APPROVAL SHEET

Title of Dissertation: The Work of Cybersecurity Advocates

Name of Candidate: Julie Haney
Doctor of Philosophy, 2020

Dissertation and Abstract Approved: [Signature]

Wayne Lütters
Associate Professor
Department of Information Systems, Human-Centered Computing

Date Approved: March 26th, 2020

NOTE: *The Approval Sheet with the original signature must accompany the thesis or dissertation. No terminal punctuation is to be used.
Cyber attacks are on the rise, with potentially devastating effects at the personal, business, and national levels. Despite real and evolving cyber threats, people often fail to implement and effectively use basic, well-known cybersecurity technologies and practices. Further contributing to the cybersecurity problem is the shortage of security personnel to address these challenges.

A critical role and force-multiplier in security adoption is the cybersecurity advocate: a security professional who has the skills to effectively promote security and facilitate positive security behavior change. Cybersecurity advocates attempt to remedy implementation failures by promoting and facilitating the adoption of security best practices and technologies as an integral component of their jobs.

Currently, there is no clear career track and few resources for educating professionals on how to be good cybersecurity advocates. Furthermore, it is unclear as to what advocacy techniques may be most effective. In addition to the bias towards technical skills, these gaps are likely due to the fact that we have little understanding of the work practices and competencies that lead to successful security advocacy.

The purpose of my research is to gain a better understanding of these work practices. A first stage in my investigation involved interviews of professional security advocates. Since this interview data was one-sided from the perspective of advocates themselves, I validated the
findings with a second stage exploring the effectiveness of advocates’ approaches via a case study of a security awareness team at a U.S. government agency.

This research uncovers definitional boundaries of cybersecurity advocates, including skills, characteristics, motivations, challenges, and tactics. Findings reveal that advocates employ technical and non-technical skills and a variety of techniques to overcome negative perceptions of security and other barriers to security adoption. A better understanding of the work of advocates can inform more effective security advocacy techniques and resources to aid in professional development of advocates. A promulgation of this understanding to practitioners and educators may result in an increase in cybersecurity advocates armed with the necessary tools to be successful. This growth of the advocate workforce might then lead to increased adoption of cybersecurity best practices.
THE WORK OF CYBERSECURITY ADVOCATES

By

Julie Marie Haney

Dissertation submitted to the Faculty of the Graduate School of the University of Maryland, Baltimore County, in partial fulfillment of the requirements for the degree of Doctor of Philosophy
2020
Dedication

To my husband, Mark: Thank you for your unconditional love and support, for never complaining when I was occupied with schoolwork and research, and, most of all, for believing in me. You are my love and my best friend. I couldn’t have done this without you.

To my daughters, Anna and Faith: Thanks for your constant encouragement and for not thinking your mom was crazy for going back to school. I am so blessed to be your mother.
Acknowledgements

I would like to thank the following individuals:

- Dr. Wayne Lutters for his encouragement, amazing mentorship, and the many hours he spent supporting me as an advisor;
- My committee members (Dr. Richard Forno, Dr. Kirstie Hawkey, Dr. Anita Komlodi, Dr. Ravi Kuber, and Dr. Aaron Massey) for their guidance and challenging me to look at things in a different light;
- My amazing work colleagues and supervisors at NIST and, previously, at Department of Defense for their encouragement and support;
- My professors and fellow graduate students in the Human-Centered Computing program at UMBC who shared their knowledge and talents and instilled in me a love of this field;
- The participants in my studies who took time from their busy schedules to be interviewed, especially those at “Agency A” who allowed me into their spaces to learn about their work;
- Last, but not least, my family and friends for their love and prayers throughout this journey.
Table of Contents

Dedication.................................................................................................................. ii
Acknowledgements ..................................................................................................... iii
Table of Contents ....................................................................................................... iv
List of Tables ............................................................................................................. ix
List of Figures ........................................................................................................... x

1 Introduction ............................................................................................................. 1
  1.1 The Cybersecurity Challenge .............................................................................. 1
  1.2 What is a Cybersecurity Advocate? ..................................................................... 3
  1.3 Research Motivation, Purpose, and Questions ...................................................... 4
  1.4 Approach ........................................................................................................... 6
  1.5 Contributions ..................................................................................................... 6
  1.6 Dissertation Structure ......................................................................................... 7

2 Related Literature ................................................................................................... 10
  2.1 Risk Communication ........................................................................................... 10
  2.1.1 Risk Message Receiver .................................................................................. 11
  2.1.2 Risk Message ................................................................................................ 12
  2.1.3 Risk Communicators ..................................................................................... 13
  2.2 Diffusion of Innovations Theory and Change Agents .......................................... 15
  2.2.1 Factors in Technology Adoption .................................................................. 16
  2.2.2 Change Agents ............................................................................................. 17
  2.3 Service Orientation ............................................................................................ 19
  2.4 Security Professionals ......................................................................................... 20
  2.4.1 Traditional Security Professionals ................................................................ 21
  2.4.2 Security Awareness Professionals ................................................................. 29
  2.5 Security Mental Models and Perceptions ............................................................ 30
  2.6 Economics of Cybersecurity .............................................................................. 32
  2.7 Persuasion Techniques in Cybersecurity ............................................................. 35
  2.8 Advocacy in Other Domains .............................................................................. 36
  2.9 Addressing Research Gaps .................................................................................. 37

3 Study Design and Methodology .............................................................................. 40
  3.1 Interviews of Cybersecurity Advocates .............................................................. 40
  3.1.1 Sampling and Recruitment .......................................................................... 41
  3.1.2 Participant Demographics ........................................................................... 43
3.2 Case Study: Cybersecurity Advocacy in Practice ........................................... 51
  3.2.1 Selection of Case Study Method .......................................................... 52
  3.2.2 Selection of Organization .................................................................. 53
  3.2.3 Data Collection .................................................................................. 55
  3.2.4 Analysis ............................................................................................. 61
  3.2.5 Study Design Tradeoffs ..................................................................... 62

3.3 Mapping to Research Questions ................................................................... 63

3.4 Disclosure of Researcher Experience and Biases ......................................... 63

3.5 Timeline .................................................................................................... 65

4 Interview Study: Advocate Characteristics ...................................................... 67

4.1 Skills and Characteristics ............................................................................ 67
  4.1.1 Technical Skills .................................................................................. 67
  4.1.2 Non-technical Skills .......................................................................... 69
  4.1.3 Service Orientation .......................................................................... 69
  4.1.4 Pro-Social Passion ............................................................................ 71
  4.1.5 Discipline Diversity .......................................................................... 73

4.2 Motivations .................................................................................................. 74
  4.2.1 Personal Interest ................................................................................ 75
  4.2.2 Self-Efficacy ..................................................................................... 76
  4.2.3 Sense of Duty ................................................................................... 76
  4.2.4 Evidence of Impact .......................................................................... 77
  4.2.5 Comradery ....................................................................................... 82
  4.2.6 Social Passion ................................................................................... 83

4.3 Chapter Summary ......................................................................................... 84

5 Interview Study: Overcoming Negative Perceptions of Security ..................... 85

5.1 Establishing Trust ......................................................................................... 86
  5.1.1 Relying on Organization Reputation .................................................. 86
  5.1.2 Demonstrating Technical Knowledge ............................................... 87
  5.1.3 Building Relationships ..................................................................... 88
  5.1.4 Leveraging Insider Access ................................................................ 89

5.2 Overcoming Perceptions that Security is Scary ........................................ 90
  5.2.1 Being Honest, Yet Discerning, About Risk ........................................ 91
  5.2.2 Empowering ..................................................................................... 92

5.3 Overcoming Perceptions that Security is Confusing .................................. 94
  5.3.1 Bridging the Gap ............................................................................... 95
  5.3.2 Educating .......................................................................................... 97
  5.3.3 Providing Practical Recommendations ............................................. 99
  5.3.4 Promoting Usability ......................................................................... 100

5.4 Overcoming Perceptions that Security is Dull and Not Relevant ............... 101
  5.4.1 Incentivizing Security Behaviors ..................................................... 103
  5.4.2 Using Engaging Communication Techniques .................................... 106

5
### 6 Interview Study: Organizational Challenges to Cybersecurity Adoption .............................................. 110

#### 6.1 Challenges ................................................................................................................................. 111

- 6.1.1 Weak Security Culture ........................................................................................................... 111
- 6.1.2 Economic Barriers .................................................................................................................... 113
- 6.1.3 Cybersecurity Workforce .......................................................................................................... 115
- 6.1.4 Policies and Regulations .......................................................................................................... 120

#### 6.2 Mitigation Strategies .................................................................................................................. 124

- 6.2.1 Bolstering the Cybersecurity Workforce .................................................................................. 126
- 6.2.2 Making a Business Case ........................................................................................................... 130
- 6.2.3 Targeting Multiple Levels ........................................................................................................ 133
- 6.2.4 Contributing to Policies & Regulations ..................................................................................... 136

#### 6.3 Chapter Summary ...................................................................................................................... 137

### 7 Case Study: Context ......................................................................................................................... 139

#### 7.1 Agency Description ..................................................................................................................... 139

- 7.1.1 Structure .................................................................................................................................. 139
- 7.1.2 Security Culture Expectations .................................................................................................. 140

#### 7.2 Security Awareness Team ......................................................................................................... 142

- 7.2.1 Placement within the Agency ................................................................................................... 142
- 7.2.2 History ..................................................................................................................................... 142
- 7.2.3 Mission ..................................................................................................................................... 142
- 7.2.4 Team Composition .................................................................................................................... 144

#### 7.3 Security Awareness Events ....................................................................................................... 145

- 7.3.1 Lunchtime Events ..................................................................................................................... 147
- 7.3.2 Security Officer Forums ............................................................................................................ 148
- 7.3.3 Security Days ........................................................................................................................... 149

#### 7.4 Other Security Awareness Approaches ..................................................................................... 150

- 7.4.1 Campaigns ............................................................................................................................... 150
- 7.4.2 Phishing exercises ..................................................................................................................... 150

#### 7.5 Challenges to Security Awareness Efforts ................................................................................ 152

- 7.5.1 Lack of Workforce Buy-in ........................................................................................................ 152
- 7.5.2 Human Error ............................................................................................................................ 154
- 7.5.3 Compliance-driven Training ..................................................................................................... 155
- 7.5.4 Resources ................................................................................................................................... 157

#### 7.6 Chapter Summary ...................................................................................................................... 157

### 8 Case Study: From Compliance to Advocacy and Empowerment .................................................... 159

#### 8.1 Evolving to a Cybersecurity Advocate Role ............................................................................... 160

- 8.1.1 Technical Knowledge and Relevance ......................................................................................... 160
- 8.1.2 Service Orientation ................................................................................................................... 163
- 8.1.3 Creativity and Adaptability ....................................................................................................... 164
- 8.1.4 Interpersonal Skills .................................................................................................................... 166
- 8.1.5 Communication Skills and Context Awareness .......................................................................... 166
- 8.1.6 Discipline Diversity .................................................................................................................. 169
8.2 Engaging and Empowering the Workforce ................................................................. 170
  8.2.1 Topicality .............................................................................................................. 172
  8.2.2 Work-Home Connection .................................................................................... 175
  8.2.3 Varied, Engaging Communication Techniques .................................................. 178
  8.2.4 Practical Recommendations ............................................................................... 184

8.3 Gauging Success ....................................................................................................... 186
  8.3.1 Compliance Metrics ............................................................................................ 186
  8.3.2 Event Attendance ............................................................................................... 187
  8.3.3 Employee Feedback ........................................................................................... 189
  8.3.4 User-Generated Incidents and Reporting ............................................................. 195
  8.3.5 Evidence of Leadership Support ....................................................................... 196

8.4 Continuously Improving .......................................................................................... 198
  8.4.1 Holistic Approach .............................................................................................. 199
  8.4.2 Developing New Incentives ............................................................................... 201
  8.4.3 Broader Reach .................................................................................................... 201
  8.4.4 Alignment with Other Agencies ........................................................................ 203

8.5 Chapter Summary ..................................................................................................... 204

9 Study Synthesis .......................................................................................................... 206
  9.1 Security Awareness Case as an Instantiation of Cybersecurity Advocacy ............... 206
  9.2 Advocate Skills & Characteristics ......................................................................... 207
    9.2.1 Technical Knowledge and Discipline Diversity ................................................. 208
    9.2.2 Non-technical Competencies .......................................................................... 209
    9.2.3 Service Orientation and Pro-social Passion ..................................................... 212
    9.2.4 Motivations ...................................................................................................... 213
  9.3 Organizational Challenges to Cybersecurity Advocacy .......................................... 215
    9.3.1 Cybersecurity Culture and Buy-in .................................................................... 217
    9.3.2 Economic Barriers ........................................................................................... 218
    9.3.3 Human Element ............................................................................................... 219
    9.3.4 Compliance-driven Cybersecurity Awareness .................................................. 220
    9.3.5 Policy Relevance ............................................................................................. 221
  9.4 Advocacy Techniques .............................................................................................. 222
    9.4.1 Communication Channels ................................................................................ 222
    9.4.2 Making Security Relevant ............................................................................... 224
    9.4.3 Use of Rhetorical Devices ............................................................................... 226
    9.4.4 Extrinsic Incentivization .................................................................................. 228
    9.4.5 Influence on Technical Solutions .................................................................... 229
  9.5 Audience Empowerment .......................................................................................... 230
  9.6 Measures of Effectiveness ...................................................................................... 232
  9.7 Chapter Summary ..................................................................................................... 233

10 Implications ................................................................................................................ 235
  10.1 Defining the Emerging Cybersecurity Advocate Role ............................................. 235
    10.1.1 Defining an Advocate Career Track ................................................................. 236
    10.1.2 Bolstering Non-Technical Competencies ......................................................... 237
    10.1.3 Attracting a Cybersecurity Advocate Workforce ............................................. 241
10.2 Communicating Cybersecurity Risk and Guidance ......................................................... 245
10.3 Advancing Security Awareness Programs ................................................................. 246

11 Contributions and Future Work ....................................................................................... 249
11.1 Contributions to the Research Body of Knowledge ...................................................... 249
11.1.1 Security Professionals ................................................................................................. 249
11.1.2 Technology Adoption and Change Agentry .............................................................. 251
11.1.3 Advancing Risk Communication ............................................................................... 252
11.1.4 Persuasion Techniques ............................................................................................... 255
11.2 Contributions to Cybersecurity Practice ........................................................................ 257
11.3 Limitations ..................................................................................................................... 258
11.4 Future Work .................................................................................................................... 260
11.5 Researcher Positionality ................................................................................................. 262
11.6 Conclusion ...................................................................................................................... 264

Appendix A: Interview Study Protocol ................................................................................. 265
Appendix B: Interview Study Demographic Survey ............................................................. 266
Appendix C: Interview Study Codebook .............................................................................. 269
Appendix D: Case Study Security Awareness Team Demographic Survey ......................... 272
Appendix E: Case Study Security Awareness Team Interview Protocol .............................. 274
Appendix F: Case Study Manager Interview Protocol ......................................................... 277
Appendix G: Case Study Employee Interview Protocol ....................................................... 278
Appendix H: Case Study Codebook ..................................................................................... 280

Bibliography .......................................................................................................................... 283
List of Tables

Table 1. Participant Demographics................................................................. 45
Table 2. Case Study Employee Demographics................................................ 60
Table 3. Mapping data collection methods to research questions ..................... 62
Table 4. Mapping organizational challenges to advocate mitigation strategies .......... 125
Table 5. Observed Events .................................................................................. 146
Table 6. Interview study challenges mapped to case study challenges .................. 216
Table 7. Rhetorical devices and examples from the interview and case studies ............. 227
Table 8. Proposed educational program for cybersecurity advocates ..................... 240
List of Figures

Figure 1. Framework of how cybersecurity advocates overcome negative perceptions of security .................................................................................................................................................. 86

Figure 2. Phishing awareness handout.............................................................................................................. 165

Figure 3. Tips for Security Holiday Tech Gifts handout. .................................................................................. 177

Figure 4. Click with Care Campaign handout. .................................................................................................... 180

Figure 5. “To send or not to send” lunchtime event handout excerpts. ............................................................... 183

Figure 6. Reasons for security day event attendance.......................................................................................... 192
1 Introduction

1.1 The Cybersecurity Challenge

Cyber attacks are on the rise, and companies, government agencies, and individuals are being exploited at an alarming pace by both known “tried and tested techniques” (Verizon, 2018, p. 2) and “zero-day” exploits (new, unexpected attack methods) (Symantec, 2018). A 2016 survey conducted by a major telecommunications provider found that over 60% of the businesses surveyed had an information technology (IT) security breach in 2015, with 42% of those indicating that the breach resulted in significant negative impact (AT&T, 2016). The number of reported security breaches increased almost 600% between 2005 and 2016 (Statista, 2017). This growth does not even include the many unreported breaches affecting both organizations and individuals. The effects of cyber attacks can be devastating on personal, business, national, and global levels. In 2016, cybercrime and espionage cost the global economy over $450 billion with more than two billion personal records stolen (Hiscox, 2017).

