associated with interview question 12.

Although in the initial planning stages, P8 described the proposed plans by which the institution will begin assessing policy success. The institution leverages the support of audit, "so at any point, I can go in and see over the past three months what were the top policies that we had audit findings for" (personal communication, March 14, 2016). Additionally, the institution has an investigation tracker that indicates violations of policies. The third tool referenced was the

anonymous hotline. The proposed plan is to fully utilize these tools, and integrate them into a report for senior leadership.

Research question 3 summary. Interview questions eight through 12 helped the researcher explore the third research question: How do higher education institutions measure the success of cyber-harassment policies and procedures? Given that participants could not reference a cyber-harassment policy, participants responded to the best of their ability or addressed the question, leveraging their previous experience with similar types of policies. Participants would not or could not provide a thorough response to the eighth interview question: How does your institution measure the success of cyber-harassment policies and procedures? as none of the participants had a policy to measure.

In response to IQ 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment? participants provided responses that were aligned to similar behavioral policies. Participant responses were categorized as follows: (a) no formalized evaluation method, (b) evaluation metrics, and (c) review process, where 11 of the 12 participants had no formalized evaluation method. One of the participants provided a thoughtful response, but clarified that this was something in development and would take some time to fully implement. Four participants provided a method in which some form of assessment was conducted. However, all neglected to provide an evaluation method that would specifically measure the success of a cyber-harassment program.

When asked IQ 10, how do you assess your interim success through the policy development and implementation process? participant responses were themed as follows: (a) defined processes and procedures, (b) meeting the milestones with the process, and (c) no

formalized evaluation method. Eight (66%) participants indicated that policy development was a "linear progression" (P10, personal communication, March 17, 2016). The second theme that emerged from participant responses indicated that meeting milestones within the process was an indicator of interim success. For the final theme identified, three participants indicated that they lacked a formalized evaluation method to identify interim success, expressing uncertainty as to how they would measure success.

Participants expressed four themes in response to the eleventh interview question, IQ 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure? Eleven of the 12 participants described specific provisions that they recommended be included in support of a successful prevention and mitigation cyber-harassment policy and program. Fifty percent, or six of the participants, identified resources as a necessity for a successful prevention and mitigation policy and procedure. Additionally, 50% of participants recognized the role that the organizational culture played on the success of a prevention and mitigation program.

Participants expressed two themes in response to IQ 12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program? Given that all participants reported the absence of a cyber-harassment policy at their respective institutions, all but one participant would not or could not provide a thorough response.

Research Question Four

Research question four asked: What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures? To address this question, participants were asked the following two interview questions:

IQ 13: What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program?

IQ 14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study?

Interview question 13. Illustrated in figure 14, participants expressed four themes in response to IQ 13: What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program? Participant responses were themed as follows: (a) ethical and cultural considerations, (b) process, (c) utilization of resources, and (d) written policy.

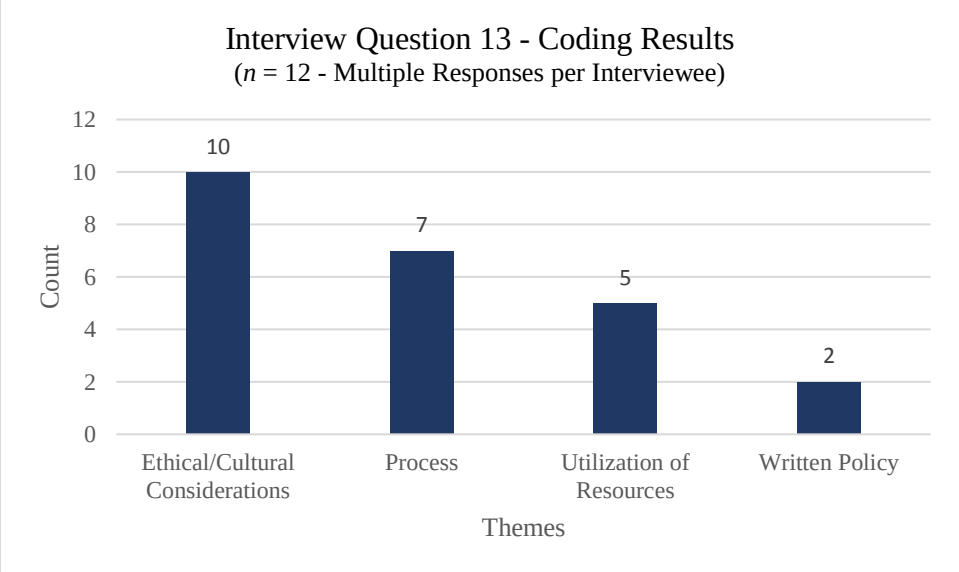

Figure 14. Themes and frequencies of responses associated with interview question 13.

Ethical/Cultural considerations. Of the 12 participants, ten (83%) responded with ethical and cultural considerations. P1 expressed the importance of communication, and "getting everybody in the same room because there is going to be a lot of different views and voices that are interested in this area" (personal communication, March 1, 2016). As policy administrators seek to understand the impact a topic may have on the university community, P4 recommended

understanding one's institution's risk tolerance. P3 described the subject area as "volatile, and it's becoming more difficult, by the ways that technology is used to do bad things" (personal communication, March 3, 2016). P8 recommends that policy administrators understand

> the orientation of your university, what meaning do they make of cyber-harassment, and that's what drives it. Often we get it backwards, we write the policy. . . look at other universities, then figure out what we want (personal communication, March 14, 2016)

Process. Seven participants touched on the process of policy development, highlighting the necessity to establish a consistent process for policy development and implementation. P4 provided a reminder that often legislation outlines the specific elements that need to be included in a policy. P5 reiterated the importance of shared governance in higher education, encouraging communication and collaboration. P8 amplified this point and recommended institutions to

> look broadly and bring in everyone who is connected: police, residence hall, student life, communications; every university knows who their important constitutions [*sic*] are: the people who may not know anything about cyber-harassment but know about the university; and then you have the people who may not know the university, but know everything about cyber-harassment; so you really need to bring those people forward, together, to figure out what you want to accomplish, and from that, write your policy. It's bigger than just your policy. (personal communication, March 14, 2016)

Utilization of resources. Although less than half of the participants reiterated the efficient and effective use of resources, P1 encouraged the use of subject matter expertise available within your institution.

Interview question 13 summary. Participants expressed four themes in response to IQ 13: What recommendations would you make for higher education institutions as they begin to

design and implement a cyber-harassment prevention program? Participant responses were themed as follows: (a) ethical and cultural considerations, (b) process, (c) utilization of resources, and (d) written policy. Of the 12 participants, ten (83%) responded with ethical and cultural considerations. Seven participants touched on the process of policy development, highlighting the necessity to establish a consistent process for policy development and implementation and less than half of the participants reiterated the efficient and effective use of resources.

Interview question 14. Participants expressed four themes in response to the final interview question, IQ 14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study? As illustrated in figure 15, five (41%) participants provided no additional recommendations, and the remaining participants expressed final thoughts regarding the policy development process, organizational culture, and resources.

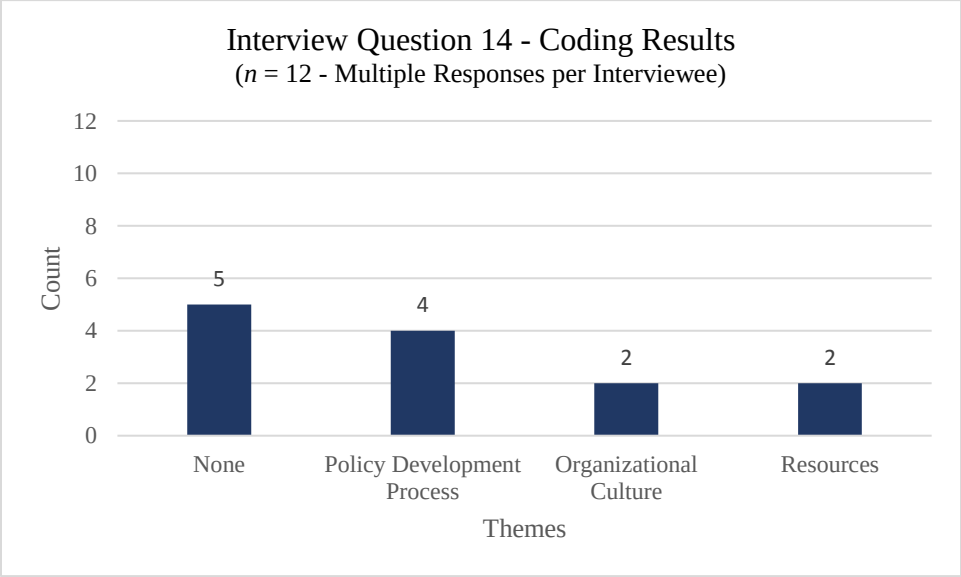

Figure 15. Themes and frequencies of responses associated with interview question 14.

As final thoughts, four participants took the opportunity to express their personal sentiments or to reiterated previously discussed themes. P2 restated the importance of having effective policies, and P3 addressed the need for policy developers to learn to "broker compromise" (personal communication, March 3, 2016). Two (16%) participants touched on organizational culture, encouraging policy developers to develop a policy that fits the culture of the organization. As final thoughts, two participants reemphasized that resources are readily available for guidance and support.

Research question 4 summary. Two interview questions helped to explore the final research question: What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures? For IQ 13, what recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program? participants expressed four themes as follows: (a) ethical and cultural considerations, (b) process, (c) utilization of resources, and (d) written policy. Participants expressed four themes in response to the final interview question, IQ 14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study? Five participants provided no additional recommendations or commentary, and the remaining participants expressed final thoughts regarding the policy development process, organizational culture, and resources.

Summary

The first four interview questions helped to explore the initial research question: What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment? From the coding, themes for strategies and best practices emerged. As the first interview question revealed, none of the represented institutions had a cyberbullying or cyber-

harassment policy implemented. Most institutions addressed cyber-harassment within the framework of an existing policy while a few policy administrators provided a definition based on their education and professional experience. In referencing similar policies, policy administrators revealed that education and training, written policy statements, a formalized policy development process, outreach to university constituents, active management and oversight, and having dedicated resources were among the best practices for the prevention and mitigation of cyber-harassment in higher education.