While sophisticated attackers may sometimes use zero-day exploits that target previously undisclosed and unpatched vulnerabilities, it is estimated that over 80 percent of cyber attacks take advantage of known vulnerabilities that could have been countered by existing solutions (Pescatore, 2017). Despite real and evolving cyber threats, organizations and individuals are falling behind in defending their systems and networks,
often failing to implement and effectively use basic, well-known cybersecurity\(^1\) practices and technologies (Clinton, 2014; Hiscox, 2017). Reasons for this failure vary. From an organizational perspective, a survey of 437 security professionals revealed that a shortage of skilled security staff, a lack of security training for non-technical employees, and management not regarding security as a priority contribute to lackluster security postures (Oltsik, 2016). From an individual perspective, less technical users often lack the awareness and skill to properly protect their digital assets and may harbor negative feelings about security, including frustration and futility (Dourish, Grinter, De La Flor, & Joseph, 2004; Stanton, Theofanos, Prettyman, & Furman, 2016).

Further contributing to the cybersecurity problem is the shortage of security personnel to address these challenges. Despite significant government and industry efforts to increase the quantity and quality of the pipeline for future security professionals (National Security Agency, 2018; McGettrick et al., 2014), industry research firms predict that there will be an estimated gap of between two and 3.5 million cybersecurity workers by 2019-2020 (Cybersecurity Ventures, 2017). In addition to the explosion in demand due to technological advancements, reasons for the shortage of security professionals may be the result of real and perceived deficiencies in the field. These deficiencies include a lack of clear career pathways, the dearth of women in the security workforce, a lack of flexibility in the workplace, an outdated educational curriculum, a

\(^{1}\) "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (National Initiative for Cybersecurity Careers and Studies, 2017)
misguided focus on technically inadequate professional certifications, and a scarcity of junior security positions to allow younger people the opportunity to explore the field (Caldwell, 2013; Evans & Reeder, 2010).

Who, then, may have a role in encouraging more security implementation given the current limited security workforce? A potential helper in security adoption is the security professional who has the skills to effectively promote security and facilitate positive security behavior change. I refer to these professionals as *cybersecurity advocates*.

### 1.2 What is a Cybersecurity Advocate?

As defined by the Merriam Webster dictionary, an advocate is “one who supports or promotes the interests of a cause or group” (2018). Within the cybersecurity field, cybersecurity advocates are security professionals who attempt to remedy implementation failures by actively promoting and facilitating the adoption of security best practices and technologies as an integral component of their jobs. These advocates not only have technical skills, but also possess the ability to educate, persuade, and serve as organizational change agents for cybersecurity adoption. They need to effectively communicate cyber risk and facilitate mitigation of that risk. Their ultimate goal is to enable positive security behavior change in their target audience.

“Cybersecurity advocate” is an emerging term-of-art among practitioners, with most advocates not identified as such by their official job title, although some do have more overt titles such as “security evangelist.” Many are part-time advocates, having to perform advocacy tasks in parallel with other responsibilities. While some advocates have formal education in computing disciplines, others may come into the profession from non-technical disciplines such as communications, law, and business. They
advocate security to a variety of individuals, including home users, office workers, students, faculty, technical staff, developers, and executives. Examples of advocates include:

- individuals designing and executing security awareness programs within their organizations
- non-profit security advocacy staff who develop security campaigns and publish guidance
- consultants who provide security recommendations and work to convince their clients about the benefit of implementing security measures
- security educators who teach technical or non-technical audiences
- senior executives who must champion security within their institution

1.3 Research Motivation, Purpose, and Questions

Given modern society’s dependence on technology and the challenges of following security best practices, cybersecurity advocacy may be a way to increase the security posture of organizations and individuals. The work of cybersecurity advocates has similarities to, but does not fall cleanly within, the boundaries of other tech administration or oversight roles (e.g., compliance officer) or traditional security work roles, for example, those defined in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (known as the NICE Framework) (Newhouse, Keith, Scribner, and Witte, 2017) and the Skills Framework for the Information Age Foundation (2018). A review of these resources reveals that much of cybersecurity education is viewed through a technical lens, with little to no mention of non-technical competencies, such as communication and interpersonal skills. These skills
are particularly important to the work of cybersecurity advocates who have a social and organizational focus (Lapena, 2017).

Currently, there is no clear career track and few resources for educating professionals on how to be good cybersecurity advocates. Furthermore, it is unclear as to what advocacy techniques may be most effective in the cybersecurity context. In addition to the bias towards technical skills, these gaps are likely due in part to the fact that we have little understanding of the work practices and competencies that lead to successful advocacy.

The purpose of my research is to gain a better understanding of cybersecurity advocate work practice. This understanding can inform more effective security advocacy techniques and resources to aid in the professional development and daily work of advocates. My dissertation goals are to answer the following research questions (RQs):

RQ1: What are the motivations, professional characteristics, and skills of cybersecurity advocates?

RQ2: What techniques do cybersecurity advocates use to encourage security adoption?

RQ3: What are the rewards and challenges experienced by cybersecurity advocates?

RQ4: From where do cybersecurity advocates get their security information and knowledge?

RQ5: What techniques and attributes of cybersecurity advocates result in motivating their clients/audience to change behavior?
1.4 Approach

My dissertation was conducted in two stages that explore cybersecurity advocacy from multiple perspectives. A first stage consisted of interviews of 28 professional security advocates with a goal of better defining the definitional boundaries of cybersecurity advocates, including who they are, what they do, and why they do it. This includes their common techniques and the skills and characteristics they must possess to be successful. Since these informative interviews were one-sided from the perspective of advocates themselves, I sought to triangulate my findings with a case study that explored cybersecurity advocacy in practice. The case study was an ethnographically-informed investigation of a security awareness team at a U.S. government agency (“Agency A”). Contextual interviews of members, their managers, and employees of Agency A were conducted to explore the advocacy techniques employed routinely and which techniques most resonated with members of the organization. In addition, I attended events organized by the team to observe techniques and audience reactions. Lastly, the examination of security awareness team documentation (including security awareness materials, post-event reports, and surveys) provided further insight into which techniques advocates implement in distributed materials and how others in the organization view security awareness efforts.

1.5 Contributions

My research makes several contributions (more details about contributions are included in Chapter 11). This is the first effort to define the cybersecurity advocate role (including skills and characteristics), gain a better understanding of advocates’ work practices in a variety of contexts, and provide an external view of organizational
cybersecurity challenges from the perspective of advocates themselves. The research also informs the development of a new cybersecurity advocate work role, including recommendations for recruitment and retention and an educational program for individuals progressing into an advocate role. Additionally, findings provide insight into actions cybersecurity advocates can take to influence real change in organizational cybersecurity practices. The cataloguing of security advocacy techniques can inform more effective security advocacy techniques and resources to aid in the professional development of advocates. This understanding also permits an investigation into how advocates leverage general risk communication practices and where they introduce security-specific innovations. These innovations contribute to and extend the risk communication body of knowledge, which currently focuses more on physical safety topics, and not as much on abstract concepts such as cybersecurity.

It is my hope that a promulgation of the identified techniques and competencies to practitioners and educators will result in an increase in the number of cybersecurity advocates armed with the necessary skills and techniques to be successful. This growth of the advocate workforce may potentially lead to increased adoption of cybersecurity best practices within organizations and turning the tide of our collective increased cyber vulnerability and loss.

1.6 Dissertation Structure
The following outlines the contents of the remainder of the dissertation.

Chapter 2 Related Literature - Chapter 2 frames the research within the context of existing research literature. Foundations can be found in risk communication, technology adoption (in particular, Diffusion of Innovations Theory), advocacy in other domains,
service orientation, and cybersecurity economics. As a point of reference for my dissertation research, I also include an overview of related, more contemporary work about security professionals, security perceptions, and persuasion within the cybersecurity context.

**Chapter 3 Study Design and Methodology** - Chapter 3 explains the overall study design and methodology choices employed during the two stages of my dissertation research: an interview study of 28 cybersecurity advocates from industry, government, higher education, and non-profits and a case study of a security awareness team in a U.S. government agency. Sampling, recruitment, data collection, analysis, and study design tradeoffs are described.

**Chapter 4 Interview Study: Advocate Characteristics** – Chapter 4 presents the interview study findings related to skills, characteristics, and motivations of cybersecurity advocates.

**Chapter 5 Interview Study: Overcoming Negative Perceptions of Security** – Chapter 5 continues to report on interview study findings by discussing the competencies and techniques advocates employ to overcome widely-held negative perceptions that security is scary, confusing, and dull/irrelevant.

**Chapter 6 Interview Study: Organizational Challenges to Cybersecurity Adoption** – Chapter 6 concludes the interview study findings by enumerating organizational challenges to cybersecurity adoption from the perspective of advocates. Advocates’ mitigation strategies for overcoming these challenges are also presented.
Chapter 7 Case Study: Context – Chapter 7 provides background and context for the case study of a security awareness team at a government agency. Descriptions of the agency, security awareness team, and security awareness approaches are provided.

Chapter 8 Case Study: From Compliance to Advocacy and Empowerment – Chapter 8 presents the findings of the case study centered on the transformation of the agency’s security awareness program from compliance-based education into an effort motivated towards security advocacy and employee empowerment.

Chapter 9 Study Synthesis – Chapter 9 situates the case study as an instantiation of the emerging cybersecurity advocate role identified in the interview study. A mapping between the two studies illustrates similarities and differences in findings.

Chapter 10 Implications – Chapter 10 discusses practical implications of the entirety of the research and what the findings suggest for shaping the cybersecurity advocate role.

Chapter 11 Contributions and Future Work – Chapter 11 summarizes contributions to both the research body of knowledge and practitioner community. Future work to address the limitations of the interview and case studies is also provided. Finally, a concluding statement summarizes the implications of the research.
2 Related Literature

In this section, I first describe theories and prior work in risk communication, technology adoption, and service orientation. This body of research provides a foundational context in which to interpret, orient, and differentiate my dissertation work. I then summarize related contemporary work within the cybersecurity context, including work practices and skills of security professionals, security mental models/perceptions of users, economics of cybersecurity, persuasion techniques, and advocacy in other domains.

2.1 Risk Communication

Security advocates attempt to motivate individuals to practice good security habits and adopt security technologies in large part by conveying and convincing them of risks within the cyber realm. To be successful, this requires an understanding of how their audiences perceive risk and knowing how to effectively communicate risk. Thus, when exploring the work practices and effectiveness of advocates, risk communication literature can provide a foundation in understanding phenomena encountered by advocates. This body of knowledge can also serve as a basis for comparison between recommended communication approaches and what is being practiced in the security field.

Risk communication is “the interactive process of exchanging information about a risk (its nature, meaning, consequences, likelihood, and response options) to individuals so that they can make informed judgements” (Nurse, Creese, Goldsmith, & Lamberts, 2011, p. 61). Risk communication goals, which, based on preliminary analysis of the first phase of my research, appear to be similar to those of security advocates, include:
advancing or changing knowledge and attitudes through information and education; modifying risk-relevant behavior; and facilitating joint conflict resolution and decision making (Covello, von Winterfeldt, & Slovic, 1988; Rohrmann, 1992).

Risk communication is not a trivial undertaking. Psychologist and decision researcher Paul Slovic contended that risk communication is a “battlefield” (1999, p. 689). It follows then that cybersecurity advocates, who are, in essence, risk communicators, must arm themselves with the proper knowledge and tools to overcome potential barriers. In this section, I summarize relevant risk communication literature in terms of the risk message receiver, the risk message, and the risk communicator. While a small set of research has been conducted on risk communication within the security field, much has its roots in other fields such as health, environmental hazards, and disaster management. However, there are still lessons to be learned from these other domains as well as points of comparison to my research to ascertain if cybersecurity may be different, for example, due to its often abstract nature.

2.1.1 Risk Message Receiver

In his well-cited paper “Perception of Risk,” Slovic (1987) emphasized that those who promote and regulate safety-related fields should have an understanding of how non-experts (referred to here as the public) consider and respond to risk:

“…there is wisdom as well as error in public attitudes and perceptions…As a result, risk communication and risk management efforts are destined to fail unless they are structured as a two-way process. Each side, expert and public, has something valid to contribute. Each side must respect the insights and intelligence of the other.” (p. 285)
This suggests that cybersecurity advocates, who indeed work in a safety-related field (albeit one with generally less physical consequences), should actively engage their audiences in order to gain an appreciation of perceptions of cyber risk and the root causes of security behavior.

Risk perception, acceptance, and communication are socially-rooted, culturally-influenced, and psychologically-oriented phenomena (Nurse et al., 2011; Slovic, 1987; Wildavsky & Dake, 1990). People use mental heuristics to make sense of their world, but these can sometimes lead to biases that impact their ability to properly assess risk. For example, misinterpretation of probability, subjective media coverage, and misleading personal experiences may result in risks being overestimated or underestimated. Starr (1969) found that factors such as level of knowledge, control, and catastrophic potential factors influence perceived risk, perceived benefit, and risk acceptance. More recently, Huang, Rau, and Salvendy (2007) and Nurse et al. (2011) noted similar influences on risk perception within the security context, including knowledge, impact, severity, controllability, awareness, and possibility.

2.1.2 Risk Message

An important aspect of risk message construction is the understanding of how people decide whether or not to trust a piece of information. Nurse et al. (2011) found that perceived information trustworthiness factors are divided into three components: source, information, and end-user. Source factors include the source’s identity (e.g. authority, credentials), reputation, recommendations/ratings, and popularity. Information factors include accuracy, believability, presentation and format, relevance, timeliness,
and verifiability. Examples of end-user trustworthiness factors include context, beliefs, motivation, expertise, and risk propensity.

Even with considerations for trustworthiness, constructing an effective risk message can be a complex task, in large part due to the inherent complexity of the risk problems themselves. Presentation format -- whether it be numeric (e.g., percentages, probabilities), verbal, or visual (e.g., graphics, charts, diagrams) -- is important, but audience dependent (Nurse et al., 2011). For example, the use of numeric data may mistakenly presume that the audience has a high level of numeracy (Peters, 2008).

Additional recommendations from previous research concerning how to construct and communicate the risk message are included in the next section on risk communicators. A related body of work on persuasion in the security context is also discussed in section 2.6.

2.1.3 Risk Communicators

To form a basis for potential skills, knowledge, and abilities necessary for cybersecurity advocacy, it is helpful to look at past literature on risk communicators. Although presented within a hazardous facilities context, Kasperson, Golding, and Tuler (1992) claimed that five risk communicator goals hold true across multiple domains and appear to be in line with my research’s preliminary findings. They said that risk communicators aim to 1) diagnose and create trust, 2) create awareness strategies, 3) understand why concepts are hard to grasp and find ways to overcome this, 4) develop mediating skills, and 5) motivate the public to act.

A body of literature explores the goals and the skills risk communicators must possess to be successful. Covello (1997) observed that risk communicators may lack the
necessary proficiencies. For example, they may use difficult-to-understand technical jargon and can be insensitive to differences between the information needs of experts and lay people. Within the toxicology field, Rowan (1994) observed that risk communication can be controversial because it involves threatening and poorly understood concepts that can invoke hostile feelings towards the risk communicator. Therefore, they also must be able to diffuse negative feelings so as not to erode trust, reframe negative messages into positives when appropriate, and practice negotiation skills (Rowan, 1994). Since a foundational aspect of risk communication is the establishment of trust and credibility, communicators need to exhibit empathy, honesty, openness, and commitment (Covello, 1997). Additionally, although historically risk communicators “have been the interpreters, clarifiers, and simplifiers of technical jargon” (Ng & Hamby, 1997, p. 474), Bradbury (1994) argued that this archetype is no longer sufficient. Like Slovic (1987), she advocated a move towards more interactive dialogue between the public and risk communicators rather than a one-way sender-receiver relationship. This new paradigm requires communicators to have listening skills and be able to respond to their audience’s concerns, opinions, and emotions. Risk communicators, in effect, must serve as the bridge between technical experts and non-experts (Gordon, 1991). As risk communicators, cybersecurity advocates serve as this bridge by translating highly technical information into terms their audience understands. This translation necessitates establishing common ground, which is the mutual knowledge, beliefs, and assumptions that are believed to be essential for successful communication between people (Clark & Brennan, 1991). Grounding approaches may vary depending on the purpose and the
medium of communication. For example, common ground establishment may be
different in face-to-face situations versus written communication.

In addition to interpersonal skills, risk communication is a learned competency
that includes a variety of approaches: practicing judicious use of jargon, visuals, and
statistics; keeping communications simple, but specific and unambiguous; customizing
security risk information to target audiences; assisting people in seeing the consequences
of their decisions, providing clear and precise directions for action; presenting
information in an engaging manner, and effectively using non-verbal cues (Covello,
communication and increasing trust and consensus, including role-playing, co-orientation
(to understand each other’s position), and efficacy building (to increase the group’s sense
of its own power).

Risk communication literature begins to form a picture of an effective risk
communicator. However, little research has investigated whether these risk
communicator characteristics, approaches, and goals hold true within the security realm.

2.2 Diffusion of Innovations Theory and Change Agents

Since the goal of security advocacy is positive behavior change and adoption of
beneficial practices or tools, technology adoption literature serves as an important
foundation for my research. There are numerous models that seek to describe the process
and influential factors of technology adoption, for example the Technology-Organization-
Environment framework (Tornatzky, Fleischer, & Chakrabarti, 1990) and the Technology
Adoption Model (Davis, 1989). In particular, Diffusion of Innovations Theory (DOI)
reveals a variety of factors that influence the acceptance of an innovation, which is “an
idea, practice, or object perceived as new by an individual or other unit of adoption” (Rogers, 2003, p. 475). In the context of my research, the innovations are focused on cybersecurity. Note that an innovation need not be something newly invented, but rather not previously used or practiced by the adopter (individual or some other unit).

2.2.1 Factors in Technology Adoption

Within DOI, the innovation-decision process is how an adopter moves from initial exposure to a decision to continue usage of the technology. This process involves five stages: 1) knowledge, which includes information gathering about the innovation; 2) persuasion, which is when a positive or negative attitude is formed towards the innovation; 3) decision, when a choice is made about whether or not to adopt the innovation; 4) implementation, when the innovation is put into use; and 5) confirmation, when the decision to adopt is reinforced or reversed (Rogers, 2003).

For individual adopters, Rogers (2003) described five attributes of innovations that impact technology adoption. These include: 1) relative advantage, the degree to which the adopter perceives the innovation to be better than the status quo; 2) compatibility, the degree to which the innovation is compatible with the adopter’s values and needs; 3) complexity, how difficult the innovation is to understand and use; 4) trialability, the degree to which the adopter can experiment with the innovation; and 5) observability, the degree to which the innovation’s results are apparent to others. From an organizational perspective, there are similar factors that can impact technology adoption, including motivation and ability to change, compatibility between the organizational technical/social constructs and the technology, and the ability of the adopters to observe the technology’s implications and impact. Adoption within organizations is often
facilitated through internal opinion leaders (well-respected individuals) and innovation champions. Preventive technologies (such as cybersecurity technologies) face a particular adoption challenge for both individuals and organizations. They often spread at a much slower rate, partly because of delayed or difficult-to-observe rewards from adoption.

DOI Theory has been occasionally applied to the cybersecurity context. Informed by DOI, Turner (2009) proposed a theory-based security adoption model, then validated the model using a mixed-methods approach of a survey and qualitative case study of a security technology implementation within a banking organization. Compatibility and complexity were found to be major factors in determining the success of security technology adoption. Xiao, Witschey, and Murphy-Hill (2014) performed a study to explore social factors influencing the adoption of secure software development tools within organizations. Interviews of software developers revealed that both organizational factors (policies, culture, security concerns, structure, and education and training) and communication channel factors (exposure and trust) impacted whether or not developers adopted security tools. These security-focused adoption studies show the successful application of DOI Theory within the cybersecurity field and allude to interesting implications for factors and barriers cybersecurity advocates need to address to persuade their target audience to adopt security technologies or practices.

2.2.2 Change Agents

DOI also identifies and defines a critical role in technology adoption: the change agent. Understanding this role has particular importance for my research since cybersecurity advocates serve as change agents in the adoption of security technologies and best practices.
Change agents were originally described in DOI as individuals who influence their clients’ (target audience’s) innovation decisions in a direction deemed desirable by a change agency (the organization or entity on behalf of which the change agent works). Rogers (2003) suggests that the change agent has several roles contributing to the innovation-decision process of clients, including creating a need for and intent to change, establishing an information exchange relationship, diagnosing problems, stabilizing adoption, and fostering client independence. The success of the change agent is positively related to her ability to develop credibility in the clients’ eyes, be client-oriented, exhibit empathy with clients, create a common bond with clients (e.g., by having a similar outlook and goals), communicate the compatibility of the technology with the clients’ needs, and assist the client in becoming independent.

To date, I have found no change agentry research within the cybersecurity field. However, there have been several applications within the related Information Systems (IS) field. One of the earliest papers about the IS change agent concept was a case study piece by Allen (1995). The author described his efforts to facilitate a shift from a technology-centered paradigm to a customer-centered paradigm during his time as a group manager within a successful software company. Through a descriptive narrative of his own experience, he highlighted the qualities of a good change agent, such as caring more about the betterment of the organization than about personal credit, teaming, and good communication skills (including messaging and framing). He also underscored the importance of self-reflection and context-dependent adaptation. Also within the IS field, Markus and Benjamin’s foundational paper (1996) offered detailed descriptions of three potential roles of change agents: traditional, facilitator, and advocate. Recognizing that
change agents rarely receive any formal training on how best to do their jobs, the authors also proposed an outline of an educational program on change agentry that included units on approaches, coping with challenges, and awareness of organizational and structural conditions. Winston (1999) extended Markus and Benjamin’s work by examining multiple real-world case studies. Her study showed that consultants who are flexible and can adapt their change agent role depending on the situation are more likely to be successful. Winston also made a case for creating specialized change agent education.

In my cybersecurity advocate research, the change agent body of research can be used as a basis against which to compare advocates’ competencies and evaluate how advocates are facilitating adoption in a variety of situations.

2.3 Service Orientation

Service orientation is a theme that emerged from my research. Hogan, Hogan, and Busch (1984) defined service orientation as the willingness to treat customers with courtesy, consideration, and tact; perceptiveness to customer needs; and the ability to communicate accurately and pleasantly. Although most prior service orientation research was conducted in a business and service industry context, my data analysis thus far leads me to believe it has implications for cybersecurity advocacy as advocates’ audiences can ultimately be viewed as “customers” of security guidance, and advocates repeatedly expressed their commitment to service.

Brown, Mowan, Donavan, and Licata (2002) examined personality characteristics in service workers with respect to customer service orientation. They proposed that customer orientation is composed of two dimensions: a needs dimension that represents worker feelings of self-efficacy in their service role, and an enjoyment dimension that
represents how much interacting with and serving customers is enjoyable to the worker. Perry (1996) created a scale to measure public service motivation, finding that motivation consisted of multiple dimensions, including commitment to the public interest, civic duty, social justice, and compassion.

Although no cybersecurity research has specifically highlighted service orientation, several studies examined service orientation within the information systems (IS) and IT contexts. For example, Lounsbury et al. (2007) found that customer service orientation is positively related to both job and career satisfaction among IT employees. Crepeau, Crook, Goslar, and McMurtrey (1992) investigated career anchors (value-based self-perceptions that guide career decisions) of IS workers. They found that service, which they defined as a “concern with helping others and seeing changes that result from efforts,” (p. 148) was an important career anchor among those working in the field.

2.4 Security Professionals

Past research has explored the work practices, challenges, motivations, and skills of security professionals. Most work has been done with “traditional” security professionals who perform one or more of the following kinds of tasks (Botta et al., 2007; Haber & Kandogan, 2007; Hawkey et al., 2008):

- Designing, installing, administering, or testing security technologies
- Creating security procedures and policies
- Monitoring, detecting, and responding to security events
- Maintaining systems or infrastructures, especially those aspects that contribute to security
Cybersecurity advocates are security professionals whose role does not fall cleanly within the boundaries of these definitions. However, it is useful to examine, learn from, and apply past methods on how to study these populations. Additionally, by understanding the practices and challenges of traditional security professionals, similarities and differences in professional development needs for advocates can be discovered.

This section highlights some of the prior research projects aimed at traditional security professionals. Also included is a section dedicated to security awareness professionals, a group of security professionals who are also cybersecurity advocates. This group is of particular interest since several participants from the interview study served in this capacity and the focus of the case study is on a security awareness team. Although I could find no research specifically examining their work practices and characteristics, looking at guidelines for security awareness programs and industry studies and resources for this particular group provides insight into the work of this kind of advocate.

2.4.1 Traditional Security Professionals

2.4.1.1 Work Practices

Security professionals hold many different titles, including security practitioners, security administrators, security leads, system analysts, and auditors (Botta et al., 2007). Two significant field studies by the University of British Columbia (UBC) (Botta et al., 2007) and IBM (Haber & Kandogan, 2007) sought to illuminate the practices and challenges of security professionals. In the UBC HOT (Human, Organization, and Technology) Admin project, Botta et al. (2007) interviewed over 30 security
professionals, uncovering that this population is unique from other technical staff.

Necessary skills were categorized into pattern recognition, inferential analysis, bricolage (construction or creation from a diverse range of available things), and communication. Security professionals’ challenges included greater diversity and complexity of tasks, the need to be up-to-date on the latest technologies and vulnerabilities, having to continually promote security, and tradeoffs between security and usability. They also found significant challenges when security professionals had to interact with other stakeholders due to differing risk perceptions, lack of security knowledge and culture, and miscommunications.

Utilizing an ethnographic and ethnomethodological approach, IBM’s Haber and Kandogan (2007) similarly found that security administrators had needs and experiences unique from their non-security counterparts, for example having to address greater technical and organizational complexity and being both proactive and reactive in their work. They found that security tasks are often distributed among multiple team members with varying skill levels, necessitating continual knowledge sharing and collaboration. Additionally, complexity and scale are looming factors in a security administrator’s environment since an attacker only has to find and exploit a single vulnerability in one system while an administrator is responsible for protecting all systems. Failures may be intolerable for typical system administrators (like database administrators), but security administrators make the assumption that any system can be eventually compromised by a determined attacker, so their focus is on detection and cessation of attacks.

Other researchers also used ethnographic approaches to explore work practices of security specializations. Paul (2014) conducted a study of analysts in a network
operations center, finding that communication with external stakeholders was an important, but challenging, aspect of the job. Sundaramurthy et al. (2015) took an anthropological approach to studying security operations center staff, noting a problem of security analyst burnout due to a lack of empowerment, skills, and professional growth opportunities. Goodall, Lutters, and Komlodi (2009) investigated the work practices of network intrusion detection analysts, identifying four core tasks: monitoring, triage, analysis, and response. They noted that socio-technical solutions are necessary to understand analysts’ environments and properly support them in their work.

This body of literature on security professionals’ work practices highlights the complexity of cybersecurity defense. Technical knowledge is important for these professionals, and there is a need to stay up-to-date on the latest security developments. However, there are social and organizational factors also at play, for example having to “sell” security and communicate with stakeholders who do not have the same understanding of security and risk. These non-technical spaces are where cybersecurity advocates most often operate.

2.4.1.2 Education and Professional Development

Various efforts have sought to enumerate and teach necessary skills for security professionals. For example, the NICE Framework outlines the knowledge, skills, and abilities for various cybersecurity work roles (Newhouse et al., 2017). The National Security Agency (NSA) and Department of Homeland Security (DHS) designate schools as National Centers of Academic Excellence in Cyber Defense Education (NSA, 2020) by documenting that their higher education curriculum produces cyber defense professionals who can reduce vulnerabilities in the U.S. national infrastructure. While
comprehensive with respect to technical competencies, many of these resources neglect to include non-technical skills highlighted as important in research studies (Dawson & Thomson, 2018).

By studying women in cybersecurity, Bagchi-Sen, Rao, Upadhyaya, and Chai (2010) identified a gap between the technical training geared towards early career professionals, and the interpersonal, communication, and business-oriented skills required to progress in the field. Dawson and Thomson (2018) acknowledged that current cybersecurity curricula is largely technology-based, but suggested that, to address the interdependencies of cybersecurity with so many organizational and social aspects, the future cybersecurity workforce will need to be proficient in systematic thinking, collaboration, technical social skill, and communication.

Although not cybersecurity specific, other studies echoed these findings by identifying essential skills for related IT and information systems (IS) professions. Huang, Kvasny, Joshi, Trauth, and Mahar (2009) categorized IT job skills into technical, business, and humanistic. Noll and Wilkins (2002) proposed a skills matrix and development model to guide IS curriculum indicating that soft skills, such as teamwork, collaboration, and presentation and writing skills, were important success factors within the field. In an industry survey of over 400 security managers and practitioners, respondents identified “ability to understand the business” and “communication” as the top two most significant gaps they see among today’s cybersecurity professionals (ISACA, 2016).