Three interview questions helped to explore the second research question: What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment? Policy administrators identified organizational culture, the social and political environment, policy development process, resources, policy impact on an organization, and policy communication as major challenges. To overcome these challenges, having clearly defined processes, a supportive organizational structure, communication and collaboration, and leadership and interpersonal skills help to negate these challenges.

Interview questions eight through 12 helped the researcher explore the third research question: How do higher education institutions measure the success of cyber-harassment policies and procedures? Most institutions lack a formalized evaluation method, and success is primarily measured as a continuum of time or through the completion of policy approval milestones. Successful programs will include an intersection of resources and processes, outlined within a framework of a policy. The final two interview questions helped to explore the last research question: What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures? Policy administrators reiterated

many of the themes explored in the previous research questions, resurfacing the notion of the complexities of policy development in higher education.

Chapter 5: Conclusions and Recommendations

Cyberbullying is a growing phenomenon, summarized as "a bullying problem occurring in a new territory" (Li, 2006, p. 166). Although no federal law specifically addresses cyber-harassment in higher education, institutions have a legal obligation to address all claims of harassment, regardless of the location or platform in which the harassing behavior occurs. With insufficient regulatory guidance addressing online codes of conduct, institutions are faced with potential legal risk and unknown levels of vulnerability (Fisher, 1995). Recent court cases are setting precedents for obligatory institutional response and potential penalties for lack thereof; conversely, institutions are left to their own devices to develop and employ policy statements and sanctions that prohibit or discourage cyber-harassment behaviors. As the legal and political environment regarding bullying and cyberbullying behaviors continues to evolve, universities are challenged to administer policies and procedures that address misconduct that occurs in physical and virtual environments.

Participants in this research study provided key insights regarding strategies, best practices, and challenges experienced by policy administrators when developing and implementing prevention and mitigation policies and programs. In an effort to seek further understanding, this study employed a phenomenological method. Members of the Association of College and University Policy Administrators (ACUPA) were invited to participate in this study. Efforts to recruit participants was terminated upon the identification of 12 eligible participants. In an effort to seek further understanding, 12 participants, representing 12 unique institutions of higher education, participated in an interview in which the researcher asked 14 interview questions. The data for this study was collected from the participants throughout the month of

March 2016 via semi-structured interviews. In an effort to seek further understanding, this study employed a phenomenological method in addressing the following research questions:

- What strategies and practices do higher education institutions employ to prevent and mitigate cyber-harassment?
- What challenges do higher education institutions face in implementing policies to prevent and mitigate cyber-harassment?
- How do higher education institutions measure the success of cyber-harassment policies and procedures?
- What recommendations would higher education institutions make for future implementation of cyber-harassment policies and procedures?

Results and Discussion of Findings

Technology has increased the effectiveness and efficiency of communication. Despite the benefits, the introduction of such technologies provides for a format in which malicious behaviors can occur (Beran & Li, 2005; Francisco, Veiga Simão, Ferreira, & Martins, 2015). The development and expansion of information and communication technologies, introduced several types of malevolent behaviors (Kubiszewski, Fontaine, Potard, & Auzoult, 2015; Willard, 2005), including "deleterious social interactions such as cyberbullying" (Kubiszewski et al., 2015, p. 49).

Cyber-harassment defined. The institutions of all the participants interviewed lacked specific policies that addressed cyber-harassment. To explore this in more detail, all of the participants were able to cite an existing institutional policy that could be applied in the event of a cyber-harassment scenario. Some participants confidently referenced existing policies, noting their broad applicability. This range of policies included a Harassment Policy, Sexual

Harassment Policy, Sexual Misconduct Policy, Acceptable Use and Network Security Policy, Responsible Use Policy, Discrimination and Harassment Policy, Title IX Policy, Violence Policy, Social Media Policy, and Student Code of Conduct Policy.

Institutions have clearly established policies that address bullying, harassment, and technology; however, none of the participants' institutions have established policies that uniquely address the divergence of this phenomenon. This variance and inconsistency is reflective of the challenges in interpreting and complying with the range and variability found in state and federal regulation. Although legislators have expressed full support and endorsement for state and federal regulation with regard to bullying in the schools, the intersection of existing laws including the Violence Against Women Act (2014), Title IX of the Education Amendments (1972), Title VII of the Civil Rights Act (1964), and the Clery Act (1998) mirror this vague approach to policy administration in higher education. Sacco et al. (2012) noted that although most state laws provide definitions of bullying behaviors, the definitions vary greatly, and the definitions as outlined in policy "do not follow research-based definitions of bullying" (p. 4). To add further complexity, policy administrators' definitions of cyber-harassment vary among participants. One participant described cyber-harassment as "unsolicited or unwelcomed messages from identified or unidentified individuals in which there are threatening or unwelcomed comments" (P3, personal communication, March 3, 2016), and another elaborated upon this definition to specify activity that is conducted "using technology to post inappropriate pictures or things that would be viewed inappropriate" (P5, personal communication, March 8, 2016).

Again, the variance and inconsistency in the participants' responses is reflective of the challenges expressed in scholarly research and in state legislation. Definitions of cyberbullying

are fundamentally derived from definitions of bullying, where conduct is defined as bullying behaviors that are facilitated by information and communication technologies (Kubiszewski et al., 2015). Crosslin and Golman (2014) defines cyberbullying as repeated, unwanted harassment or aggressive behavior conducted through the use of technologies. According to Besley (2009), the to be classified as cyberbullying, there must be an intent to harm the victim (as cited by Tokunaga, 2010). Olweus (2013) defined cyberbullying as "bullying performed via electronic means, such as mobile/cell phones or the internet [*sic*]" (p. 521). Policy administrator's definitions of cyber-harassment mirror similar variation and range with the definitions expressed through scholarly literature.

Strategies and practices for policy administrators. Given that all participants lacked a cyber-harassment policy and program, participants leveraged their personal experiences in similar policies. Similar policies and programs referenced included the Title IX program, Diversity Policy, freshman orientation, a Crisis Action Team (CAT), and Diversity Week campaigns. Participants' responses fell into three major themes; education and training, management and oversight, and clearly established policies and procedures.

Participants expressed the need to provide education and training, especially in the areas in which policies are developed with the intention of motivating behaviors throughout the university community. Examples of mechanisms and forums in which education was distributed range from information disclosure to traditional educational platforms such as formalized courses. Participants referenced training opportunities, and described education being delivered through face-to-face and virtual formats. Additionally, education and training was not limited to specific groups within the organization. Participants noted trainings that were general enough for the university at large, and trainings developed specifically for a particular audience, such as

students, staff, and faculty groups. P10 highlighted the notion that it was vital for those responsible for administering the policy to receive specific education and training as well, noting the specialized training that Title IX coordinators received from the Legal department.

To ensure that policies are adopted to their full extent, it is necessary to access organizational resources while leveraging relationships within the university community (Schmieder-Ramirez & Mallette, 2007). Kirkpatrick (2008) shared similar sentiments indicating that dedicated personnel are necessary to assess current operations, evaluate impact to operations and resources, plan a strategy for implementation, facilitate for implementation, and evaluate for effectiveness. Management oversight and identifying resources was the second theme noted by participants in the study. As colleges and universities develop policies and programs for the prevention and mitigation of cyber-harassment, the organizations must consider the "time, energy, and resources" (Bolman & Deal, 2013, p. 295) necessary.

The third theme expressed by participants, clarified the necessity of having a written policy that outlined the specifics of a prevention and mitigation program. The participants' attitudes mirrored the sentiments reflected through recent legislation, requiring that institutions publish clear policy statements with regard to campus safety and security. In addressing policy implementation strategies and best practices, participants expressed the importance of having a formalized policy development process, outreach with respective stakeholders, and education and training efforts. Policy development processes ranged in complexity, inclusive of formal and informal policy development procedures. P5 described a formal approval process, requiring endorsement for proposed policies from the Staff Council president, Faculty Council president, and Student Council president. Once the policy standards have been established, institutions can coordinate efforts between leadership, subject matter experts, and university constituencies.

Senior management participation and support are fundamental in implementing change at an organization. Once objectives are established, implementing a policy may require the collaboration of subject matter expertise from a cross-functional team of experts.

Outreach with the university community was a theme expressed by participants. P8 stressed the importance of face-to-face discussions and focus groups as a way to socialize a policy into the university community. P2 describes a process that solicits conversation, that "creates an environment that encourages participation" (personal communication, March 2, 2016). To gain support from the university community, Cohen (2005) recommends communicating "sound business rationale that is based on facts as well as on possible consequences" (p. 15). Again, as participants discussed implementation process techniques and methods, education and training surfaced as the third theme. As a policy is approved and implemented, P4 stressed the importance of public disclosures and fully informing the campus community of the new or revised policy.

Challenges for policy administrators. When addressing the challenges related to developing and implementing policies related to the prevention and mitigation of cyber-harassment, participant responses were categorized in four distinctive themes: (a) organizational culture, (b) policy development process, (c) social and political environment, and (d) resources. All participants discussed the challenges they faced internally within the organization. It is important to acknowledge the organizational culture, taking into consideration the "connectedness that makes up the social community of the organization" (Schmieder-Ramirez & Mallette, 2007, p. 7). Catherine E. Lhamon, Assistant Secretary for Civil Rights, applauded Princeton University's policy change implementation with regard to "its commitment to ensuring

a community-wide culture of prevention, support, and safety, for its students, staff, and community" (U.S. Department of Education, 2014b, para. 1).

Participants exploited the opportunity to discuss the challenges between individuals and between departments, noting the inherent conflict that may surface within an organization. When developing and implementing policy, there is an opportunity in which changes to policy and procedure may have a greater impact on some individuals, in that some individuals may exhibit "more passion or interest than others" (P7, personal communication, March 10, 2016). Although all conflict isn't entirely avoidable, P3 described how some have reacted to the conflict in that "people are reluctant to speak up because they feel like their opinions, or what they have to say, or how they say it, may be misconstrued by the other side" (personal communication, March 3, 2016).

Over 80% of the participants interviewed indicated that writing the policy and the policy development process itself was a challenge. P8 is challenged with identifying language that "people are comfortable with" (personal communication, March 14, 2016) while P12 was concerned with ensuring that the policy language captures "the depth and breadth" (P12, Personal Communication, March 29, 2016) of the institution's intent. Institutions must establish a policy that is reflective of the risk tolerance of individual institutions. P8 described the institutions policy development process as a mechanism to facilitate change. When embarking on organizational change, "mission, strategy, leadership, and culture have more weight than structure, management practices, and systems" (Burke & Litwin, 1992, p. 529).