This body of related work illuminates a need for technical personnel to possess non-technical skills and a void within current security curricula to support these. I have
yet to find prior literature that specifically address the competencies of security professionals whose primary task is the promotion of security practices. This is a gap my research begins to explore by identifying the skills and qualities security advocates should possess.

### 2.4.1.3 Motivations

Past research on professional work motivation provide context for examining the cybersecurity advocate role. Work motivation is “a set of energetic forces that originates both within as well as beyond an individual’s being, to initiate work-related behavior, and to determine its form, direction, intensity and duration” (Pinder, 2014). Motivation is often described in terms of being either intrinsic or extrinsic. Intrinsic motivators arise from an individual’s feelings about a work activity and are inherent within the work itself (Amabile, 1993). These motivators can include interest, enjoyment, or feelings of accomplishment. Conversely, people are extrinsically motivated when they do the work in order to “obtain some goal that is apart from the work itself” (Amabile, 1993). Within the workplace, extrinsic motivators may include recognitions and monetary compensation.

While intrinsic and extrinsic motivators do interact, psychologists have found that intrinsic motivators most positively impact employee performance, creativity, and job retention (Griggs, 2010). In fact, offering excessive extrinsic rewards for work that is already intrinsically rewarding can be detrimental and lead to a decrease in overall motivation.

Work motivations of technology professionals were first explored within IT and IS fields. Based on Shein’s career anchors (1978) (factors that give stability and direction
to a person’s career). Crepeau et al. (1992) identified significant IS worker anchors that included identity, service, and variety. Over 10 years later, Sumner and Yager (2004) perhaps captured the evolving landscape of IT work, finding that the most compelling anchors for IT workers included organizational stability and variety, while identity, competence, creativity, and autonomy were viewed as less important.

Others explored motivation through lenses other than career anchors. Thatcher et al. (2002) revealed that intrinsic motivators positively affected IT workers’ job attitudes and suggested that further research is needed to identify nuances in motivation among different job types. Lounsbury et al. (2007) found that disposition to teamwork and the motivation to achieve were positively related to both job and career satisfaction. Blum (2001) explored gender-specific motivations for entering the computer science field, which is a primary feeder discipline into cybersecurity. She found that for men, computer science was seen as an interesting, fun discipline. Women, however, viewed it more as a means to achieve a socially motivated purpose.

Subsequent studies built upon this work to explore motivators within the much newer cybersecurity field. Chai and Kim (2012) and Bashir et al. (2017) identified security skill self-efficacy as a strong motivator for attraction to cybersecurity careers. Grounded in a literature survey, Dawson and Thomson (2018) suggested that the future cybersecurity workforce should include those with a love of learning, a strong desire to work in teams, and sense of civic duty.

Others focused on retention. Burrell et al.’s (2012) analysis of focus groups of government cybersecurity employees implied that intrinsic motivators are more effective than extrinsic motivators for retention and success in the public sector since government
institutions cannot compete with private-sector salaries. An industry survey (ISC2, 2018) revealed that over 60% of cybersecurity job seekers desire to work in a job where they are empowered and can protect data and people, while roughly half were motivated by salary.

While this literature provides valuable insight, it is unclear as to whether these same motivations apply to cybersecurity advocates. While their jobs possess similarities to those of other cybersecurity and IT workers, advocates play a unique role. For example, like their counterparts they must possess technical expertise, but their main focus is not on technology administration or oversight. They must be skilled in the art of influence but are not technical sales representatives or marketers. My research discovers where advocates’ motivations are similar and where they differ from those performing other cybersecurity roles and how these distinctions might influence advocate recruitment and retention techniques.

2.4.1.4 Diversity

Initial analysis of my in-progress study reveals that cybersecurity advocates come from diverse backgrounds and recognize the importance of non-technical competencies in their work. This analysis needs to be contextualized in an understanding of the landscape of diversity within cybersecurity and efforts at encouraging demographic and discipline diversity. The following provides a high-level overview of this space.

Despite rising numbers of women in STEM fields such as social sciences, mathematics, and engineering, women’s participation in the U.S. computer technology field has been falling (Landivar, 2013). Women now make up only 24% of the overall computing workforce (Accenture, 2016) and only 14% of the North American and 11%
of the global cybersecurity workforce (Frost & Sullivan, 2017). Although Hispanics make up 17% and African-Americans 13% of the U.S. population, they are only 6% and 5% of STEM workers, respectively (National Science Foundation, 2017). Several studies (Gonzalez, 2015; Margolis & Fisher, 2003; Shumba et al., 2013) explored reasons for the underrepresentation of women and minorities within the security field. They found that these populations are often deterred by the perception of security as a “male-dominated, solitary profession with no social benefit” (Shumba et al., 2013, p. 5), a lack of understanding of the breadth of opportunities available in security careers, and the belief that only those with highly technical skills can work in the field. The lack of participation of women and minority populations in the cybersecurity field no doubt contributes to the workforce shortfall.

In addition to demographic diversity, cybersecurity requires discipline diversity, with the security community needing to focus more on “dispelling the misconception that cybersecurity is a purely technical discipline” (Arbuckle, 2018). The cybersecurity field is complex, touching many aspects of society. Therefore, effective cybersecurity requires a multidisciplinary workforce (Hoffman, Burley, & Toregas, 2012) with expertise that extends beyond technical knowledge, for example legal, managerial, business, and human factors. Stockman (2013) infused social sciences into cybersecurity curricula to aid students in developing a more complete picture of security challenges. Lawrence-Fowler (2013) also advocated for a multidisciplinary approach to cybersecurity education, claiming that it improves critical thinking, communication, and encourages alternative perspectives. Exemplar programs that recognize the importance of discipline diversity within the cybersecurity field are the Cyber Scholars Program at University of Maryland,
Baltimore County (2019) and the Advanced Cybersecurity Experience for Students (ACES) at the University of Maryland (2018). These programs offer scholarships and a community of support for undergraduate students from diverse majors via cybersecurity courses and exploration of the relationship between their primary field of study and security.

2.4.2 Security Awareness Professionals

Security awareness professionals are responsible for developing and executing security awareness programs within their own organizations. Several industry organizations and non-profits surveyed security awareness professionals to learn more about their programs, skills, and challenges. The SANS Institute, a popular U.S.-based cybersecurity training organization, conducts an annual security awareness survey that provides insight into the current state of security awareness programs. Key findings in the 2018 report (SANS, 2018) provided insight into the day-to-day work and challenges of these professionals, finding that the majority of respondents perform security awareness duties on a part-time basis with little budget. Many lack sufficient background and soft skills (e.g., communications and marketing) that are needed to effectively engage the workforce and key departmental stakeholders such as the finance and operations departments. Woelk (2015) had similar findings in a report commissioned by the higher education non-profit EDUCAUSE. A survey of 46 professionals was conducted to determine the appropriate qualifications for an effective security awareness professional. The survey revealed that most professionals were only part-time on security awareness tasks, many did not have technical backgrounds, and they viewed soft skills, such as
communication skills and relationship building, as more important than technical skills in their security awareness roles.

Several professional organizations provide resources for security awareness professionals. The International Association of Security Awareness Professionals (2018) holds quarterly meetings, hosts webinars, and provides an online sharing forum for members to ask questions and provide lessons learned. SANS facilitates a Security Awareness community, providing security awareness training courses, an online forum, and other resources to help professionals build and sustain awareness programs within their organizations (SANS, 2019a). The U.S. National Institute of Standards and Technology (NIST) published “Building an Information Technology Security Awareness Program” (Wilson & Hash, 2003) to provide guidance to professionals. NIST also leads the Federal Information Systems Security Educators Association (FISSEA) (2019) which hosts annual conferences and periodic meetings aimed at government security awareness professionals.

While several projects have aimed to discover more about the security awareness professional role, no holistic effort has been made to define its characteristics and practices. In addition, although security awareness professionals are a type of cybersecurity advocate, they are but one manifestation. Deeper exploration into the variety and diversity of advocate roles must be conducted to inform a more accurate definitional boundary.

2.5 Security Mental Models and Perceptions

Before determining the most effective way to persuade people to practice good security, there needs to be an underlying understanding of their perceptions of security.
Numerous studies have explored these perceptions, mostly among non-technical users. Huang et al. (2007) conducted a survey of over 600 individuals that revealed factors that influence security perceptions, including knowledge, impact, controllability, and awareness of exposure to a threat. Furnell and Thomson (2009) and Stanton et al. (2016) discussed “security fatigue,” a weariness towards security when it becomes too burdensome. Herley (2009) claimed that users ignore security advice because they are overwhelmed by the sheer volume of advice and because they perceive security actions to be moot in the face of myriad threats. Pfleeger and Caputo (2012) described impacts of human cognition on security behaviors, (e.g., cognitive load, biases, and framing effects) and how addressing those might lead to more success in mitigating cyber risk. West, Mayhorn, Hardee, and Mendel (2008) focused on why users make poor security decisions, suggesting that the tendency to satisfice, cognitive biases, time pressures, and inattentional blindness contribute to this phenomenon. From an organizational perspective, Post and Kagan (2007) found that employees view stringent security measures as counterproductive since it impedes their ability to be flexible in their day-to-day operations.

A set of researchers explored mental models of security, with some examining the general public’s often incomplete and inaccurate mental models and how these perpetuate poor security practices, for example: Prettyman, Furman, Theofanos, and Stanton (2015); Kang, Dabbish, Fruchter, and Kiesler (2015); and Wash (2010). Other researchers shed light on the differences in mental models of security experts and nonexperts, e.g., Ion, Reeder, and Consolvo (2015) and Posey, Roberts, Lowry, and Hightower (2014). Bravo-Lillo, Cranor, Downs, and Komanduri (2011) and Raja, Hawkey, Hsu, Wang, and
Beznosov (2011) examined mental models while applying risk communication principles to security warnings. Camp (2009) discussed how mental models of physical security, medical infections, criminal behavior, economics failure, and warfare might be applied to communicate cybersecurity risk. Zhang-Kennedy, Chiasson, and Biddle (2014) extended these models, suggesting that the use of surveillance and medical metaphors within infographics and a comic resulted in better security learning. However, Brase, Vasserman, and Hsu (2017) investigated the impact of Camp’s suggested models in cybersecurity situations and found that there was little indication that any of these resulted in significantly better outcomes.

2.6 Economics of Cybersecurity

After years of conducting research on the economics of cybersecurity, Anderson and Moore observed that “security failure is caused at least as often by bad incentives as by bad design.” (2007, p. 68). The economics of cybersecurity research area encompasses a variety of topics, including cost-benefit trade-offs; strategies, behaviors, and benefits of market participants; market analysis; economics of cybercrime; and economic impact of cyber regulations (Jentzsh, 2016). This section focuses on how economic incentives (or lack thereof) can influence the security adoption of organizations. Influences on individuals’ security decision making are discussed in a subsequent section.

Moore and Anderson (2011) describe three categories of economic barriers facing cybersecurity: misaligned incentives, asymmetric information, and externalities. Misaligned incentives are disparities between what the motivations of those who are responsible for security and those who benefit from security. For example, financial institutions promote online banking in order to save in operating costs, but this transfers
partial risk to their customers who would like to protect their privacy and account information. Jentzsch (2016) surveyed cybersecurity economics literature and suggested the need for more evidence-based incentives advice grounded in an understanding of consumer behavior.

The asymmetric information barrier refers to unreliable or incomplete security data, sometimes manifested as an overrepresentation or underrepresentation of risk. Under-reporting of security incidents cripples the community in being able to properly evaluate risk, while over-inflating risk metrics erodes trust. Difficulties in calculating the value of security and determining the appropriate level of investment also interfere. As a preventive technology, security successes are often not measurable or observable, so organizations may have a hard time justifying investment (Gordon et al., 2018). In addition, cost savings are less tangible than earnings. Moore, Dynes, and Chang (2015) interviewed 40 Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) from multiple sectors and found that “few CISOs view security spending as an opportunity to reduce costs for the firm.” Several efforts attempted to provide guidance to provide better data. For example, Gordon and Loeb (2002) proposed a model to determine optimal investment to protect a set of information. They suggest that an organization should only invest a small fraction of expected security breach loss in order to maximize investment benefit. In a Tenable Network Security white paper (2016), industry experts suggested that risk-cost awareness helps leadership make financial decisions about where to invest in security, so security metrics presented to executives should be associated with the “price tag” of a risk. Based on their findings, Moore,
Dynes, and Chang (2015) recommended an emphasis on security process measures rather than outcome measures (e.g., return on investment) when making budgeting decisions.

Finally, externalities are cases in which security actions have side effects. A tendency to rely on others who are perceived as being security-conscious discourages investment in one’s own security. Vendors may have little incentive to invest in creating secure software due to time-to-market pressures and customers valuing visible features over invisible security mechanisms. In addition, with some security technologies, the cost may be greater than the benefit until adoption reaches critical mass. For example, this is the case today with secure internet protocols such as the Domain Name System Security Extensions (DNNSEC) that have been slow in adoption because they require others to also adopt them before experiencing full benefit. Herley (2009) examined externalities from the perspective of individual users. He claimed that people’s rejection of security advice “is entirely rational from an economic perspective” because of the burden of effort required to take action.

Several papers provided recommendations to overcome externalities. Kunreuther and Heal (2003) developed a model to describe this interdependence and examined the roles of incentives, such as inspections, subsidies, fines, and regulations in overcoming this challenge. Jentzsch (2016) suggested more research into understanding the interconnected risks of security incidents. Security should also be framed as a business enabler and competitive advantage in a marketplace that is becoming increasingly cognizant of the consequences of insecure products (Tenable Network Security, 2016; Gordon et al., 2018). Herley (2009) suggested five general directions to make security advice more compelling to users: 1) gain a better understanding of actual harms and
victimization rates when crafting advice; 2) ensure the cost of recommended action is proportional to the victimization rate (do not focus on advice to protect against rare exploits); 3) discontinue older, overly burdensome advice that does not address current harms users face; 4) prioritize advice; and 5) respect users’ time and effort.

2.7 Persuasion Techniques in Cybersecurity

Protection Motivation Theory (PMT) (Maddux & Rogers, 1983; Rogers, 1983) claims that risk behavior is based on a cost-benefit analysis in which a threat appraisal (severity, likelihood, rewards/consequences) is weighed against a coping appraisal (response cost, effectiveness of response, self-efficacy). Sommestad, Karlzen, and Hallberg (2015) sought to determine whether the PMT held true in the information security domain and found that it did explain security behavior if the threat and coping mechanism were concrete and when the threat was personally relatable.

Several studies applied PMT to explore the effectiveness of fear appeals in changing security behaviors within organizations. Johnston and Warkentin (2010) suggested that, because people naively think that bad things will not happen to them, fear appeals should emphasize the likelihood of an occurrence by using concrete examples of negative consequences related to a threat. Herath and Rao (2009) found that both intrinsic (perceived effectiveness, contribution to the greater good) and extrinsic (social pressures, penalties) motivators influenced security behaviors. However, the severity of penalty approach had negative impact because penalties are often inconsistently applied or may generate hostilities.

Additional efforts investigated approaches for influencing security behavior change among employees. Albrechtsen and Hovden (2010) found that small group
workshops were more effective at changing security behaviors than mass communications. Siponen (2000) suggested that security awareness programs should include reasons for why people should follow security guidelines and engender feelings of wellbeing, rationality, and logic. Other efforts examined similar techniques from a home user perspective. Rhee, Kim and Ryu (2009) discovered that the threat of negative consequences has limited impact on decisions to implement security, whereas users with higher feelings of security self-efficacy were more likely to engage in positive behaviors. In a study on the adoption of security technologies, Shropshire, Warkentin, and Johnston (2010) found that negative framing (presenting outcomes in loss terms) is better suited for detection technologies (e.g., virus scanners, firewalls) than for prevention technologies (e.g., password settings, access controls). Redmiles, Malone, and Mazurek (2016) investigated why people choose to accept security advice, discovering that advice sources were evaluated based on perceived trustworthiness, and that fictional narratives with relatable characters may be effective for teaching security concepts.

Although much literature has focused on persuasion in security, little research examined this topic from the viewpoint of those attempting to do the persuading and if their techniques match purported best practices. My dissertation seeks to understand their expert craft and how they appropriate these techniques and innovate on others to respond to their particular context at hand. Ultimately this will reveal the art of effective security advocacy.

2.8 Advocacy in Other Domains

There is also an opportunity to compare and learn from advocacy techniques in non-cybersecurity fields, especially those with longer histories and hard-fought successes, for
example, environmental advocacy (Searles, 2010) (Jurin, Roush, & Danter, 2010). In particular, health advocacy may be a particularly relevant domain against given that this connection is often employed when describing cybersecurity concepts to non-experts (Camp, 2009)(Charney, 2012). Nutbeam (2000) and Sørensen et al. (2012) discussed advocacy in the context of public health education and promotion, empowerment, facilitation of health literacy, and social determinants of health, all of which are relevant within the cybersecurity realm. Kelland et al. (2014) interviewed advocates within the physiotherapy profession and found eight attributes of successful advocates: collaboration, communication, scholarly practice, management, professionalism, passion, perseverance, and humility.

Like cybersecurity, health concerns are wide-spread and have both personal and institutional consequences (Bassett, 2003). However, others, including Weber (2017), caution that health metaphors may be flawed since public health differs from cybersecurity in two important areas: 1) cybersecurity is conceptually seen as consisting of “public” goods or goals versus the more personal nature of public health concerns, and 2) contrasted with the long public health policy history and acceptance of such, there is a lack of “readiness of the relevant actors and institutions to exert and accept coercive authority” (p. 173) with respect to cybersecurity. One of the goals of my research is to further identify differences and determine if, why, and how cybersecurity advocates skills and techniques should deviate from those of advocates in other fields.

2.9 Addressing Research Gaps

The prior literature discussed in this section forms the foundation for my research but reveals that little has been applied to the role of cybersecurity advocates, or sometimes
even within the cybersecurity context at all. The following synthesizes the research topics described above as applied to cybersecurity advocacy and summarizes the current research gaps my dissertation hopes to fill.

Cybersecurity advocates bear similarities to various roles detailed in past literature, including risk communicator, change agent, and advocate. These roles aim to educate, persuade, and facilitate positive behavior change and the adoption of measures meant to benefit individuals and society as a whole. Decades of risk communication literature reveal that effective risk communication is a non-trivial undertaking, necessitating that risk communicators have a keen understanding of their audience, strong translation skills, and the ability to negotiate controversial topics. Advocates working in a multitude of disciplines, including health and public safety, often take on the risk communicator role, aiming to highlight and offer mitigations to potentially harmful situations. Change agents advocate for the adoption of a technology or practice, but first must establish a need. In the case of cybersecurity, a need for protection is created by convincing people about the risk of cyber attack or loss of information. However, a gap exists in that there is currently little understanding of advocacy, technology adoption, or risk communication from the perspective of the advocate, change agent, or risk communicator within the cybersecurity field. There are also questions as to whether there are inherent aspects of the cybersecurity field that require different approaches.

From a more contemporary literature perspective, the evolving understanding of people’s security mental models, the economics of cybersecurity, and which persuasion techniques have been found to be effective in cybersecurity help to shape a picture of effective risk communication and advocacy in cybersecurity. But there is little empirical
evidence that advocates are actually following recommended practices. If they aren’t, what are they doing instead, and are these other methods effective? My research hopes to address this hole in our collective knowledge.

Research within the last decade has also investigated the practices, motivations, and skills of security professionals and forms an initial understanding of those working in cybersecurity professions. This body of literature highlights the complexity of cybersecurity jobs, suggesting that technical knowledge is foundational for security professionals, but there are contextual, social, and organizational factors also at play in security adoption and behavior change. These non-technical spaces are where cybersecurity advocates most often operate. However, there has been no prior work to document the skills and attributes specific to the cybersecurity advocate role and how these skills may differ from those of other traditional security professionals. My research is the first to define and enumerate competencies for this role.
3 Study Design and Methodology

This chapter describes the study design and methodology of an interview study and a case study. Each research study looks at cybersecurity advocacy through a different lens: what advocates say they do and what they actually do in practice.

3.1 Interviews of Cybersecurity Advocates

The first part of my research was an interview study meant to gain an initial sense of cybersecurity advocates’ motivations, characteristics, and skills (RQ1), techniques (RQ2), rewards and challenges (RQ3), and sources of security information (RQ4) from the perspective of the advocates themselves. The UMBC institutional review board approved the study (IRB Protocol Y17WL12070).

Between November 2016 and August 2017, I conducted semi-structured interviews of 28 individuals performing security advocacy tasks as a major component of their jobs. I chose semi-structured interviews over other methods, such as surveys, because of the richness of data afforded by interviews, the latitude to ask follow-up questions to clarify or delve deeper into participant responses, and the ability to encourage participants to add other relevant information not explicitly asked in the interview protocol (Corbin & Strauss, 2015).

The interview study was an example of fundamental qualitative descriptive study, which has a goal of “a comprehensive summary of events [phenomena] in the everyday terms of those events” (Sandelowski, 2000). Qualitative description is especially useful when attempting to answer research questions of particular concern to practitioners (Sandelowski, 2000). Although qualitative description was the primary method, as with many qualitative studies, I drew on approaches from other methods as appropriate. Data
collection and analysis was informed by Grounded Theory qualitative methods (Glaser & Strauss, 2009). Although my research was not aimed at generating new theory, I chose to follow aspects of this approach for several reasons: 1) Concepts are derived directly from the data and not from *a priori* assumptions from prior work. This is appropriate for my research since cybersecurity advocacy is a new and emerging research area. Although foundations, such as risk communication and change agentry, do exist, there is not enough evidence to support cybersecurity advocacy mapping neatly to previously discovered frameworks or theories. 2) Data collection and analysis are tightly coupled and usually happen in parallel, with analysis of data informing subsequent data collection decisions. Since a goal of my research is to define the role of cybersecurity advocate, I have to constantly adapt my own understanding by being open to where the data leads me and being able to adjust data collection as needed to accommodate unanticipated findings. 3) Grounded Theory allows for a deep examination of different perspectives, underlying beliefs and actions, and the impact of emotion and logic on behaviors (Corbin & Strauss, 2015). Cybersecurity, although frequently viewed as a purely technical field, is influenced by myriad individual, social, and organizational factors. Advocacy within this space can be complex, nuanced, and messy, which necessitates exploration through multiple lenses.

3.1.1 Sampling and Recruitment

I selected information-rich cases (Patton, 2015) by recruiting a purposeful sample of participants based on their roles as cybersecurity advocates. My conceptualization of an advocate originated from my own experience in the cybersecurity field and how this group of professionals described their roles. Therefore, I initially recruited those who
publicly self-identified as security advocates in some manner, and then was open to snowballing recommendations that allowed interviewees to identify others like themselves.

I also employed theoretical sampling throughout data collection to guide recruitment (Corbin & Strauss, 2015). As the definitional boundary of the cybersecurity advocate role continued to take shape as the interviews progressed, it influenced subsequent recruitment decisions. Following this approach, I recruited participants four or five at a time. The next group of potential participants was then purposely chosen to include those who might be able to provide more insight on concepts or areas of interest emerging from the analysis of the preceding set. For example, when several male participants discussed the need for greater gender diversity within the security field, I subsequently made an effort to recruit additional female participants to gain their perspectives.

In addition to theoretical sampling, to ensure that a broad range of security advocacy roles would be included in the study, I also purposefully selected individuals who performed different types of security advocacy, for example, security awareness training, public campaigns, advocacy for a particular community, or security consultation. Additionally, I sampled advocates working in a variety of organizational types, including government, industry, higher education, and non-profits, to account for different viewpoints that may be inherent in each of these sectors.

I identified specific potential participants in several different ways. Eight participants were personal contacts or advocates I had specific knowledge of from working in the security field for over 20 years. Three were recommended by professional
contacts not participating in the study, and six were snowballing recommendations from interview participants. Eleven participants were found via internet searches e.g., cybersecurity award winners, points of contact at security advocacy groups, speakers at security awareness conferences. An invitation to contribute to the study was sent to each potential participant via email.

3.1.2 Participant Demographics

I interviewed 10 female and 18 male professionals, clustered in age from 25-34 (3 participants), 35-44 (7), 45-54 (7), and 55+ (10), with one undisclosed. Overall, they were a veteran group, with all but six having more than 10 years of experience in the security field, and the rest having at least five years. Table 1 summarizes participant demographics. Some details are generalized to protect confidentiality.

The participants had diverse educational and career backgrounds. Interestingly, 14 participants had at least one degree in a non-technical field, with 11 only having degrees in areas such as public policy, communication, history, law, business, English, and graphic design. Participants had worked in a variety of government, private industry, higher education, and non-profit organizations, with most having experience in more than one of these sectors. When asked to describe their target audience, 9 said their audience was mainly external to their organization, five mainly focus within their organization, and 14 said they advocate both externally and internally. Their diverse audiences included the general public, co-workers, professional communities, government organizations, students and faculty, policy makers, corporate boards, developers, and other security professionals. The advocates performed a number of roles, several having more than one. Some were security engineers, led organizational security awareness programs, or served
as security consultants. Others were security educators, non-profit organizers, researchers, or secure development experts.
Table 1

**Participant Demographics**

<table>
<thead>
<tr>
<th>ID</th>
<th>Current Role</th>
<th>Gen</th>
<th>Age</th>
<th>Ed</th>
<th>Degree Area(s)</th>
<th>Sector</th>
<th>Audience Type</th>
<th>Audience Description</th>
<th>Advocacy Role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Security analyst</td>
<td>M</td>
<td>55+</td>
<td>M</td>
<td>business and management, information security</td>
<td>G</td>
<td>B</td>
<td>tech staff, managers</td>
<td>Recommends security mitigation strategies to government organizations after a vulnerability assessment or cyber intrusion; promotes professional development of security professionals at a government organization</td>
</tr>
<tr>
<td>P02</td>
<td>Professor</td>
<td>M</td>
<td>35-44</td>
<td>P</td>
<td>national security policy and foreign affairs, internet studies</td>
<td>E,G,I</td>
<td>B</td>
<td>general public, students</td>
<td>Led cybersecurity programs as a chief security officer at organization; Currently teaches cybersecurity at a university; serves as a subject matter expert for media inquiries</td>
</tr>
<tr>
<td>P03</td>
<td>Computer scientist</td>
<td>F</td>
<td>55+</td>
<td>M</td>
<td>computer science</td>
<td>G,I</td>
<td>B</td>
<td>tech staff, managers, general public</td>
<td>Researches and promotes usable security at a government organization</td>
</tr>
<tr>
<td>P04</td>
<td>Security evangelist</td>
<td>M</td>
<td>55+</td>
<td>M</td>
<td>mathematics, computer science</td>
<td>N,G</td>
<td>B</td>
<td>tech staff, managers</td>
<td>Runs volunteer projects for a non-profit that develops, sustains, and promotes best practices in cybersecurity</td>
</tr>
<tr>
<td>P05</td>
<td>Security researcher</td>
<td>M</td>
<td>55+</td>
<td>B</td>
<td>computer science</td>
<td>I,G</td>
<td>B</td>
<td>tech staff, managers</td>
<td>Conducted vulnerability assessments and worked with government organizations to understand threats and mitigate security vulnerabilities; conducts research on and promotes security automation</td>
</tr>
<tr>
<td>ID</td>
<td>Current Role</td>
<td>Gen</td>
<td>Age</td>
<td>Ed</td>
<td>Degree Area(s)</td>
<td>Sector</td>
<td>Aud Type</td>
<td>Audience Description</td>
<td>Advocacy Role(s)</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------</td>
<td>-----</td>
<td>------</td>
<td>----</td>
<td>--------------------</td>
<td>--------</td>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>P06</td>
<td>Non-profit director</td>
<td>M</td>
<td>55+</td>
<td>P</td>
<td>communication theory</td>
<td>N,G,E,I</td>
<td>B</td>
<td>public policy makers, managers</td>
<td>Leads a security non-profit with a goal of influencing public policy</td>
</tr>
<tr>
<td>P07</td>
<td>Senior technologist, professor</td>
<td>F</td>
<td>45-54</td>
<td>P</td>
<td>computer science, engineering</td>
<td>G,E,I</td>
<td>E</td>
<td>general public, managers, students</td>
<td>Promotes and teaches usable security; advises government organization leadership on technology issues; provides public speaking and outreach</td>
</tr>
<tr>
<td>P08</td>
<td>Security consultant, attorney</td>
<td>M</td>
<td>45-54</td>
<td>J</td>
<td>English, history, law</td>
<td>I</td>
<td>E</td>
<td>non-tech professionals, managers</td>
<td>Teaches security topics to non-technical audiences</td>
</tr>
<tr>
<td>P09</td>
<td>Security awareness training director</td>
<td>M</td>
<td>45-54</td>
<td>M</td>
<td>history, business</td>
<td>E,G</td>
<td>E</td>
<td>tech staff</td>
<td>Manages a security awareness community; designs and teaches associated educational curriculum</td>
</tr>
<tr>
<td>P10</td>
<td>Instructor, consultant</td>
<td>M</td>
<td>45-54</td>
<td>M</td>
<td>engineering</td>
<td>I,E,G</td>
<td>E</td>
<td>tech staff, managers</td>
<td>Designs and teaches security courses; conducts penetration testing and serves as a security consultant to organizations</td>
</tr>
<tr>
<td>P11</td>
<td>Non-profit director</td>
<td>M</td>
<td>35-44</td>
<td>B</td>
<td>philosophy</td>
<td>N,I</td>
<td>E</td>
<td>public policy makers, tech staff, managers</td>
<td>Leads a security non-profit; works to influence sector-specific and public security policy</td>
</tr>
<tr>
<td>P12</td>
<td>Security engineer, instructor</td>
<td>M</td>
<td>35-44</td>
<td>M</td>
<td>IT</td>
<td>I,E,G</td>
<td>E</td>
<td>tech staff, managers, students</td>
<td>Provides security engineering and consulting support to organizations; teaches security courses at a university</td>
</tr>
<tr>
<td>P13</td>
<td>Security engineer</td>
<td>M</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>I</td>
<td>I</td>
<td>tech staff, managers</td>
<td>Conducts organization’s incident response and handling; implements and creates security policies; consults with other organization teams about security issues</td>
</tr>
<tr>
<td>ID</td>
<td>Current Role</td>
<td>Gen</td>
<td>Age</td>
<td>Ed</td>
<td>Degree Area(s)</td>
<td>Sector</td>
<td>Audience Type</td>
<td>Audience Description</td>
<td>Advocacy Role(s)</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------</td>
<td>-----</td>
<td>-------</td>
<td>----</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>P14</td>
<td>Security awareness director</td>
<td>M</td>
<td>35-44</td>
<td>J</td>
<td>policy, law, business</td>
<td>E,G</td>
<td>I</td>
<td>students, faculty, tech staff, managers</td>
<td>Leads security awareness program at a university</td>
</tr>
<tr>
<td>P15</td>
<td>Non-profit director</td>
<td>F</td>
<td>35-44</td>
<td>J</td>
<td>international relations, economics,</td>
<td>N,E,I</td>
<td>B</td>
<td>tech staff, managers</td>
<td>Runs cybersecurity outreach program for non-profit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Russian, law</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P16</td>
<td>Computer scientist</td>
<td>M</td>
<td>45-54</td>
<td>P</td>
<td>chemistry, political science,</td>
<td>G,E,I</td>
<td>B</td>
<td>researchers, managers</td>
<td>Conducts research and development on techniques to prevent the disclosure of</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>journalism, computer science</td>
<td></td>
<td></td>
<td></td>
<td>confidential information at a government organization; promotes usable security</td>
</tr>
<tr>
<td>P17</td>
<td>Researcher</td>
<td>M</td>
<td>45-54</td>
<td>M</td>
<td>computer science</td>
<td>I</td>
<td>E</td>
<td>developers, tech staff</td>
<td>Researches, writes about, and consults with organizations about devops</td>
</tr>
<tr>
<td>P18</td>
<td>CIO</td>
<td>M</td>
<td>55+</td>
<td>M</td>
<td>mathematics, computer science,</td>
<td>E</td>
<td>I</td>
<td>students, faculty, tech staff, managers</td>
<td>Leads technology and cybersecurity activities at a university</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>operations analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P19</td>
<td>Senior architect</td>
<td>F</td>
<td>55+</td>
<td>M</td>
<td>computer science</td>
<td>I</td>
<td>I</td>
<td>developers</td>
<td>Promotes secure development practices and leads organization’s security compliance activities</td>
</tr>
<tr>
<td>P20</td>
<td>Professor</td>
<td>M</td>
<td>55+</td>
<td>P</td>
<td>computer science, engineering</td>
<td>E,G</td>
<td>B</td>
<td>students, tech staff, managers</td>
<td>Teaches cybersecurity courses; promotes security best practices to the critical infrastructure community</td>
</tr>
<tr>
<td>P21</td>
<td>Company co-founder, former</td>
<td>F</td>
<td>25-34</td>
<td>B</td>
<td>computer science</td>
<td>I,G</td>
<td>E</td>
<td>end users, tech staff, managers</td>
<td>Led a security awareness program at an organization;</td>
</tr>
<tr>
<td>ID</td>
<td>Current Role</td>
<td>Gen</td>
<td>Age</td>
<td>Ed</td>
<td>Degree Area(s)</td>
<td>Sector</td>
<td>Aud Type</td>
<td>Audience Description</td>
<td>Advocacy Role(s)</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------</td>
<td>-----</td>
<td>------</td>
<td>----</td>
<td>--------------------------</td>
<td>-------------</td>
<td>----------</td>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>P22</td>
<td>Security researcher</td>
<td>M</td>
<td>35-44</td>
<td>P</td>
<td>electronics, computer engineering</td>
<td>I, E</td>
<td>B</td>
<td>developers</td>
<td>Promotes and teaches secure development lifecycle practices; addresses security governance issues within the organization</td>
</tr>
<tr>
<td>P23</td>
<td>Security consultant</td>
<td>F</td>
<td>25-34</td>
<td>U</td>
<td>art history, French, history</td>
<td>I, E</td>
<td>B</td>
<td>tech staff, general public</td>
<td>Consults with organization about security communications; conducts security awareness training for general public audiences</td>
</tr>
<tr>
<td>P24</td>
<td>Non-profit director</td>
<td>F</td>
<td>25-34</td>
<td>M</td>
<td>international studies</td>
<td>N</td>
<td>E</td>
<td>general public, tech staff, managers</td>
<td>Leads cybersecurity campaigns and initiatives at a non-profit</td>
</tr>
<tr>
<td>P25</td>
<td>Deputy CIO</td>
<td>F</td>
<td>35-44</td>
<td>B</td>
<td>social and decision science</td>
<td>G, I</td>
<td>B</td>
<td>end users, tech staff, managers</td>
<td>Consulted with organizations about security vulnerabilities and mitigations; manages technology and security programs for a government organization</td>
</tr>
<tr>
<td>P26</td>
<td>CISO</td>
<td>F</td>
<td>45-54</td>
<td>M</td>
<td>computer science</td>
<td>G, I</td>
<td>B</td>
<td>end users, tech staff, industry partners</td>
<td>Leads cybersecurity awareness programs for a local government</td>
</tr>
<tr>
<td>P27</td>
<td>Non-profit director</td>
<td>M</td>
<td>55+</td>
<td>B</td>
<td>French, Spanish</td>
<td>N, I</td>
<td>B</td>
<td>tech staff, managers</td>
<td>Leads cybersecurity research, consulting, and collaboration activities for a non-profit</td>
</tr>
<tr>
<td>P28</td>
<td>Security awareness director</td>
<td>F</td>
<td>55+</td>
<td>A</td>
<td>marketing, graphic design</td>
<td>I, E</td>
<td>I</td>
<td>end users, tech staff, managers</td>
<td>Leads security awareness program at an organization</td>
</tr>
</tbody>
</table>