Although not a common theme expressed by participants, it was important to note the challenges that policy administrators faced when internal change was as a result of external societal and political environments. Burke and Litwin (1992) acknowledged these external

societal and political environmental forces that "as a consequence require significantly new behavior from organizational members" (Burke & Litwin, 1992, pp. 529-530). Changes in recent legislation served as the external political force driving internal policy and procedural change, which ultimately impacted the organization through policy, process, and procedure—all of which required organizations to respond and change. These changes solicited a reactionary response on behalf of the institutions, and the institutions were faced with the challenge of interpreting and implementing legislative regulation. However, as with any piece of legislation, there is room for interpretation.

Cyber-harassment in higher education rose to the forefront of the public agenda after events were broadcasted in the media (Tokunaga, 2010). The case of the unfortunate suicide of Tyler Clementi, at Rutgers University in New Jersey (Crosslin & Golman, 2014; Foderaro, 2010) served as another example of a societal and political driver encouraging policy change in higher education. P3 described the subject area as "volatile, and it's becoming more difficult, by the ways that technology is used to do bad things" (personal communication, March 3, 2016). In an effort to overcome these challenges, participant's responses were categorized in four themes: (a) communication and collaboration, (b) leadership and interpersonal skills, (c) clearly defined processes, and (d) supportive organizational structure. As one of the 11 key components among state cyber-bullying laws, Stuart-Cassel et al. (2011) identified a communication plan as a necessary component. Although some participants expressed having a formalized process that innately encourages discussion and collaboration among university stakeholders, having informal in-person conversations was a method to which a policy administrator could "soften the ground" (personal communication, March 8, 2016).

Some participants described their policy development and implementation process as inherently built with a mechanism to solicit feedback, adhering to a procedure does not negate the need for leadership and interpersonal skills. Burke (2011) identified leadership as one of the transformational dimensions in their causal model, specifically stating that "leadership is about vision; change; using one's intuition, influence, persuasion . . . and rewarding people with personal praise and providing opportunities to learn new skills" (p. 220). As a method to overcome challenges, participants described qualities and attributes including patience and being "open minded about how we are dealing with things" (P12, personal communication, March 29, 2016).

How policy administrators measure success. Given that all participants reported the absence of a cyber-harassment policy at their respective institutions, when participants were asked interview questions with regard to measuring the success of cyber-harassment policies and procedures, participants would not or could not provide a thorough response. Some of the policy administrators provided examples that served as assessments or assessment tools, including surveys or counting the number of infractions. However, none of the participants provided examples of methods or processes for measuring the success of a policy or program.

In the areas of meeting legislative requirements, institutions' evaluations are simplified as to whether or not the institution complied with the legal requirements. In a study conducted by SAFER and V-Day (2013) reviewing the effectiveness of policies from 299 4-year institutions of higher education, 32.6% did not fully comply with the legislative requirements for public disclosure of policies. In the event that the laws are so vague or ambiguous, as in the case of cyber-harassment, it is reasonable to expect that higher rates of noncompliance. Though some participants expressed that a written policy itself can serve as the educational tool, a program

cannot be truly evaluated for effectiveness if the trainer or institution fails to provide the most essential aspects of the training—the knowledge required for the learner (Lawson, 2008).

Not having an evaluation methodology did not undermine the desires expressed by participants, such as, "I wish I could say we do something, but to be honest with you, we really don't" (P1, personal communication, March 1, 2016). If an educational program lacks evaluation, the program's effectiveness remains unknown, and any changes to behaviors or attitudes cannot be directly attributed to the training itself. P12 indicated that an evaluation method is the "next frontier for the compliance unit"; however, clarified by stating that the compliance unit is limited to "me, myself, and I" (personal communication, March 29, 2016). As resources are an essential component to developing an evaluation method, the lack of resources would in turn serve as the inhibiting factor.

In describing elements for a successful prevention and mitigation cyber-harassment policy and procedure, participant responses were themed to include specific components addressed within a written policy, identified resources, an organizational culture that is conducive to policy development and implementation, and communication and dissemination to the university community. A clearly written policy that describes an institution's program objectives addresses "knowledge (cognitive), skill (behavioral), and attitude (affective)" (Lawson, 2008, p. 234)—key foundational aspects of effective learning outcomes. P8 suggested that the verbiage include a statement regarding the institution's values, and P5 suggested that policies be written from a standardized template. Recommendations for policy elements mirrored those identified by Stuart-Cassel et al. (2011), where 11 key parts among cyberbullying state laws were identified. Based on their experience, participants were asked to provide recommendations as to how these elements could be measured and tracked by the institution.

Given that all participants reported the absence of a cyber-harassment policy at their respective institutions, all but one participant would not or could not provide a thorough response. One of the participants, while providing a thoughtful response, could only describe the future plans for an evaluation mechanism at the respective institution.

Recommendations for other policy administrators. The final interview questions explored recommendations that policy administrators would make for future implementation. As all participants indicated that their institution did not have a specific policy that addressed cyber-harassment, participant recommendations lacked substance. Many of the participants reiterated previous responses, and they themselves second guessed how applicable and relevant their experience in developing and implementing policies would be in implementing this type of policy at their institutions.

Institutions are limited in their ability to influence federal, state, and legislative mandates. As a result, changes in legislation solicit a reactionary response, and institutions must face the challenge of interpreting the legislation, with the responsibility for developing appropriate plans for effective and efficient implementation. After the entire discussion, P9 responded candidly with "wow, I would advise them against it. You don't want to walk this path" (P9, Personal Communication, March 17, 2016). Despite federal mandates, there is still much confusion in the interpretation and compliance with the provisions outlined in the legislation.

Implications of the Study

University policy administrators who participated in this study have the responsibility to develop, approve, or influence institutional policy. As such, this study examined the perspectives, insights, and understandings of those individuals responsible for developing and operationalizing policies in the areas of cyber-harassment. The intent of this study was to explore

those perspectives and contribute to a better understanding of the strategies and challenges associated with policy administration. The implications resulting from this study are as follows: (a) implications for current and future policy administrators, (b) implications for institutions of higher education, and (c) implications for students.

Implications for current and future policy administrators. This study on cyber-harassment in higher education is important for the following reasons. Although a plethora of research is available with regard to cyber-bullying victimization, and the prevalence and impact on pre-adolescent and adolescent groups, there appears to be a gap in the research available with regard to cyber-harassment in higher education, specifically in the areas of higher-education response and responsibility. This study provides the insights and perspectives of those who are responsible for the administration of such policies.

As this study sought to understand strategies and best practices pertaining to cyber-harassment policies, the findings of this study not only revealed the lack of existence of such policies, but also revealed the lack of definition and understanding of the behavior the policies would mitigate or prevent. Additionally, this study surfaced the challenges and frustrations that hinder policy administrators from developing and implementing such policies. Another aspect that this study revealed was in the complexities within institutions and the driving forces outside of institutions that motivate or discourage policy development. Hinduja and Patchin (2013) indicated that, in an effort to protect students and the organization, institutions must "have a clear and comprehensive policy regarding bullying, harassment, technology, and the intersection: cyberbullying" (as cited by Sabella, Patchin, & Hinduja, 2013, p. 2,707). This study revealed that institutions have a clear understanding of the individual components of bullying, harassment, and technology. However, they fail to address the impact when those components converge.

Implications for institutions of higher education. Legislators have clearly addressed campus safety and security risks by adopting a variety of regulatory measures. As a strategy to promote a culture of safety on college and university campuses, the U.S. Department of Education has prescribed prevention and mitigation efforts, mandated educational programs, and enforced sanctions on those that fail to meet regulatory standards (Krebs et al., 2007; National Victim Center, 1992). Given the quantity and the frequency of legislative changes, it is reasonable to believe that legislators will continue enhancing existing regulation or approve additional legislation. With that said, institutions must be cognizant of these changes and respond appropriately in an effort to stay in compliance with the legal environment. As college and university policy administrators coordinate efforts to develop and implement programs and policies in areas in which legislation provides little to no guidance, institutions are left to their own devices to employ policies and procedures that prohibit, discourage, and respond to cyber-harassment behaviors.

Implications for students in higher education. Although this particular study explored the risk and responsibilities of higher education institutions, it would be negligent to not include the implications that this may have on college and university students. Technology has increased the effectiveness and efficiency of communication. Despite the advantages technology provides, technology has fundamentally changed communication in schools (Rogers, 2000). Despite the benefits of such technologies, technology now serves as the conduit for malicious behaviors (Beran & Li, 2005). As students in higher education continue to embrace technological advances, it is important for students to identify such behaviors and more importantly, be aware of the resources and support that institutions can provide in the event of cyber-harassment.

Recommendations for Future Research

An abundance of research is available with regard to the prevalence and impact of bullying and cyber-bullying on pre-adolescent and adolescent groups, however there appears to be a gap in the research available with regard to cyber-harassment. The objective of this qualitative study was to determine the strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. Based on the findings of this study, there is an apparent need for future research. The following suggestions are based on those findings.

- A study of the intersection of federal law, as it applies to cyber-harassment. The intersection of existing laws including, but not limited to, the Violence Against Women Act (2014), Title IX of the Education Amendments (1972), Title VII of the Civil Rights Act (1964), and the Clery Act (1998).
- A study of cyber-harassment legislation and policy as defined by State Education Authorities. Of the 49 states that have bullying laws, 48 include provisions that address bullying through technological platforms, of which 20 specifically state *cyberbullying* within the legislation (Hauck, 2014).
- A study of the students' perceptions with regard to cyber-harassment behaviors. College students have expressed that cyberbullying is "childish and not something you communicate with others" (Crosslin & Golman, 2014, p. 16).
- A review of the coping mechanisms of students in response to cyber-harassing behaviors, a comparative study in traditional undergraduate student populations versus graduate students.

Broader Application and Final Thoughts

The effects of cyber-harassment are clear. They include anxiety and isolation (Crosslin & Golman, 2014), depression, paranoia, and even suicide (Schenk et al., 2013). The psychological and emotional impacts are not limited to victims, as studies have also shown impacts to bystanders and the bullies themselves (Schenk et al., 2013). With the expansion of information and communication technologies, cyberbullying behaviors are causing great concern (Kubiszewski et al., 2015; Willard, 2005). Extensive research has been conducted on school bullying and workplace harassment; however, little research has been conducted in the areas of cyber-harassment (Kiriakidis & Kavoura, 2010).

Bullying behaviors foster "a climate of fear and disrespect that can seriously impair the physical and psychological health of its victims and create conditions that negatively affect learning" (Ali, 2010, p. 1), undermining a student's ability to reach their full potential. What was once a behavior that only took place on a school playground, now occurs in the virtual environment, where behavioral oversight and control are nonexistent. With that said, one can easily conclude that cyber-harassment is simply harassing behaviors that occur through technological means. However, technology has opened Pandora's box, and has introduced a new breed of malevolent behaviors that can occur online, including stalking, impersonation, trickery, and exclusion to name a few (Francisco et al., 2015). This public display of anger, judgement, and sometimes hate, have implications on victims, students, bystanders, institutions, and the community at large (Kiriakidis & Kavoura, 2010).

The significance of this study has become progressively important due to recent changes in legislation, case law, and media attention with regard to cyber-harassment in higher education. Is an institution of higher education responsible for activity that occurs in the virtual

environment? And if so, to what degree? Institutions must promote a safe learning environment beyond the boundaries of the physical classroom and into the virtual classroom thus the findings of this study will help in furthering that dialogue so that more can be done to establish practices and strategies that will result in safer environments for students.

Policy development. A clearly written policy describes an institution's program objectives and addresses "knowledge (cognitive), skill (behavioral), and attitude (affective)" (Lawson, 2008, p. 234)—key foundational aspects of effective learning outcomes. In response to interview question 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing a policy related to the prevention and mitigation of cyber-harassment, participants expressed the challenge in writing a policy. Specific challenges included writing a thoroughly written policy (P1, personal communication, March 1, 2016) and one that was clearly articulated (P1, personal communication, March 8, 2016). Institutions should develop and implement a zero-tolerance policy that addresses students, faculty, and staff (Minor et al., 2013). In a study conducted by Kokkinos, Antoniadou, and Markos (2014), it is recommended that universities "aim at the prevention of the incidents through proper ICT [information communication technologies] use, by the inclusion of proper online social conduct . . . and the thorough expression of the institution's expectations" (p. 212).

Explored in more detail in interview question 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure, participants suggested that the policy statements include (a) the definition of cyber-harassment, (b) a clearly written policy statement emphasizing the institution's position regarding this behavior, (c) who this policy applies to, (d) what an individual should do if they witness the behavior, (e) who to report the behavior to, (f) what the institution must do in response to

receiving the report, (g) disciplinary measures or sanctions for non-compliance, and (h) any laws governing this behavior. Additionally, policies should include additional information such as (a) the effective date of the policy, (b) responsible officer or office, and (c) contact information for where to get assistance or support.

In developing a cyber-harassment policy, it is recommended that institutions adopt a structured cyber-harassment policy which contains (a) policy caption, (b) scope, (c) policy statement, (d) definitions, (e) standards, (f) procedures, (g) references, (h) history, and (i) responsibility. As an introductory section of the policy, all policies should contain caption information that includes a policy number, the name of the respective policy, the effective date of the policy, the issuing office and the issuing officer. Should the policy be included in a student handbook or a general catalog, the caption information is naturally contained in the form of a catalog version number with the issuing office being the respective university.

Within the scope section of the policy, the section should specify the intended audience and the constituencies to which the policy applies which may include students, faculty, staff, visitors, consultants, and any combination thereof. The policy section provides a clear and concise statement of the policy. This should consist of a short introductory statement summarizing the policy at a high-level and a general statement outlining the requirement or provisions that are placed o or extended to the university community. The policy statement should reflect the University's mission and values, objectives, and other considerations such as compliance with applicable laws and regulations.

Within the definition section of the policy, key terms used throughout the policy are clearly defined. Terms listed may have a unique or special meaning, may address a technical or legal term, acronyms, and similar terms that add to the users understanding of the policy. For a

cyber-harassment policy, it is recommended that the policy include definitions for bullying, harassment, verbal harassment, physical harassment, social harassment, sexual harassment, gender-based harassment, sexual violence, Title IX, and cyber-harassment. It is recommended that definitions are listed alphabetically, for user ease and organization of the overall policy section.

The standards section sets forth the required conduct to conform with the respective policy. This section of the policy addresses the authority issued to an individual or office responsible for addressing the reported concern, the rights of the parties including both the accuser and the accused. Additionally, this section describes the appropriate sanctions if any, such as disciplinary action and potential civil or criminal penalties. The procedure section specifies the steps or methods necessary for complying with the policy. This section elaborates upon and provides more depth and breadth, and provides a more detailed account with regard to the policy section. Additionally, the procedures provide for a course of action for implementation of the policy. The procedures may outline specific information necessary for the implementation, administration, and compliance of the policy. Note, the procedures are not guidelines, but instead are regulations to which amplify the policy.

The references section of the policy provides an outline of related policies, documents, or applicable laws that support the policy or procedure. This section may include internal policies or external sources that provide helpful and relevant information that may aid or supplement the users understanding of the policy at hand. For a cyber-harassment policy, it is recommended that the listing of supplemental or related policies, or applicable laws referenced include Title IX (1972), Clery Act (1998), and the Violence Against Women Reauthorization Act (2014). The history section provides the policy effective date, and the information for the policy superseded.

The responsibility section identifies the persons responsible for the implementation or administration of the respective policy. A summary of the framework, brief description of the contents found within the framework, and contents specific to a policy for cyber-harassment are outlined in table 5.

Table 5

Cyber-Harassment Policy Framework

Section	Description of Section	Information Specific to a Cyber-Harassment Policy
Caption	Includes the policy number scheme, to serve as a unique identifier in relation to other institutional policies, the name of the policy, the effective date of the policy, and responsible officer or office.	Not applicable as policy numbering schemes, policy naming conventions, effective dates, and responsible officers or offices will vary at each institution.
Scope	Identifies the constituents to whom the policy will apply to.	Specify if the policy will apply to students, faculty, staff, or any combination of constituencies.
Policy	Provides a clear and concise statement of the institution's position, that reflects the organizational culture and risk tolerance of the institution.	Include an introductory statement summarizing the institutions prohibition of class-based discrimination or harassment.
Definitions	Provides definitions of all key terms used within a specific policy,	Include definitions for Bullying, Harassment, Verbal Harassment, Physical Harassment, Social Harassment, Sexual Harassment, Gender-Based Harassment, Sexual Violence, Title IX, and Cyber-Harassment.
Standards	Sets forth the required conduct to conform to in accordance with a policy.	Address the authority issued to the individual responsible for addressing the reported concern, the rights of the parties including the accuser and the accused.
Procedures	Specifies the steps or methods for complying with the policy.	Address what an individual should do, should they witness the described behavior, who and how to report the behavior, and describe the institutional process when a report is received.
References	Provides related policies, documents, or links that provide helpful and relevant information supporting the policy, procedure, or guideline.	Include supplemental or related policies, which may include institutional policies related to Title IX (1972), Clery Act (1998), and the Violence Against Women Reauthorization Act (2014).

(continued)

Section	Description of Section	Information Specific to a Cyber-Harassment Policy
History	Provides the policy effective date and the policy number of the policy superseded.	Not applicable as the effective dates and prior policies will vary at each institution.
Responsibility	Identifies the individuals responsible for implementing a policy.	Not applicable as the individuals or offices responsible for the policy will vary at each institution.

To ensure consistency and quality when drafting policies, it is further recommended that institutions adopt a uniform policy framework to be utilized as a standard for development of all institutional policies. Willard (2005) proposes a clear and well communicated policy. Policies should promote governance, management practices and behaviors that are consistent with the mission and values, promote operational efficiencies, and reflect the culture of the institution.

Policy implementation strategy. As a strategy for implementing a cyber-harassment policy, participants in the study described leveraging a formalized policy development process as a key technique. In addition to describing the process, participants described a process that embraces a collaborative approach to socializing a policy into the university's culture. Encouraging collaboration among focus groups and through face to face discussions supports socialization of such policies. Participants in the study unanimously referenced the effect and impact the organizational culture had on developing and implementing policy. It is highly recommended that to successfully implement a policy, cross collaboration among constituents is a fundamental and a necessary component of the process.

Broader application for policy framework. Extensive research has been conducted on school bullying and workplace harassment, however little research has been conducted in the areas of cyber-harassment (Kiriakidis & Kavoura, 2010); therefore, it is logical to conclude that organizations and industries beyond institutions of higher education that are faced with minimizing cyber-harassment behaviors may benefit from this policy framework. Laws that

address cyberbullying-type behaviors are often times applied in the context of harassment, stalking, libel, workplace sexual harassment. It is reasonable to believe that since harassing behaviors can occur in almost every type of environment including educational settings, workplace settings, and social settings, that cyber-harassment behaviors will appear in schools, colleges, industry, and virtually.

The proposed framework and implementation strategies have applicability in a variety of settings and industries that are faced with minimizing and negating the impacts of such behaviors. Although the varying federal, state, or agency laws that govern a specific employee or consumer groups, regional locations, industry types, or types of organizations including for-profits, not-for-profits, or governmental agencies, all organizations are charged with the legal, ethical, and moral considerations with regard to harassing and cyber-harassing behaviors.

Cyber-harassment defined. Although definitions of cyberbullying have been fundamentally derived from definitions of bullying, where conduct is defined as bullying behaviors that are facilitated by information and communication technologies (Kubiszewski et al., 2015), it is important to highlight the variences and clearly distinguish the two. In traditional bullying, bullying behaviors "generally occur during school hours and cease once a victim returns home" (Tokunaga, 2010, p. 279), whereas cyberbullying transcends geographical restrictions and boundaries. Additionally, cyberbullying can continue online without the presence or participation of the victim (Crosslin & Golman, 2014).

Advances in technology communication systems have provided users with mechanisms in which the perpetrator has the option to remain completely anonymous (Kokkinos, Antoniadou, & Markos, 2014). Ultimately, this provides for a situation in which a victim cannot identify their perpetrator. Additionally, bullying through technologies is easier and provides a greater return on

investment for bullying efforts (Antoniadou & Kokkinos, 2015). Others highlight that cyberbullying provides a forum in which individuals can play the role of victim and bully (Antoniadou & Kokkinos, 2015). Although there are notable similarities between harassment and cyber-harassment, it is recommended that institutional policy specifically differentiate and define cyber-harassment as a unique phenomenon.