**Gen (Gender):** A=Associate’s degree, B=Bachelor’s degree, M=Master’s degree, P=Ph.D, J=J.D., U=Unknown; **Sector (Current, Past):** E=Education, G=Government, I=Industry, N=Non-profit; **Aud (Audience) Type:** I=Internal to own organization, E=External to own organization, B=Both internal and external
3.1.3 Data Collection

I conducted 28 semi-structured interviews lasting on average 45 minutes. If logistically feasible, interviews were face-to-face (12 interviews). Otherwise, participants were given the option of a phone (9) or video conference (7) interview. Prior to the interviews, I informed participants of the purpose of the study and how their data would be used and protected. Participants then signed a consent-to-participate form, also indicating whether they would allow audio recording of the interview (two declined). Data were stored without personal identifiers, rather with a participant code like P10. Interviewees were not compensated for participation.

The first three interviews were pilots to ensure the questions were understandable and to discover potential flow and timing issues. Because there were only minor revisions to the protocol following, data from these interviews are included in the final data set. In line with accepted qualitative research methods, I interviewed until reaching theoretical saturation, the point at which no new themes or ideas emerged from the data (Merriam & Tisdell, 2016).

Interview questions addressed several areas: work practices and approaches, professional motivations and challenges, characteristics of successful advocacy, and how participants stay up-to-date on security happenings. The interview protocol, with each question mapped to the research questions, is included in Appendix A. Separate from the interview, participants also completed a short, online demographic survey (Appendix B) that collected information about years of experience in the field, current position, sectors in which they had worked, and education. One participant did not complete the survey.

Although audio recording was preferred, it was not a mandatory requirement of the interviews. Two participants opted not to have their interviews recorded. In those cases,
detailed notes were taken during the interviews. All interviews were transcribed from the audio recordings and field notes.

3.1.4 Analysis

Iterative, inductive coding and analysis was conducted on the data with my advisor. This commonly used qualitative research approach allows for an organic emergence of core concepts, starting with the categorization of the data into initial codes and then progressing to the recognition of relationships among those codes (Glaser & Strauss, 2009). Preliminary analysis was begun at the onset of data collection to assess the quality of data and themes arising from the interviews. This allowed for small adjustments in the interview protocol over time as some questions reached saturation or when new themes started to arise as part of theoretical sampling. Throughout this process, we also engaged in axial coding to link related codes, writing analytic memos, and identifying core concepts. We met regularly to discuss emerging themes and our interpretations.

At the conclusion of data collection, we constructed a final codebook. We reviewed five interviews (2,482 lines) individually and performed open coding to label, look for meaning, and begin to categorize the data. We then met multiple times to discuss identified concepts in those interviews. These discussions led to the development of the codebook (Appendix C). I then used the codebook to deductively code the remaining interviews.

3.1.5 Study Design Tradeoffs

The interview study has several methodological tradeoffs. The study is a one-sided view through the eyes of security advocates themselves and does not provide empirical evidence that any of the techniques deemed successful by the participants were indeed
effective with the intended audiences. Rather, participant responses were based on their own professional experience and empirical understanding. In addition, interviews may suffer from self-report or social desirability bias in which participants may adjust their answers to appear more acceptable to the researcher, especially since I revealed my background as a security practitioner prior to the interviews. However, since this study is a first attempt at gathering information about cybersecurity advocates, it makes sense to start with talking to those who perform the job, then conduct follow-on efforts to validate findings.

There may also be a self-selection bias among participants. Those who were willing to participate may be more passionate about their roles than those who declined. Since all but one participant were based in the United States, there is also the possibility of a cultural bias. Cybersecurity advocates in other countries may have different characteristics, so my results may not be widely transferrable outside the U.S.

3.2 Case Study: Cybersecurity Advocacy in Practice

The interview study began to form a picture of the work of cybersecurity advocates by identifying what advocates say they do. A follow-on, in-depth, longitudinal case study provided a better understanding of what advocates actually do in practice (RQ2) and which advocate approaches were perceived as being effective in influencing clients’ security decisions and behaviors (RQ5). More detail on the value of the chosen case study in complementing the interview study is discussed in Chapter 9 Study Synthesis.
In addition to working towards the requirements of a doctoral degree at UMBC, the case study was conducted as part of my official work duties at NIST\(^2\). The study was reviewed and approved by both the UMBC IRB (Protocol Y17WL12070) and NIST IRB (Protocol ITL-2018-0119) as exempt human subjects research.

3.2.1 Selection of Case Study Method

A case study is a clearly scoped and bounded “investigation and analysis of a single or collective case, intended to capture the complexity of the object of study” (Hyett, Kenny, & Dickson-Swift, 2014) and involves the use of multiple data collection and analysis methods (Flyvbjerg, 2006; Baxter & Jack, 2008). The collection of evidence from multiple sources allows for triangulation to strengthen interpretations (Yin, 1999). The case is also explored through multiple lenses, which allows for nuanced facets to be revealed (Baxter & Jack, 2008).

Case study research is particularly suited to the goals of this follow-on research effort since it attempts to confirm the wider view of advocacy gained in the interviews through a more holistic understanding of cybersecurity advocacy in great detail (Noor, 2008). In my research, the case study is manifested as an “instrumental case study” (Stake, 2003) in which the particular case provides insight into a generalization. In this case, the generalization consists of the interview study findings, with the case study having a supportive role in understanding the cybersecurity advocate role.

The case study examined one kind of cybersecurity advocate, security awareness professionals, within a real-world, observable setting. The subject of the case study was

\(^2\) Any mention of commercial products or reference to commercial organizations in this document is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.
the security awareness team and program at a medium-sized U.S. federal government agency (referred to as Agency A). Security awareness professionals were chosen as an instantiation of cybersecurity advocates for several reasons. Four security awareness professionals were interviewed in the first study, thus providing a basis for a clear job description and organizational mission. Security awareness programs also provide a bounded case within an organization with a defined team and audience with which to engage. In addition, security awareness efforts offered an opportunity to observe live events and employee reactions. A single case study, versus multiple case studies, was chosen in order to avoid confounding variables that might be introduced by different organizational contexts. Examining just one instantiation also allowed for much richer, longitudinal investigation rather than multiple, superficial snapshots.

As with the interview study, I also took a qualitative descriptive approach during data collection and analysis (Sandelowski, 2000) that incorporated elements of Ground Theory and ethnography. This approach supported my primary goal of providing a comprehensive description of the advocacy/security awareness function within Agency A.

3.2.2 Selection of Organization

A U.S. federal government agency was chosen as the object of the case study for several reasons. First, as a federal employee representing a government agency, my studying other government agencies was less administratively cumbersome, for example, obviating the need for the lengthy U.S. Government Paperwork Reduction Act\(^3\) approval required for NIST studies involving non-federal employees. Second, there is a tendency

of federal agencies to accept and trust the ethical research standards employed by other agencies. Third, government agencies are a less-studied population, often due to access problems, which offered a unique glimpse into this domain. Lastly, due to a preponderance of federal cybersecurity mandates, government agencies tend to be compliance-oriented organizations, offering an opportunity to explore how an agency balances security awareness compliance pressure with achieving actual impact.

Agency A was specifically chosen for a number of practical reasons. There was an existing relationship between NIST and Agency A based on staff participation in previous security awareness events at both agencies. Convenience also played a large role in Agency A’s selection: my NIST identification badge also granted access to Agency A buildings; Agency A was located within a reasonable driving distance to NIST, which allowed for frequent visits; and, unlike some government agencies, Agency A allowed audio recording in spaces designated for the interviews. With respect to security awareness program attributes, Agency A had a varied security awareness program that included in-person events, classroom and online training, campaigns, which afforded a more interesting case. In addition, although the majority of Agency A’s employees were located at their headquarters, regional offices provided an opportunity to examine remote outreach efforts. Finally, Agency A’s security awareness team and leadership were enthusiastic and receptive to participating in the case study when asked.

The Agency A CIO provided a signed letter in support of the agency’s participation in the case study. Permission was also obtained from the Agency A Contracting Officer Representative (COR) to interview the two contractors on the security awareness team. Because of the sensitivity of Agency A’s mission, Agency A was assured that researchers
would protect the confidentiality of both the organization and personnel. Data is, therefore, reported in aggregate with no personal identifiers or information that could uniquely identify Agency A. In addition, it was agreed that Agency A would be provided a draft of any case study paper meant for public dissemination (including this dissertation) so that they could review and determine factual accuracy and if their confidentiality was adequately protected before publishing. However, the agency was not permitted censorship of results. Ultimately, this agreement allowed uniquely deep and robust access to an understudied organization type.

3.2.3 Data Collection

Data collection for the case study was conducted over the course of one year between December 2018 and December 2019. The majority of on-site collection (interviews) occurred during the first half of that timeframe, with additional follow-up conversations with security awareness team members to clarify and further explore emerging themes taking place through the end of 2019. Events were attended throughout the year.

The study allowed for examination of cybersecurity advocacy from several perspectives within the security awareness context via a multi-methods approach involving:

- **Interviews of security awareness team members** to understand their work practices, approaches, motivations, and challenges
- **Interviews of managers** in the security awareness team’s chain-of-command to understand their vision and views of the security awareness program and how internal security awareness priorities and resources were determined
• **Interviews of employees** who have consumed agency security awareness information to explore their opinions of the security awareness program and which awareness/education techniques they feel were most impactful in shaping their security behaviors

• **Field observations of security awareness events** to document advocacy in action

• **Collection and review of security awareness documents** (pamphlets, posters, post-event reports, and employee feedback surveys) to determine which advocacy techniques were used and examine how markers of success were determined by the security awareness team

Data was collected via 14 on-site Agency A visits (meetings with the team, interviews, and field observations), eight email exchanges (document collection and answering emerging questions), and two phone conversations (answering emerging questions), totaling approximately 28 hours in the field. This section describes sampling and data collection methodology for all aspects of the case study.

3.2.3.1 *Case Study Interviews*

The security awareness team consists of the program lead (security awareness lead) (a federal employee) and two contractors. Demographic details, including career and education history, are included in Chapter 7. All three team members were interviewed. Prior to the interview, security awareness team members were asked to complete a paper survey that collected demographic information including formal education, work experience, gender, age range, and age (Appendix D). The security awareness team interview protocol (Appendix E) was based on the protocol used in the preceding interview study with some modifications to account for capturing Agency A
organizational details and the specific security awareness focus. The security awareness lead (designated as a “key individual” in the interview protocol) was asked more questions than the two contractors in order to obtain details about the security awareness team composition and security awareness efforts. The lead’s interview lasted 69 minutes and the two contractor interviews were approximately 30 minutes each.

To obtain a management perspective of the security awareness team and program, two managers in the team’s chain-of-command were interviewed. Both managers were federal employees. One manager was the direct supervisor of the team lead (interview time 44 minutes), and the other was the CISO (interview time 18 minutes). The manager interview included questions about the manager’s views about the security awareness program, how resource decisions are made for the program, and thoughts about the biggest security challenges to the organization and its employees. No demographic questionnaire was completed for managers, but they were asked about their role and number of years at Agency A. The interview protocol for managers is included in Appendix F.

Nine federal employees at Agency A who were “consumers” of the security awareness team’s events and materials were interviewed to gain an understanding of which advocacy techniques were viewed as most valuable and impactful by clients. Employees were selected and recruited via email and face-to-face contact by members of the security awareness team based on a request to include individuals in both technical and non-technical roles. The employee interview protocol is included in Appendix G. Employee interviews lasted on average 27 minutes. All interviews were held within Agency A’s workspaces. These interviews included questions about employees’ views of
the organization’s security awareness program, the security information they received, and the impact of that information on their behaviors. A full demographic questionnaire was not completed for employees, although they were asked about their job role and how long they had been at Agency A. At the end of the interview, so as not to impact answers to previous questions, employees were asked to assess their own familiarity with IT and cybersecurity. Note that self-reported familiarity may not accurately represent a participant’s actual knowledge in that area. However, self-assessments may provide insight into how an individuals’ perception of their own knowledge and abilities matches to their interview question answers.
Table 2 contains high-level employee participant information, including role, number of years working at Agency A, and self-assessment of IT and cybersecurity familiarity.

Prior to the interviews, participants in all three types of interviews were provided with an information sheet describing the study procedures and were given the opportunity to ask questions. Interviewees were not compensated for participation. Interviews were audio-recorded and transcribed. Data were stored without personal identifiers, rather with a participant code. Participant codes for security awareness team members are indicated with an “S” (e.g., S1), managers begin with an “M,” and employees begin with an “E.” The name of Agency A was also not recorded in transcriptions.
### Table 2

**Case Study Employee Demographics**

<table>
<thead>
<tr>
<th>ID</th>
<th>Role</th>
<th># Years at Agency</th>
<th>IT Familiarity</th>
<th>Cybersecurity Familiarity</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Research librarian</td>
<td>12</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>E2</td>
<td>Manager of an information security organization</td>
<td>12</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>E3</td>
<td>Team leader of a research and technology resources organization</td>
<td>14</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>E4</td>
<td>Engineer</td>
<td>12</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>E5</td>
<td>Attorney</td>
<td>30+</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>E6</td>
<td>Attorney</td>
<td>12</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>E7</td>
<td>IT specialist, information systems security officer</td>
<td>11</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>E8</td>
<td>Information systems security officer</td>
<td>17</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>E9</td>
<td>IT specialist</td>
<td>13</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

#### 3.2.3.2 Field Observations of Security Awareness Events

The security awareness team organizes three different types of events throughout the year: informal lunchtime events, security days, and security officer forums. To observe the security awareness team’s approaches in action, I captured an annual cycle of events by attending six in-person cybersecurity awareness events, aiming to attend at least one of each type of event. I observed three lunchtime events (involving three different formats), one security officer forum, and two security days (described in Chapter 7). Field notes taken during the events captured advocacy techniques, the kinds of security information provided, and general audience reactions. The events were not able to be audio or video recorded.

#### 3.2.3.3 Collection of Security Awareness Documents

I collected over 25 electronic copies of security awareness materials disseminated to Agency A employees and physical copies of handouts provided at security awareness
events. The security awareness team provided me with two other types of documents for analysis: 1) 20 post-event reports from 2017-2019 written by the team which were provided to their leadership and event attendees and 2) six feedback survey results from security officer forums and security day events in 2018-2019 (surveys are not distributed after lunchtime events). The reports and survey results provided insight into how the team frames events to others in the organization as well as how attendees viewed the events.

3.2.3.4 Emerging Questions

As analysis progressed concurrently with data collection, emerging themes and additional questions arose. Therefore, additional data was collected as needed via email exchanges with the team and via several phone conversations when more detailed information was needed. For example, one phone conversation revolved around learning more about past, current, and future phishing exercise processes.

3.2.4 Analysis

Data analysis of interviews and event field notes was initially guided by a subset of applicable deductive codes observed during the prior interview study, with inductive coding being employed as new data labels emerge. My advisor and I individually coded a sample of interviews (all security awareness team interviews, one manager interview, and two employee interviews), then met to discuss the applicability of the deductive codes, reorganize codes based on differences in the case study focus as compared to the interview study, and suggest new codes as appropriate to construct a final codebook (Appendix H). The codebook was then used to deductively code the remaining interviews and field notes. During our regular meetings, we also discussed emerging themes and our interpretations of the data. Similar to the first study, I engaged in memo-writing to
capture reflections about the data, axial coding to incorporate new codes or to adjust existing codes into new structures, and selective coding to identify core concepts.

Memos captured general observations and my interpretations of collected security awareness documents. I reviewed the security awareness documents with an eye towards gleaning which security topics the security awareness team and agency deemed important to distribute and how the team leverages third party resources. A review of post-event reports provided a deeper understanding of past security awareness events, including attendance and topics and how the events were portrayed to the team’s leadership. Event feedback surveys offered insight into how the events were viewed by attendees and how employee feedback contributed to subsequent events.

3.2.5 Study Design Tradeoffs

The security awareness team’s involvement in the recruitment of potential employees to interview may have resulted in a biased sample. Although a diverse sample representative of multiple work roles within Agency A was requested, employees more familiar with and favorable towards the security awareness team and cybersecurity in general may have agreed to be interviewed. In fact, four out of the nine employee participants worked in a cybersecurity-related role. However, this recruitment method was the most reasonable avenue given my limited access to employee contact information and desire to maintain agency employee anonymity. In addition, as with the interview study, security awareness techniques cited by participants as being successful only account for participant perceptions.
3.3 Mapping to Research Questions

The advocate interview study and case study both serve as different lenses to the work of cybersecurity advocates. The combined studies provide insight into all five research questions. Error! Reference source not found. maps the data collection methods of each study to the research questions.

Table 3

Mapping data collection methods to research questions

<table>
<thead>
<tr>
<th>Research Question</th>
<th>Interview Study</th>
<th>Case Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SI MI EI EO MA</td>
<td></td>
</tr>
<tr>
<td>RQ1: What are the motivations, professional characteristics, and skills of</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>cybersecurity advocates?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RQ2: What techniques do cybersecurity advocates use to encourage security</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>adoption?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RQ3: What are the rewards and challenges experienced by cybersecurity advocates?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RQ4: From where do cybersecurity advocates get their security information and</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>knowledge?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RQ5: What techniques and attributes of cybersecurity advocates result in</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>motivating their clients/audience to act or change behavior?</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>


3.4 Disclosure of Researcher Experience and Biases

In qualitative research, the researcher, with all her biases, past experiences, and subjectivism, is ultimately the primary instrument for data collection and analysis (Merriam & Tisdell, 2016). Therefore, in this section, to remain transparent and acknowledge potential influences on data collection and interpretation, I describe my professional experience related to the topic of study.
Prior to conducting this research, I spent over 20 years working in a cybersecurity advocate role within the U.S. government writing security guidance, evaluating the security of other organizations’ computer networks, and helping to educate people on how to better secure their digital assets. Although I had some successes, I was often frustrated about how slowly organizations changed their security behaviors and learned hard lessons about how security recommendations that seemed to make good technical sense did not always work well in reality. My professional experiences ultimately led me to an interest in researching non-technical aspects of cybersecurity and the human-centered computing field.

Having worked in an advocate role was valuable to my research project in several ways. During the interviews and case study, I understood and could converse in the technical language used by the participants, which eliminated the need to ask clarifying questions about what certain terms meant. Revealing that I had worked as a security practitioner also helped in establishing credibility and trust with the interview study participants because I was viewed as one of them. In particular, representing my employer, NIST, during the case study afforded me immediate credibility since NIST is generally well-respected and known throughout the government. The case study agency had previous positive experiences with others at NIST. In addition, agency employees might have been more willing to be interviewed and observed by someone from another federal agency as opposed to someone from an academic institution. There is a sense of trust that their information will be handled appropriately because of government standards. Finally, although my agency is quite different than Agency A, government
agencies share common experiences since they have many of the same challenges, mandates, etc. especially with respect to cybersecurity.

Although my professional background brought value, I had to be keenly cognizant of the biases I brought to the research given my prior experience in the field so as not to influence participant responses or skew data analysis. I had to guard against making assumptions or drawing conclusions based on my own experience as these might have resulted in not delving as deeply into participant responses as an outsider to the field might. In addition, as a former security professional, I do view security best practices and advocacy as being valuable; therefore, I had to be careful not to make assertions based on my own opinions when those have not been scientifically proven.

Although I had some initial thoughts about what the research might reveal, I found that the data took me in directions never anticipated, in large part due to the strategy to sample across a variety of sectors and roles, most of which I had not worked in. For example, the discipline diversity of participants and the emphasis on non-technical competencies were surprising and quite different from my own experience working in an organization where technical skills were the basis of recruitment and performance evaluation. In addition, I had no prior experience working in security awareness, so the case study afforded an opportunity to become more familiar with different applications of security advocacy.

3.5 Timeline

The following timeline shows completion of major research milestones.

*Interviews of Cybersecurity Advocates:*

- October 2016 – November 2016: Study design, research protocol approved
- November 2016 – August 2017: Data collection
- December 2016 – January 2019: Data analysis

**Proposal Defense:** September 2018

**Case Study:**
- November 2018 – December 2018: Recruitment of security advocacy group, study design, research protocol amendment approved
- December 2018 – December 2019: Data collection
- February 2019 – December 2019: Data Analysis

**Synthesis:**
- July 2019 – December 2019: Synthesis and dissertation writing

**Final Defense:** February 2020
4 Interview Study: Advocate Characteristics

The enumeration of advocate characteristics and competencies can be used to better define the role and provide a starting point for professional development resources for advocates. These results were also reported in my previously-published papers (Haney and Lutters, 2017a; Haney and Lutters 2017b; Haney & Lutters, 2018b; Haney & Lutters, 2019). In this chapter, I present discoveries addressing:

RQ1: What are the motivations, professional characteristics, and skills of cybersecurity advocates?

RQ3 (in part): What are the challenges and **rewards** experienced by cybersecurity advocates?

4.1 Skills and Characteristics

This section presents findings on commonly self-reported skills and characteristics of cybersecurity advocates as viewed by participants. These data are complementary to the techniques and approaches noted by security advocates in the interviews as described in Chapters 5 and 6.

4.1.1 Technical Skills

Cybersecurity is often viewed from a technocentric perspective. Therefore, not surprisingly, participants asserted that effective cybersecurity advocates should possess technical literacy to be able to gain credibility with their target audiences and communicate security-related messages. One security analyst noted, “*if you don’t know what you’re doing, that’s going to become apparent very quickly*” (P01).
Although technical knowledge is important, staying up-to-date on constantly changing technology and security risks is not a trivial task. As one participant noted, “it’s impossible to keep track of everything” (P02). Staying relevant is a conscious choice that requires significant and sustained effort. A security consultant reflected, “It’s a way of life” (P10). Another participant commented:

“I’ve always believed that this job is not a 9 to 5 job. There are a lot of jobs you come into, you can get away with that. In this job because it changes so fast, there’s so much whether it’s the technology, the threats, the security pieces. It’s something you just have to really want to be doing and be very passionate about, that when you go home, you just don’t leave it behind. It’s that article that you see in the newspaper, that thing you hear on the news about a new technology that you just, you want to read about it, you want to learn a little bit more about it. I think that’s important” (P05).

Participants revealed a number of ways they try to keep abreast of the latest security happenings, including: reading online reports, articles, and newsletters; subscribing to technical forums and mailing lists; following social media posts; joining security information sharing communities (e.g., InfraGard, a public-private partnership with the FBI); and attending security conferences and other events. They also extensively draw on their professional network. P04, a non-profit executive, spoke about the value of his organization’s large volunteer network: “Part of the role that we have is kind of community organizer. Actually, I often joke, I have more people working for me than I ever did, it’s just I’ve never met most of them. So, that’s a powerful thing.” However, he
also relies on his smaller, inner circle: “I have a few, I’ll say really trusted friends that are especially I would call them industry watchers...So they’re always looking for the newest thing. When I hear things and don’t have time to dig in, one phone call or email to them, ‘Hey what do you think about this?’” Indeed, advocates repeatedly mentioned professional networks as being critical to their ability to keep updated on security risks and technologies.

4.1.2 Non-technical Skills

Participants felt that technical knowledge is important, but those trained only in computing disciplines may not have all the skills necessary to be an effective advocate. The interviews revealed that the ability to navigate social and organizational factors were viewed as perhaps more important in addressing cybersecurity issues than technology alone. All participants mentioned less conventional, non-technical skills and abilities when asked to describe qualities of those successful in security advocacy. Competencies most often mentioned were interpersonal skills, context awareness, and communication skills. These competencies are described in more detail in Chapters 5 and 6 within the context of advocate approaches and techniques.

4.1.3 Service Orientation

While technical and soft skills may be expected competencies of cybersecurity advocates, a surprising finding was participants’ strong sense of service in helping others to protect themselves and their information. Hogan, Hogan, and Busch (1984) defined service orientation as the willingness to treat customers with courtesy, consideration, and tact; perceptiveness to customer needs; and the ability to communicate accurately and pleasantly. Although most prior service orientation research was conducted in a retail
business context as opposed to my sample, the interview data appears to have implications for cybersecurity advocacy since advocates’ audiences can ultimately be viewed as “customers” of security guidance.

Service orientation was portrayed by 25 participants not only in how they performed advocacy-related tasks, but also in their own self-reflective perceptions of their identity and work. A former lawyer now serving as a director at a non-profit considered how her security advocacy work aligned with her predispositions: “I think fundamentally I am the type of person that likes to help other people. That’s been pretty clear in my whole career” (P15). Another participant, who mainly advocates to non-technical audiences, remarked, “It is nice to be able to help....There’s so much stuff going on for people nowadays...We have almost an information overload happening...If I can take a worry off the table for people, I’m happy to do that” (P08).

Participants had a keen desire to help people navigate the dangers and complexities of the cyber world. A usable security champion commented, “I like making people’s lives easier” (P03). A CISO working in local government said, “There’s huge difference between my job satisfaction level when I know what I’m doing, day-in and day-out, is out there helping ultimately the citizens and the general population” (P26). Another participant talked about the rewards of serving as both a corporate consultant and a community educator: “I always get really excited when I can just tell people have learned something...I know that I’ve done something good” (P23).

All participants attempted to address the gap in security knowledge by playing formal or informal educator roles. Fifteen served as mentors to future and current security professionals. An interviewee who teaches at local colleges commented, “I’m not going
to be in this forever, so I really want to make sure that I kind of bring in that education piece and try to help the next group” (P12). Three participants had positive experiences providing security education to youth. One remarked, “I really...like trying to influence a younger age because I think those people have an appreciation for the technology, but maybe not the security aspects of it” (P05). Other advocates educated less-technical audiences. For example, one participant extended her advocacy responsibilities outside of work:

“I actually spend a significant time of my personal life...educating teachers and working with the old lady gang on my block to get them to understand security so that they’re not in a position where they have to deal with some criminal stealing their information or stealing their hard-earned money” (P23).