In an effort toward identifying a more comprehensive definition of cyberbullying, research conducted by Tokunaga (2010) expressed the need for consistent and operational definitions. In an analysis of cyberbullying and cyber-harassment definitions proposed by Crosslin and Golman (2014), Besley (as cited by Tokunaga, 2010), Patchin and Hinduja (2006), Olweus (2013), Stuart-Cassel et al. (2011), and Tokunaga (2010), all researchers propose a policy that contain varying degrees of the following attributes (a) description of the behavior, (b) the frequency of the behavior, (c) intent of the behavior, (d) inequity of power between two parties, and (e) the utilization of technology. However, none of the proposed policies address all of the listed attributes. Table 6 outlines the definitions as proposed by the researchers with regards to the aformentioned attributes.

Table 6

Analysis of Cyberbullying and Cyber-Harassment Definitions

Study	Behavior	Frequency	Intent	Power Distribution	Technology
Crosslin and Golman (2014)	X	X			X
Besley (2009)	X	X	X		X
Patchin and Hinduja (2006)	X	X			X
Olweus (2013)	X				X
Stuart-Cassel et al. (2011)	X	X	X	X	
Tokunaga (2010)	X	X	X		X

As such, the researcher proposes the following definition of cyber-harassment, which addresses all of the common attributes necessary for a comprehensive and consistent definition. Cyber-harassment is defined as a repeated pattern of overt or covert bullying or harassing behaviors involving an inbalance of power, by an individual or a group facilitated through the use technological means with the intent of causing harm upon others. As defined, the proposed definition addresses the behavior, frequency, intent, distribution of power, and the use of technological means.As institutions become increasingly liable for the prevention and mitigation of, and appropriate response efforts to, cyber-harassment, it is vital that institutions acknowledge potential implications and associated risks. When legislation is vague and inconsistent, institutions are faced with the challenge of interpreting and operationalizing compliance measures. It is the researcher's hope that despite the lag in legislation, policy administrators remain encouraged and vigilant regarding the multi-faceted and ambiguous safety culture within academic establishments.

REFERENCES

Adult Bullying. (n.d.). *Retrieved from bullying statistics; Anti-bullying help, facts and more*: Retrieved from http://www.bullyingstatistics.org/content/adult-bullying.html

Ali, R. (2010). *Dear colleague letter: Harassment and bullying.* Washington, DC: U.S. Department of Education.

Ali, R. (2011). *Dear colleague letter: Sexual violence.* Washington, DC: Department of Education Office of Civil Rights.

Allen, E. I., & Seaman, J. (2011). *Going the distance: Online education in the United States*. Retrieved from http://www.onlinelearningsurvey.com/reports/changingcourse.pdf

Allen, E. I., & Seaman, J. (2013). *Changing course: Ten years of tracking online education in the United States*. Retrieved from http://www.onlinelearningsurvey.com/reports/changingcourse.pdf

American Council on Education. (2012). *A president's guide to the clery act.* Retrieved from http://www.acenet.edu/news-room/pages/president's-Guide-to-the-Clery-Act.aspx

American Council on Education. (2013). *New requirements imposed by the violence against women reauthorization act.* Retrieved from http://www.acenet.edu/news-room/Documents/VAWA-Summary.pdf

Antoniadou, N., & Kokkinos, C. M. (2015). Cyber and school bullying: same or different phenomena? *Aggression and violent behavior, 25*, 363-372. doi:10.1016/j.avb.2015.09.013

Armstrong, D., Gosling, A., Weinman, J., & Marteau, T. (1997). The place of inter-rater reliability in qualitative research: An empirical study. *Sociology, 31*(3), 597-606. doi:10.1177/0038038597031003015

Association of College and University Administrators. (2015a). *About ACUPA*. Retrieved from ACUPA: https://acupa.site-ym.com/

Association of College and University Policy Administrators. (2015b). *ACUPA E-List: Acceptable Use*. Retrieved from ACUPA: http://c.ymcdn.com/sites/acupa.site-ym.com/resource/resmgr/Docs/ACUPA_E-list_Acceptable_Use.pdf

Baum, K., & Klaus, P. (2005). *National Crime Victimization Survey: Violent Victimization of College Students, 1995-2002.* Office of Justice Programs. U.S. Department of Justice.

Beran, R., & Li, Q. (2005). A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277. doi:10.2190/8YQM-B04H-PG4D-BLLH

Black, M. C., Basile, K. C., Breiding, M. J., Smith, S. G., Walters, M. L., Merrick, M. T., . . . Stevents, M. R. (2011). *National Intimate Partner and Sexual Violence Survey.* Atlanta, GA: Centers for Disease Control and Prevention.

Bolman, L. G., & Deal, T. E. (2013). *Reframing organizations* (5th ed.). San Francisco, CA: John Wiley & Sons.

Burczak, A. (2007). *Change happens: A Guide to Reforming Your Campus Sexual Assault Policy.* Retrieved from http://www.ncdsv.org/images/SAFER_ChangeHappens_2007.pdf

Burke, W. W. (2011). *Organizational change theory and practice* (3rd ed.). New Delhi, India: Sage Publications.

Burke, W. W., & Litwin, G. H. (1992). A causal model of organizational performance and change. *Journal of Management, 18*(3), 523-545.

Campus Sex Crimes Prevention Act of 2000, Pub. L. 106-386, 114 Stat. 1465, *codified as amended* at title 20 U.S.C. § 1601 (2000).

Campus Sexual Assault Victims' Bill of Rights of 1998, Pub. L. 102-325, 106 Stat. 448, *codified as amended* at title 20 U.S.C. § 1092 (1998).

Campus Sexual Violence Elimination Act of 2011, S. 128, 112th Cong. (2011).

CampusClarity. (2013). Offer students federal aid? A new law requires sexual violence training. Walnut Creek, CA.

Carter, S. D. (2014). *Jeanne clery act information*. Retrieved from: http://www.cleryact.info

Clery Center for Security On Campus. (2012). *The Campus Sexual Violence Elimination (SaVE) Act*. Retrieved October 31, 2015, from Clery Center for Security on Campus Website: http://clerycenter.org

Cohen, D. S. (2005). *The Heart of Change Field Guide: Tools and Tactics for Leading Change in Your Organization.* Boston, MA: Deloitte Development.

College and University Security Information Act. PA Act 73: 24 P.S. § 2502-1 *(1988)*.

Cornell University Law School. (n.d.-a). *Preponderance*. Retrieved from Legal Information Institute: https://www.law.cornell.edu/wex/preponderance

Cornell University Law School. (n.d.-b). *Prima facie*. Retrieved from Legal Information Institute: https://www.law.cornell.edu/wex/prima_facie

Cortina, L. M., Swan, S., Fitzgerald, L. F., & Waldo, C. (1998). Sexual Harassment and assault. *Psychology of Women Quarterly, 22*(3), 419-441. doi:10.111/j.1471-6402.1998.tb00166.x

Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.

Crosslin, K., & Golman, M. (2014). "Maybe you don't want to face it" - College students' perspectives on cyberbullying. *Computers in Human Behavior, 41*, 14-20. doi:10.1016/j.chb.2014.09.007

DeMarrais, K. (2004). *Qualitative interview studies: Learning through experience.* New York, NY: Routledge.

DeSantis, N. (2015, February 23). *U. of Colorado to pay suspended male student $15,000 to settle Title IX suit* [Web log post]. Retrieved from The Chronicle of Higher Education: http://chronicle.com/blogs/ticker/jp/u-of-colorado-to-pay-suspended-mail-student-15000-to-settle-title-ix-suit?cid=at&utm_source=at&utm_medium=en

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). *Frequency of social media use.* Retrieved from http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf

Duggen, M. (2014). *Online Harassment.* Washington, DC: Pew Research Center.

Fisher, B. S. (1995). Crime and fear on campus. *The Annals of the American Academy of Political and Social Science, 539*(1), 85-101. doi:10.1177/0002716295539001007

Foderaro, L. W. (2010, September 29). Private moment made public, then a fatal jump. *The New York Times*. Retrieved from http://www.nytimes.com/2010/09/30/nyregion/30suicide.html?pagewanted=all%2526_r=1

Francisco, S. M., Veiga Simão, A. M., Ferreira, P. C., & Martins, M. J. (2015). Cyberbullying: The hidden side of college students. *Computers in Human Behavior, 43*, 167-182. doi:10.1016/j.chb.2014.10.045

Gahagan, K., Vaterlaus, J. M., & Frost, L. R. (2015). College student cyberbullying on social network sites: Conceptualization, prevalance, and perceived bystander responsibility. *Computers on Human Behavior, 55*, 1097-1105. doi:10.1016/j.chb.2015.11.019

Grasgreen, A. (2012). *Deadlines for Campus Justice*. Retrieved from Foundation for Individual Rights in Education: https://www.thefire.org/deadlines-for-campus-justice/

Gupta, U. G. (2008). *Cyber-harassment in academia.* Retrieved from University Business: http://www.universitybusiness.com/article/cyber-harassment-academia

Hall of Justice. (n.d.). *Criminal justice system*. Retrieved from http://www.sdcda.org/office/criminal-justice-system.html

Hauck, A. (2014, July 1). *Cyberbullying laws by state* [Web log post]. Retrieved from Crime Wire: http://www.instantcheckmate.com

Higher Education Compliance Alliance. (n.d.). *Compliance Matrix*. Retrieved from http://www.higheredcompliance.org/matrix/

Hill, E. G. (2007). *California Criminal Justice System: A Primer* [Report]. Sacramento, CA: Legislative Analyst's Office. Retrieved from Legislative Analyst's Office: http://www.lao.ca.gov/publications/detail/2682.

Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998. Pub. L. 101-542, 104 Stat. 2381, *codified as amended* at title 34 C.F.R. § 668.46 (1998).

Hinduja, S., & Patchin, J. W. (2013). Social Influences on Cyberbullying Behaviors among Middle and High School Students. Journal of Youth and Adolescence, 42(5), 711-722. doi:10.1007/d10964-012-9902-4

Jozkowski, K. N., Henry, D. S., & Sturm, A. A. (2014). College students' perceptions of the importance of sexual assault prevention education:Suggestions for targeting recruitment for peer based education. *Health Education Journal, 74*(1), 46-59. doi:10.1177/0017896913516298

Karjane, H. M., Fisher, B., & Cullen, F. T. (2005). *Sexual assault on campus: What colleges and universities are doing about it.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Kingkade, T. (2013). *UConn faces lawsuit for handling of sexual assault and harassment on campus*. Retrieved from Huffington Post: http://www.huffingtonpost.com/2013/11/01/uconn-lawsuit-sexual-assault-harassment_n_4191839.html

Kiriakidis, S. P., & Kavoura, A. (2010). Cyberbullying: a review of the literature on harassment through the internet and other electronic means. *Family and Community Health, 33*(2), 82-93.

Kirkpatrick, D. L. (2008). Evaluating training programs. In A. S. Development, *ASTD Handbook for Workplace Professionals* (pp. 485-491). Danvers, MA: ASTD Press.

Kokkinos, C. M., Antoniadou, N., & Markos, A. (2014). Cyberbullying: an investigation of the psychological profile of university student participants. *Journal of Applied Developmental Psychology, 35*(3), 204-214. doi:10.1016/j.appdev.2014.04.001

Kowalski, R. M., Giumetti, G. W., Schroader, A. N., & Lattner, M. R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-1137. doi:10.1037/a0035618

Kowalski, R. M., Limber, S., & Agatston, P. W. (2012). *Cyberbullying: bullying in the digital age.* Malden, MA: Wiley-Blackwell.

Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*(6), S22-S30. doi:10.1016/j.jadohealth.2007.08.017

Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical and Academic correlates of cyberbullying and tradtional bullying. *Journal of Adolescent Health, 53*(1), S13-S20. doi:10.1016/j.jadohealth.2012.09.018

Krebs, C. P., Lindquist, C. H., Warner, T. D., Fisher, B. S., & Martin, S. L. (2007). *The campus sexual assault (CSA) study.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Kubiszewski, V., Fontaine, R., Potard, C., & Auzoult, L. (2015). Does cyberbullying overlap with school bullying when taking modality of involvement into account? *Computers in Human Behavior, 43*, 49-57.

Lacher, R., & Ramos, P. A. (2014). *United States: US Department of Education levies more fines for Clery Act violations*. Retrieved from http://www.mondaq.com/unitedstates/x/289764/Education/US+Department+Of+Education+Levies+More+Fines+For+Clery+Act+Violations

Langbein, L. I., & Kerwin, C. M. (2000). Regulatory negotiation versus conventional rule making: Claims, counterclaims, and empirical evidence. *Journal of Public Administration Research and Theory, 10*(3), pp. 599-632. doi:10.1093/oxfordjournals.jpart.a024283

Lawson, K. (2008). Instuctional design and development. In E. Beich, *ASTD handbook for workplace professions* (pp. 223-250). Alexandria, VA: ASTD Press.

Lhamon, C. E. (2015a). *Dear colleague letter: Title IX coordinators.* Washington, DC: U.S. Department of Education.

Lhamon, C. E. (2015b). *Dear Title IX coordinator.* U.S. Department of Education.

Li, Q. (2006). Cyberbullying in schools: a research of gender differences. *School Psychology International, 27*(2), 157-170. doi:10.1177/0143034306064547

Li, Q. (2007). New bottle but old wine: a research of cyberbullying in schools. *Computers in Human Behavior, 23*(4), 1777-1791. doi:10.1016/j.chb.2005.10.005

Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research, 50*(3), 223-234. doi:10.1080/00131880802309333

Lipka, S. (2013, November 11). *Lincoln U. of Missouri faces $275,000 fine for Clery Act violations*. Retrieved from Chronicle of Higher Education: http://chronicle.com/article/Lincoln-U-of-Missouri-Faces/142929/.jobs_topjobs-slider

Luby, C., Angell, K., Daniels, E., Richi, R., v. University of Connecticut No. 3:13-cv-1605 (D. Conn, filed Nov. 1, 2013).

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation.* Hoboken, NY: Wiley.

Minor, M. A., Smith, G. S., & Brashen, H. (2013). Cyberbullying in higher education. *Journal of Educational Research and Practice, 3*(1), 15-29. Retrieved from http://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=1043&context=jerap

Musgrove, M., & Yudin, M. K. (2013). *Dear colleague: Bullying of students with disabilities.* Washington, DC: U.S. Department of Education.

National Center for Victims of Crime. (2012). *The criminal justic system*. Retrieved from National Center for Victims of Crime: http://www.victimsofcrime.org/help-for-crime-victims/get-help-bulletins-for-crime-victims/the-criminal-justice-system

National Centre Against Bullying. (n.d.). *Four kinds of bullying*. Retrieved from http:///www.ncab.org.au/Page.aspx?ID=88

National Conference of State Legislatures. (2015, January 12). *State cyberstalking and cyberharassment laws*. Retrieved from National Conferene of State Legislatures: http://www.ncsl.org

National Crime Prevention Council. (n.d.). *Cyberbullying*. Retrieved from http://www.ncpc.org/cyberbullying

National Institute of Justice. (2010, October 26). *Reporting of sexual violence incidents*. Retrieved from http://www.nij.gov/topics/crime/rape-sexual-violence/pages/rape-notification.aspx

National Victim Center. (1992). *Rape in America: A report to the nation.* Arlington, VA.

Negotiated Rulemaking Act of 1990, Pub. L. 101-648, 104 Stat. 4969, *codified as amended* at title 5 U.S.C. 561 et seq. *(1990)*

Obama, B. (2014). *Memorandum: establishing a white house task force to protect students from sexual assault*. [Press release]. Retrieved from https://www.whitehouse.gov/the-press-office/2014/01/22/memorandum-establishing-white-house-task-force-protect-students-sexual-a

Olweus, D. (1993). *Bullying in school: What we know and what we can do.* Oxford, UK: Blackwell Publishers.

Olweus, D. (2013). School bullying: development and some important challenges. *Annual Review of Clinical Psychology, 9*(1), 751-780. doi:10.1146/annurev-clinpsy-050212-185516

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: a preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 148-169. doi:10.1177/1541204006286288

Patchin, J. W., & Hinduja, S. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence, 42*(5), 711-722. doi:10.1007/d10964-012-9902-4

Patterson, M. (2011, April 5). *Murder at Lehigh University shocked the nation 25 years ago*. Retrieved from Emmaus Patch: http://patch.com/pennsylvania/emmaus/murder-at-lehigh-university-shocked-the-nation-25-years-ago

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology, 52*(2), 137-145.

Protection of Human Subjects, *45 C.F.R.* § 46.101 (2009).

Reynolds, G. A. (2003). *Dear colleague letter: First amendment.* Washington, DC: Department of Education, Office of Civil Rights.

Richards, L., & Morse, J. M. (2013). *Qualitative methods* (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.

Rogers, D. L. (2000). A paradigm shift: Technology integration for higher education in the new millennium. *AACE Journal*, 19-33. Retrieved from http://www/editlib/org/p/8058/

Rothman, E., & Silverman, J. (2007). The effect of college sexual assault prevention program on first year students' victimization rates. *Journal of American College Health, 55*(5), 283-290. doi:10.3200/JACH.55.5.283-290

Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior, 29*(6), 2703-2711. doi:10.1016/j.chb.2013.06.040

Sacco, D., Silbaugh, K. B., Corredor, F., Casey, J., & Doherty, D. (2012). *An overview of state anti-bullying legislation and other related laws.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2197961

Sander, L. (2012, May 16). *Yale u. is fined $165,000 under crime-reporting law*. Retrieved from http://www.chronicle.com/article/Yale-U-Is-Fined-165000/139343

Schenk, A. M., Fremouw, W. J., & Keelan, C. M. (2013). Characteristics of college cyberbullies. *Computers in Human Behavior, 26*(6), 2320-2327. doi:10.1016/j.chb.2013.05.013

Schmieder-Ramirez, J., & Mallette, L. (2007). *The SPELIT Power Matrix.* Lexington, KY: Booksurge Publishing.

Shouse Law Group. (n.d.). *Legal definition of a felony in California Law*. Retrieved from http://www.shouselaw.com/felony/html

Sicking, J. (2011, October 20). *Bullying still occurs in college, professors find*. Retrieved from Indiana State University Newsroom: http://www.indstate.edu/news/news.php?newsid=2904

Siegle, D. (2010). Cyberbullying and sexting: technology abuses of the 21st century. *Gifted Child Today, 32*(2), 14-17.

Simmons, K. D., & Bynum, Y. P. (2014). Cyberbullying: six things administrators can do. *Education, 134*(4), 452-456.

Stuart-Cassel, V., Bell, A., & Springer, J. F. (2011). *Analysis of state bullying laws and policies.* U.S. Department of Education. Retrieved from https://www2.ed.gov/rschstat/eval/bullying/state-bullying-laws/state-bullying-laws.pdf

Student Right-To-Know and Campus Security Act of 1990. 20 U.S.C. § 1601 (1990).

Students Active for Ending Rape & V-Day. (2013). *Making the grade: Findings from the campus accountability project on sexual assault policies.* Retrieved from http://www.vday.org/~assets/downloads/2013-Campus-Accountability-Project-Full-Report.pdf

The Tyler Clementi Foundation. (n.d.). *Tyler's story*. Retrieved from http://www.tylerclementi.org/tylers-story

Title IV of the Higher Education Act of 1965. Pub. L. 89-329, 79 Stat. 1219, *codified as amended* at title 20 U.S.C. ch.28 § 1001 et seq. (1965).

Title IX of the Education Amendments of 1972. Pub. L. 92-318, 86 Stat. 235, *codified as amended* at title 20 U.S.C. ch.38 § 1681 et seq. (1972).

Title VII of the Civil Rights Act of 1964. Pub. L. 88-352, 78 Stat. 241, *codified as amended* at title 42 U.S.C ch.21 § 2000e-2 (1964).

Tokunaga, R. S. (2010). Following you home from school: a critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277-287. doi:10.1016/j.chb.2009.11.014

Townley, A. J., & Schmieder-Ramirez, J. H. (2010). *School law: A California perspective* (4th ed.). Dubuque, IA: Kendall Hunt Publishing Company.

U.S. Census Bureau. (2011). *Statistical abstract of the United States: 2012*. Retrieved from https://www.census.gov/library/publications/2011/compendia/statab/131ed.html

U.S. Department of Education. (2010). *Action guide for emergency management.* Office of Safe and Drug Free Schools. Washington: U.S. Department of Education, Office of Safe and Drug Free Schools.

U.S. Department of Education. (2014a). *U.S. Department of Education releases list of higher education institutions with open Title IX sexual violence investigations*. [Press release]. Retrieved from http://www.ed.gov/news/press-releases

U.S. Department of Education. (2014b). *Princeton University found in violation of Title IX, reaches agreement with U.S. Education Department to address, prevent seuxual assault and harassment of students*. [Press release]. Retrieved from http://www.ed.gov/news/press-releases

U.S. Department of Education. (2014c). *Campus security*. Retrieved from http://www2.ed.gov/admins/lead/safety/campus.html

U.S. Department of Education. (2014d). *Questions and answers on Title IX and sexual violence.* U.S. Department of Education Office for Civil Rights.

U.S. Department of Education. (2015). *Title IX resource guide.* Washington, DC: U.S. Department of Education, Office for Civil Rights.

U.S. Department of Education. (2016). *National center for education statistics*. Retrieved from College Navigator: http://nces.ed.gov/collegenavigator/

U.S. Department of Education. (n.d.). *About Ed: Overview and mission statement*. Retrieved from http://www2.ed.gov/about/landing.jhtml

U.S. Department of Health and Human Services. (2013). *What is cyberbullying?* Retrieved from http://www.stopbullying.gov/cyberbullying/what-is-it

U.S. Department of Health and Human Services. (n.d.). *What is bullying?* Retrieved from http://stopbullying.gov/what-is-bullying/definition/index.html

U.S. Department of Justice. (2000). *Prevalence, incidence, and consequences of violence against women.* Rockville, MD: National Institute of Justice.

U.S. Department of Justice. (2001). *Title IX legal manual.* Washington, DC: U.S. Department of Justice, Civil Rights Division.

U.S. Department of Justice. (2015a). *Overview of Title IX of the Education Amendments of 1972, 20 U.S.C A§ 1681Et. Seq*. Retrieved from http://www.justice.gov/crt/overview-title-ix-education-amendments-1972-20-usc-1681-et-seq

U.S. Department of Justice. (2015b). *Questions and answers regarding Title IX procedural requirements.* Retrieved from http://www.justice.gov/crt/federal-coordination-and-compliance-section-152

U.S. Equal Employment Opportunity Commission. (2015). *Harassment*. Retrieved from http://www.eeoc.gov/laws/types/harassment.cfm

U.S. Equal Employment Opportunity Commission. (2016a). *Overview*. Retrieved from https://www.eeoc.gov/eeoc/index.cfm

U.S. Equal Employment Opportunity Commission. (2016b). *Sexual harassment*. Retrieved from https://www.eeoc.gov/laws/types/sexual_harassment.cfm

United Educators. (2014). *The Campus SaVE Act: A compliance guide.* Retrieved from http://www.uthscsa.edu/sites/default/files/police/CampusSaVEAct.pdf

Vance, J. W. (2010). *Cyber-harassment in higher education: online learning environments.* (Doctoral dissertation, University of Southern California). Retrieved from http://digitallibrary.usc.edu/cdm/ref/collection/p15799coll127/id/309077

Victims of Trafficking and Violence Protection Act of 2000, Pub. L. 106-386 22 U.S.C. § 7101 et seq. (2000).

Violence Against Women Act; Final Rule, Pub. L. 113-14, 127 Stat. 54, 42, *codified as amended* at 34 C.F.R. 668.46 (2014).

Violence Against Women Reauthorization Act of 2013, Pub. L. 113-14, 127 Stat. 54, 42, *codified as amended* at Title 42 U.S.C. § 13701-14040 (2013).

Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, 108 Stat. 1796, *codified as amended* at Title 42 U.S.C. § 14141 (1994).

Westat, Ward, D., & Mann, J. L. (2011). *The handbook for campus safety and security reporting.* Retrieved from https://www2.ed.gov/admins/lead/safety/handbook.pdf

What is adult bullying? (2014). Retrieved from http://nobullying.com/adult-bullying/

Willard, N. (2005). *Educators guide to cyberbullying and cyberthreats.* Retrieved from http://bcloud.marinschools.org/SafeSchools/Documents/BP-CyberBandT.pdf

Zalaquett, C. P., & Chatters, S. J. (2014). Cyberbullying in college: Frequency, characteristics, and practical implications. *SAGE Open, 4*(1), 1-8. doi:10.1177/2158244014526721

APPENDIX A

Protecting Human Research Certificate of Completion

COLLABORATIVE INSTITUTIONAL TRAINING INITIATIVE (CITI PROGRAM)
COURSEWORK REQUIREMENTS REPORT*

* NOTE: Scores on this Requirements Report reflect quiz completions at the time all requirements for the course were met. See list below for details. See separate Transcript Report for more recent quiz scores, including those on optional (supplemental) course elements.

- Name: Victoria Schaefer-Ramirez (ID: 4075360)
- Email: uaschaef@pepperdine.edu
- Institution Affiliation: Pepperdine University (ID: 1729)
- Institution Unit: School of Education and Psychology

- Curriculum Group: GSEP Education Division
- Course Learner Group: GSEP Education Division - Social-Behavioral-Educational (SBE)
- Stage: Stage 1 - Basic Course

- Report ID: 18653857
- Completion Date: 02/08/2016
- Expiration Date: 02/06/2021
- Minimum Passing: 80
- Reported Score*: 85

REQUIRED AND ELECTIVE MODULES ONLY	DATE COMPLETED	SCORE
Belmont Report and CITI Course Introduction (ID: 1127)	03/16/14	3/3 (100%)
History and Ethical Principles - SBE (ID: 490)	02/08/16	5/5 (100%)
Defining Research with Human Subjects - SBE (ID: 491)	02/08/16	4/5 (80%)
The Federal Regulations - SBE (ID: 502)	02/08/16	4/5 (80%)
Assessing Risk - SBE (ID: 503)	02/08/16	4/5 (80%)
Informed Consent - SBE (ID: 504)	02/08/16	5/5 (100%)
Privacy and Confidentiality - SBE (ID: 505)	02/08/16	3/5 (60%)

For this Report to be valid, the learner identified above must have had a valid affiliation with the CITI Program subscribing institution identified above or has been a paid Independent Learner.

CITI Program
Email: citisupport@miami.edu
Phone: 305-243-7970
Web: https://www.citiprogram.org

COLLABORATIVE INSTITUTIONAL TRAINING INITIATIVE (CITI PROGRAM)

COURSEWORK TRANSCRIPT REPORT**

** NOTE: Scores on this Transcript Report reflect the most current quiz completions, including quizzes on optional (supplemental) elements of the course. See list below for details. See separate Requirements Report for the required scores at the time all requirements for the course were met.

- Name: Victoria Schaefer-Ramirez (ID: 4075360)
- Email: vaschaefer@pepperdine.edu
- Institution Affiliation: Pepperdine University (ID: 1729)
- Institution Unit: School of Education and Psychology

- Curriculum Group: GSEP Education Division
- Course Learner Group: GSEP Education Division - Social-Behavioral-Educational (SBE)
- Stage: Stage 1 - Basic Course

- Report ID: 18653857
- Report Date: 02/08/2016
- Current Score**: 85

REQUIRED, ELECTIVE, AND SUPPLEMENTAL MODULES	MOST RECENT	SCORE
History and Ethical Principles - SBE (ID: 490)	02/08/16	5/5 (100%)
Defining Research with Human Subjects - SBE (ID: 491)	02/08/16	4/5 (80%)
Belmont Report and CITI Course Introduction (ID: 1127)	03/16/14	3/3 (100%)
The Federal Regulations - SBE (ID: 502)	02/08/16	4/5 (80%)
Assessing Risk - SBE (ID: 503)	02/08/16	4/5 (80%)
Informed Consent - SBE (ID: 504)	02/08/16	5/5 (100%)
Privacy and Confidentiality - SBE (ID: 505)	02/08/16	3/5 (60%)

For this Report to be valid, the learner identified above must have had a valid affiliation with the CITI Program subscribing institution identified above or have been a paid Independent Learner.

CITI Program
Email: citisupport@miami.edu
Phone: 305-243-7970
Web: https://www.citiprogram.org

APPENDIX B

ACUPA Site Approval

Victoria Schaefer-Ramirez

From: noreply@ymem.net
Sent: Thursday, February 04, 2016 1:22 PM
To: Victoria Schaefer-Ramirez
Subject: Re: Contact Us

Association of College and University Policy Administrators

In response to your "Contact Us" submission:

Hi Victoria,

I shared your request with the ACUPA Board members and we approve your request. You also have the capbility of using the Forums feature of our website to contact our members, but either way is fine. We do request, however, that you ask our members to contact you directly at a personal email address rather than having them respond to the entire e-list.

Thanks,

Donna Meeks

APPENDIX C

Recruitment Letter

Dear Potential Research Participant,

I am a member of the Association of College and University Policy administrators (ACUPA), and am entering into the research phase of my doctoral program in Organizational Leadership at Pepperdine University. My research is in partial fulfillment of the requirements for the dissertation, titled *Cyber-Harassment in Higher Education: A Study of Institutional Policies and Procedures*.

The purpose of my research is to examine strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. This study is fulfilling an academic requirement, and is not commissioned by ACUPA.

Your participation in this research study will take the form of a one-hour interview. The interview may take place in person or facilitated through technological means. During the interview, you will be asked a series of questions pertaining to your experience in higher education policy development and implementation.

Please contact me directly, within the next week expressing your willingness to participate in this research study. Thank you, in advance, for the consideration.

Respectfully,
Victoria Schaefer-Ramirez

APPENDIX D

IRB Exemption Notice

PEPPERDINE

Pepperdine University
24255 Pacific Coast Highway
Malibu, CA 90263
TEL: 310-506-4000

NOTICE OF APPROVAL FOR HUMAN RESEARCH

Date: February 25, 2016

Protocol Investigator Name: Victoria Schaefer-Ramirez

Protocol #: 16-02-203

Project Title: Cyber-harassment in higher education: A study of institutional policies and procedures

School: Graduate School of Education and Psychology

Dear Victoria Schaefer-Ramirez:

Thank you for submitting your application for exempt review to Pepperdine University's Institutional Review Board (IRB). We appreciate the work you have done on your proposal. The IRB has reviewed your submitted IRB application and all ancillary materials. Upon review, the IRB has determined that the above entitled project meets the requirements for exemption under the federal regulations 45 CFR 46.101 that govern the protections of human subjects.

Your research must be conducted according to the proposal that was submitted to the IRB. If changes to the approved protocol occur, a revised protocol must be reviewed and approved by the IRB before implementation. For any proposed changes in your research protocol, please submit an amendment to the IRB. Since your study falls under exemption, there is no requirement for continuing IRB review of your project. Please be aware that changes to your protocol may prevent the research from qualifying for exemption from 45 CFR 46.101 and require submission of a new IRB application or other materials to the IRB.

A goal of the IRB is to prevent negative occurrences during any research study. However, despite the best intent, unforeseen circumstances or events may arise during the research. If an unexpected situation or adverse event happens during your investigation, please notify the IRB as soon as possible. We will ask for a complete written explanation of the event and your written response. Other actions also may be required depending on the nature of the event. Details regarding the timeframe in which adverse events must be reported to the IRB and documenting the adverse event can be found in the *Pepperdine University Protection of Human Participants in Research: Policies and Procedures Manual* at community.pepperdine.edu/irb.

Please refer to the protocol number denoted above in all communication or correspondence related to your application and this approval. Should you have additional questions or require clarification of the contents of this letter, please contact the IRB Office. On behalf of the IRB, I wish you success in this scholarly pursuit.

Sincerely,

Judy Ho, Ph.D., IRB Chairperson

cc: Dr. Lee Kats, Vice Provost for Research and Strategic Initiatives

PEPPERDINE

Pepperdine University
24255 Pacific Coast Highway
Malibu, CA 90263
TEL: 310-506-4000

Mr. Brett Leach, Regulatory Affairs Specialist

APPENDIX E

Informed Consent

PEPPERDINE UNIVERSITY

INFORMED CONSENT FOR PARTICIPATION IN RESEARCH ACTIVITIES

CYBER-HARASSMENT IN HIGHER EDUCATION:
A STUDY OF INSTITUTIONAL POLICIES AND PROCEDURES

You are invited to participate in a research study conducted by Victoria Schaefer-Ramirez, under the direction of Dr. Farzin Madjidi, at Pepperdine University, because you are over the age of 18, a member of the Association of College and University Policy Administrators (ACUPA), and have responsibility at your respective institution, to significantly influence policy change.

Your participation is voluntary. You should read the information below, and ask questions about anything that you do not understand, before deciding whether to participate. Please take as much time as you need to read the consent form. You may also decide to discuss participation with your family or friends. If you decide to participate, you will be asked to sign this form. You will also be given a copy of this form for you records.

PURPOSE OF THE STUDY

It is vital for institutions to prevent and mitigate unwelcome conduct and to respond appropriately and effectively should misconduct occur. Accordingly, the purpose of this qualitative study is to determine the strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. Additionally, this study seeks to determine success measures and recommendations for future implementation for higher education institutions when preventing and mitigating cyber-harassment.

STUDY PROCEDURES

If you volunteer to participate in this study, you will be asked to participate in a one-hour interview that will be audio recorded. Interviews will be conducted in person, face-to-face, in an office or conference room at the participant's respective higher education institution. The interview may also be conducted virtually through a recordable format such as Adobe Connect.

In the event the participant refrains from providing consent to be audio-recorded during the interview, the participant may still elect to participate. As an alternative, the researcher will take notes during the interview.

POTENTIAL RISKS AND DISCOMFORTS

The potential and foreseeable risks associated with participation in this study do not exceed risks associated with day-to-day activities. Potential risks subjects may be exposed to include fatigue, boredom, or feeling uncomfortable with certain questions. Other risks may include disclosures of internal policies and procedures in reference to participant's role at their relative place of employment, which may impact their relationship with their employer.

POTENTIAL BENEFITS TO PARTICIPANTS AND/OR TO SOCIETY

While there are no direct benefits to the study participants, there are several anticipated benefits to society by contributing to the current gap in literature.

CONFIDENTIALITY

I will keep your records for this study confidential, as far as permitted by law. However, if I am required to do so by law, I may be required to disclose information collected about you. Examples of the types of issues that would require me to break confidentiality are if you tell me about instances of child abuse and elder abuse. Pepperdine's University's Human Subjects Protection Program (HSPP) may also access the data collected. The HSPP occasionally reviews and monitors research studies to protect the rights and welfare of research subjects.

Any identifiable information obtained in connection with this study will remain confidential. Audio recordings from the interview will be immediately transcribed, and all recordings will be destroyed. Your responses will be coded with a pseudonym and transcript data will be maintained separately. Any reference made to you, or respective institution will be redacted from the transcripts. Upon completion of each transcript, the associated audio file will be immediately destroyed. The transcribed data will be stored on a password protected computer in the principal investigators place of residency. The transcribed file will not be named, to ensure additional confidentiality. All records, handwritten and electronic, will be stored in a secure file cabinet in a locked office, in the principal researcher's home. The data will be stored for a minimum of three years, after which the data will be destroyed. Reporting of the data will be done in aggregate. Participants will be provided a copy of the formal report, upon completion of the study.

PARTICIPATION AND WITHDRAWAL

Your participation is voluntary. Your refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may withdraw your consent at any time and discontinue participation without penalty. You are not waiving any legal claims, rights or remedies because of your participation in this research study.

ALTERNATIVES TO FULL PARTICIPATION

The alternative to participation in the study is not participating or completing only the items which you feel comfortable.

INVESTIGATOR'S CONTACT INFORMATION

I understand that the investigator is willing to answer any inquiries I may have concerning the research herein described. I understand that I may contact Dr. Farzin Madjidi at farzin.madjidi@pepperdine.edu if I have any other questions or concerns about this research.

RIGHTS OF RESEARCH PARTICIPANT – IRB CONTACT INFORMATION

If you have questions, concerns or complaints about your rights as a research participant or research in general please contact Dr. Judy Ho, Chairperson of the Graduate & Professional Schools Institutional

Review Board at Pepperdine University 6100 Center Drive Suite 500, Los Angeles, CA 90045, 310-568-5753 or gpsirb@pepperdine.edu.

APPENDIX F

Letter of Intent

Dear [Participant],

Thank you for your response to my request for participation. I am a member of the Association of College and University Policy administrators (ACUPA), and am entering into the research phase of my doctoral program in Organizational Leadership at Pepperdine University. My research is in partial fulfillment of the requirements for the dissertation, titled *Cyber-Harassment in Higher Education: A Study of Institutional Policies and Procedures*.

The purpose of my research is to examine strategies, best practices, and challenges experienced by higher education institutions when preventing and mitigating cyber-harassment. Please note that this study is fulfilling an academic requirement, and is not commissioned by ACUPA.

Your participation in this research study will take the form of a one-hour interview. With your permission, the interview audio will be recorded. Immediately following the interview, the conversation will be transcribed to ensure that inadvertent references made to your name or institution are redacted. The transcribed file will not be named, to ensure additional confidentiality, and the associated audio file will be immediately destroyed. The information shared in the interview will be confidential, and to further ensure confidentiality, reporting of the data will be done in aggregate and only themes will be disclosed as part of the research study.

The interview may take place in person or facilitated through technological means. During the interview, you will be asked a series of questions pertaining to your experience in higher education policy development and implementation. Potential risks subjects may be exposed to include fatigue, boredom, or feeling uncomfortable with certain questions. Other risks may include disclosures of internal policies and procedures in reference to participant's role at their relative place of employment, which may impact their relationship with their employer. Your participation in this study is completely voluntary, and you may elect to withdraw at any point and time during the study. The results of the study will be used to increase the body of knowledge with regard to cyber-harassment policy development and implementation. Attached you will find an *Informed Consent* form, which will provide additional details of the study.

Thank you again for your expressed willingness to participate in this research study.

Respectfully,
Victoria Schaefer-Ramirez

APPENDIX G

Nondisclosure and Review Form for Inter-Rater Reliability

PEPPERDINE UNIVERSITY

INTER-RATER PEER REVIEWER NONDISCLOSURE

Reviewer will protect the information related to participant interview data and the review associated with the dissertation entitled *Cyber-harassment in Higher Education: A Study of Institutional Policies and Procedures*.

The reviewer will be privy to notes, transcripts, and coding associated with participant interviews. As such, the reviewer shall treat all interview data as protected information, regardless of the format (e.g., electronic, paper, oral). Additionally, the reviewer agrees to not use, share, or disclose the interview data with anyone other than the researcher. Though the interview files will only contain redacted information and participant codes, this form serves as an additional level of confidentiality.

SIGNATURE OF PEER REVIEWER

I have read the information provided above, and have been given a chance to ask questions. My questions have been answered to my satisfaction and I agree to the terms and conditions outlined herein. I have been given a copy of this form.

_____

Name of Reviewer

_____ _____

Signature of Reviewer Date

APPENDIX H

Interview Questions

Interview Question 1: How do you define “cyber-harassment”?

Interview Question 2: What are your best practices for the prevention and mitigation of cyber-harassment?

Interview Question 3: What resources (e.g., training, education, etc.) do you think are most helpful in implementing a successful prevention and mitigation program for cyber-harassment?

Interview Question 4: What policy implementation process techniques and methods have worked in your development of prevention and mitigation programs for cyber-harassment?

Interview Question 5: What were the major challenges and/or obstacles (direct or indirect) in developing and implementing policy related to prevention and mitigation of cyber-harassment?

Interview Question 6: What were the major challenges and/or surprises in the development and implementation process related to prevention and mitigation of cyber-harassment?

Interview Question 7: How did you deal with and/or overcome those challenges?

Interview Question 8: How does your institution measure the success of cyber-harassment policies and procedures?

Interview Question 9: What evaluation methods does your institution use to measure success for the program and policy implementation effectiveness related to prevention and mitigation of cyber-harassment?

Interview Question 10: How do you assess your interim success through the policy development and implementation process? For instance, how did you know things were going according to plan?

Interview Question 11: How would you personally describe the elements of a successful prevention and mitigation cyber-harassment policy and procedure?

Interview Question 12: How could these elements be measured and tracked by the institution to ensure a successful cyber-harassment prevention program?

Interview Question 13: What recommendations would you make for higher education institutions as they begin to design and implement a cyber-harassment prevention program?

Interview Question 14: Is there anything else you would like to share about your experience in prevention and mitigation of cyber-harassment that you think would be relevant to this study?