Another discussed his upcoming talk to a local community group:

“I’m trying to tune the message. What should citizens care about?...They’re all great people, but they’re not going learn what I’ve learned. So what is it that I can tell them that will help them, to get their attention, to cause them to change behavior?...There’s a lot of great technologists in this business, but based on technology, we’re not going to change people’s behavior – well, only in niches. So, how do we put our work in other people’s context?” (P04).

4.1.4 Pro-Social Passion

Accompanying the sense of service was a deep, pro-social passion for the work. Even though security problems may seem intractable in the midst of dynamic threats,
participants reflected that the economic, physical, and national security consequences are too dire for them not to do something. A government advocate discussed his advocacy motivation: “I primarily do it to fix society. I see that we have a lot of problems that are getting worse” (P16). Another participant, who worked with U.S. government customers, commented: “It’s important because of the implications of not doing it...the significance and the potential of loss of dollars, of information, of man hours, of intellectual property, sensitive information” (P01). An advocate who works for a non-profit also remarked on the societal impact of security: “security is an enabler for us to do the things that we want to do...It’s beyond critical” (P24). A participant who works to influence public policy stated, “I think we’re making the world a better place” (P06). Several advocates saw the potential of poor cybersecurity resulting in the loss of lives. One participant warned, “If we don’t get computers right, people are going to starve. And right now, we’re not doing a good job” (P16). Another advocate who leads a non-profit discussed his group’s motivation:

“We had said we want to save lives through security research. It was really wherever bits and bytes meet flesh. That could be cars, medical devices, industrial control systems. But everyone’s so focused on data and the confidentiality of data...We’re spending nothing on our life and limb” (P11).

Thus, interviewed advocates saw their work as having positive societal impact, so were passionate about their choice of careers.
4.1.5 Discipline Diversity

My findings reveal that while some participants who were trained primarily in the technical aspects of their job had a natural proclivity to non-technical competencies, many brought skills honed by formal education in non-technical fields or prior careers in other domains. I show how “discipline diversity,” the incorporation of individuals with non-technical professional experience into the cybersecurity advocate capacity, was viewed by participants as beneficial.

Of the 14 participants with at least one non-technical degree, six had primarily worked in tech positions for their entire careers, while eight worked in non-tech positions prior to their advocacy roles. They viewed their educations as advantageous in developing the non-technical competencies important for security advocacy. One participant, who had worked in computer security his entire career without a formal technical degree, stated, “As I stopped having imposter syndrome about it, I’ve really leveraged my undergraduate philosophy background, soft skills, instead of thinking they were a deficiency” (P11).

Four participants had backgrounds in marketing or communications. One participant utilized prior experience studying interpersonal communications when influencing executives and government officials about cybersecurity policies: “You need to take the other’s perspective...Then you need to be able to be flexible in terms of adapting your argument to their particular needs. And you need to be honest with them...So those basic skills, which also happen to work with interpersonal relationships, absolutely work in this space” (P06). A graphic designer saw the benefit of being an experienced marketer who could speak in terms understood by other non-technical people: “because I’m not an
IT person, all of this that I come in touch with I find interesting and scary and realize that the rest of the population isn’t getting this information” (P28).

Three participants with law degrees became advocates because of their ability to understand the relationship between law, policy, and cybersecurity. One said, “They were looking to have a lawyer on staff to help them translate...legal requirements for information technology into a language that...technologists could understand” (P15). Another, who started out by educating other lawyers, commented on the benefit of engaging others with similar backgrounds, “I know that audience because that’s the audience I relate to. As I understand the information, that’s how I presented it to them” (P08).

Four other participants had business-oriented degrees, and often leveraged their interpersonal skills and understanding of business contexts in their advocacy work. When asked how to establish trust and credibility, a participant harkened back to his formal training: “I think that kind of goes back to being a student of the humanities and knowing...how to deal with people” (P02). A former management consultant’s tendency to pitch cybersecurity as a “competitive advantage” (P27) helped convincing corporations to implement incentive structures for rigorous security practices.

4.2 Motivations

Interview study findings revealed a number of professional drivers for cybersecurity advocates, most of which were intrinsic motivators. These included interest in the field, self-efficacy, evidence of impact, comradery, and, to a lesser degree, awards and monetary compensation. A sense of duty was another motivator but is discussed more in
terms of service orientation as an innate characteristic of cybersecurity advocates in section 4.1.

4.2.1 Personal Interest

The belief that cybersecurity is a challenging and “intellectually exciting” (P16) field was a motivator for 19 participants. A graphic designer-turned-advocate commented that the security awareness profession is “like a giant puzzle. And challenges are my thing. I like being able to put effort into something that’s creative and interesting and different” (P28).

Since the cybersecurity field is relatively young and quite dynamic, it offers opportunities for innovation, which appealed to participants. One said, “I’m attracted to areas where there’s new things to do,...where it’s not really established, where I get to solve a new problem, and solve a new problem that matters” (P19). A security awareness program director at a public university commented, “It’s ever-evolving...I find it to be a challenge because threats and vulnerabilities in all environments...are always there and they’re always becoming more sophisticated...That’s what motivates me to stay in” (P14).

I also identified an interest in interdisciplinary work. The nature of advocates’ work is multi-faceted in that it must consider challenges “at the people level, at the business level, the strategic level” (P27). An advocate with a strong cybersecurity background fell into security awareness when she became exposed to the human aspects of security: “the power of human motivation fascinates me. And I think if I wasn’t doing this, I’d probably be a behavioral psychologist or something” (P21). Another participant worked at the intersection of cybersecurity and usability:
“I tend to have an interest in things that are interdisciplinary and kind of at the border of different things...So, this combination of the technical and human factors interests me, and I guess I seem to be good at it, so that encourages me to want to do more” (P07).

4.2.2 Self-Efficacy

Self-efficacy, a belief in one’s own ability to accomplish a task or exert control in specific situations (Bandura, 1977), can be an important motivator (Bashir et al., 2017; Chai & Kim, 2012). A large part of self-efficacy is self-confidence that one has the necessary knowledge and skillsets.

All participants exhibited self-confidence in their abilities to effectively perform advocacy tasks. This confidence was gained through years of experience and continuous learning. An advocate reflected on how his involvement with operational and threat intelligence organizations contributed to his effectiveness: “Those two perspectives help me bring some unique value to the problem” (P05).

Other advocates expressed confidence in their non-technical “soft” skills which were often deemed as more important than technical skills in advocacy work. For example, the ability to translate technical topics into layman’s terms was noted as an important competency by 24 participants. When giving presentations to nontechnical audiences, one participant commented, “I seem to have the magic power to make these things make sense” (P08).

4.2.1 Sense of Duty

Interview study participants were largely motivated by a sense of duty to individuals, organizations, and society as a whole. For example, a participant who works
to influence public policy stated, “I think we’re making the world a better place” (P06).

This sense of duty, or orientation to service, was previously described in detail in section 4.1.3.

4.2.2 Evidence of Impact

Since the goal of cybersecurity advocacy is behavior change, evidence that an advocate’s recommendations have been understood, concurred with, and acted upon served as strong motivators for our participants and contributed to self-efficacy (23 participants). One participant said the most rewarding part of her job was “seeing the impact, seeing some difference was made ...however minor or modest” (P19). Similarly, not seeing impact could be a demotivator. When asked about his professional motivation, one participant commented on his frustrations:

“I’d love to say that it’s to help people fight the good fight and make the world a better place. And it is certainly part of that, but I have to say, it isn’t all that because, if it was, I would be very discouraged...We as an industry [are making the same mistakes] we’ve been making forever” (P10).

In the following subsections, I describe ways in which advocates realized the impact of their work as categorized by the sources providing evidence of impact.

4.2.2.1 Organizational Impact

The ability to impact organizations (mentioned by 10 participants) was seen as being especially challenging since organizational barriers to cybersecurity, such as security culture, can be difficult to change. Therefore, evidence of a positive shift in attitude often provided hope of future behavior change. One participant commented: “The impact isn’t
always...an easy thing to quantify in this field. So, I think a lot of times it’s when the organization starts showing the passion, starts showing and are being responsive to the ideas you’re trying to suggest. That can be very rewarding” (P05). Another advocate, who had spent a substantial amount of his career conducting vulnerability assessments, talked about a feeling of accomplishment coming with “the knowledge that the people were really onboard and believed what it was they were doing, believed that what we were telling them was important, and had the right guidance and the right authority to be able to move forward with it” (P01).

One participant spoke about how the effectiveness of a security awareness program might be measured by incremental shifts in security culture:

“it goes beyond just behavior, but more on the culture. So when you’re talking to people, if they have a positive attitude about cybersecurity, a positive attitude about the cybersecurity team, if they feel like their behaviors have a positive impact, that’s the first real big indicator that you’ve got a long-term win. Now the problem you have is changing culture’s a three to ten-year process” (P09).

Five participants were able to influence organizations via their input into cybersecurity policies. These policies may be at organizational, sector, or national levels and may include mandates or guidance for security considerations such as network security, authentication methods, security processes, or end-user security expectations. Several participants had the opportunity to affect broad-reaching cybersecurity policies that impacted many people or organizations at once. One participant who had worked in the government sector talked about how his organization had “shaped the spending of
hundreds of millions of dollars and the behavior of thousands” (P04). P06’s non-profit successfully lobbied for a substantial paradigm shift in cybersecurity public policy within the United States. P11 influenced medical device policy that prevented serious vulnerabilities from claiming lives.

4.2.2.2 Individual Impact

Eleven participants talked about the satisfaction of educating and making an impact on individuals. One advocate said, “I always get really excited when I can just tell people have learned something. So, when I see that little lightbulb come on...when I get confirmation that something I’ve said makes a difference, I get really excited” (P23). A participant noted that, after giving a presentation, “I definitely like interacting with people and people telling me, ‘Wow, I learned something. I can use this. I’m going to change what I do, and this will help me.’ I find that rewarding” (P07). Another commented that he feels energized “when I’m working with an adult, and they have the ‘Eureka!’ moment. They’re struggling with understanding something, and you kind of sit next to them, and then they get it and you can see it in their eyes. Often a high-five moment happens” (P10). Advocates viewed these displays of audience discovery and understanding as explicit and satisfying indicators of having made an impact.

A deeply satisfying aspect of the job is the observation of the target audience taking the information they had learned and transferring that to others, as was mentioned by eight participants. A participant told a story about how an elderly neighbor whom she had taught cybersecurity best practices in turn taught her son a lesson:

“Her son was buying a house, and she kept telling him, ‘Don’t email that stuff. Don’t email your personal stuff.’ Well, probably about two weeks
into purchasing the home, he realized that his email had been completely compromised...She saved him probably three million dollars because what happened is, in the middle of setting up escrow, someone asked for a bank account number. It wasn’t anyone from the real estate firm” (P23).

Three participants discussed their roles in helping good security habits blur across the home-work divide. For example, one participant remarked:

“If you can train them with their home life and help them there, too, they can hopefully bring those behaviors to work and bring that sense of awareness up. So, a lot of the organizations share those personal, consumer-focused resources with their employees so they can keep their families safe at home, too” (P24).

A security awareness program director provided another example:

“We had a videotape...One of the presenters...had been kidnapped. She had been social engineered by a man online...And I know some of the people took their laptops home, logged in, and made their kids watch that. So, I think that’s great, too, when the information that you’re giving at work, people are sharing with friends and family, too” (P28).

4.2.2.3 Metrics

Nine participants viewed metrics as motivating evidence that they were on the right path with their approaches. Metrics mentioned by participants included how many people accessed publications and videos, the number of newsletter subscriptions, attendance of security events, the growth of non-profit membership, and statistics showing improvement in security behaviors. A participant discussed the importance of metrics in
showing success of an organization’s security awareness program: “initially you may have to measure success by some specific behaviors such as phishing, exposing of sensitive data, use of ID badges and things like that” (P09). Advocates monitored these metrics as one indicator of both the reach of their message and effectiveness of a communication channel. For example, one participant noted that one of her talks had been recorded and posted online and had “been viewed like two million times...There’s a lot of bang for that buck” (P07). A participant whose organization produced cybersecurity implementation resources said:

“We create specific things, sort of products to give away, ideas and papers. So, part of that is it comes with some natural mechanism now to calibrate feedback. How often is it downloaded, how often is it referenced?...We see lots of interest worldwide. We can count how many tens of thousands of downloads there have been” (P04).

4.2.2.4 Praise

Praise is an extrinsic motivator that, when sincere, can significantly contribute to intrinsic motivation. Fourteen participants felt valued after receiving positive feedback from their audience. Some feedback was more formal, often obtained through surveys. For example, a non-profit advocate commented:

“We have teams to reach out to adopters of our work, talk to them, ask them questions through surveys, write down use cases if they’re willing, that sort of thing ...feedback is not an issue. We get a lot of that. I’d say it’s overwhelming positive” (P04).
Informal feedback, such as face-to-face comments and email, seemed to be most personally satisfying. A participant who advocates to lawyers talked about one member of his audience saying, “‘This is amazing! So many lawyers don’t understand this.’...It’s wonderful to get those sorts of reactions” (P08). A security awareness director at a university remarked:

“I’ll get stuff directly if I run an event of some kind, an awareness event, whether it’s a conference or just a small brown bag session. I will receive emails from attendees saying, ‘Hey, this was extremely helpful. I was unaware of XYZ component of data privacy. Or HIPAA [Health Insurance Portability and Accountability Act] privacy.’ Whatever the topic might be. So the feedback that I receive in many instances is informal feedback” (P14).

4.2.3 Comradery

When asked about the rewards of their jobs, seven participants discussed their enjoyment working with others in the field. Whereas this motivation is not unique from other professions, it highlights the importance of a sense of belonging and collaboration in the cybersecurity advocate role and runs counter to commonly-held stereotypes of cybersecurity being a solitary profession (Shumba et al., 2013). A security course instructor and consultant commented, “most of my very close friends are in this industry. I love to spend time with them thinking good thoughts” (P10). A security evangelist at a non-profit described the benefits of working with a large group of volunteers to produce security guidance: “It’s a business full of really bright people, lot of diverse, creative,
smart people of good will...So I love that part of it, the sort of community, this collaboration...it’s something that’s personally satisfying” (P04).

The interactions advocates have with others in the field were viewed as not just personally satisfying but as a necessary component of the job. Because of the distinctly dynamic nature of the cybersecurity field in which major developments can occur on a daily basis, advocates relied on a symbiotic relationship of receiving and contributing information within their personal networks. For example, an advocate who is active in a security awareness community commented, “not only am I always giving to the community, I’m listening to the community...So, I always understand the latest and greatest risk from a human side” (P09).

4.2.4 Awards and Monetary Compensation

Only five participants mentioned official recognitions or monetary compensation as motivators. One participant, referencing her team’s best website award, said, “I love it when my team is recognized” (P26). Another was motivated by continued research funding: “if they didn’t like what you were doing, and they didn’t think there was value, they wouldn’t continue to fund you. And so, our funding’s pretty stable” (P03). When asked about the rewards of his work, one advocate first mentioned the fun he has educating youth about cybersecurity and the gratitude of his clients. However, he was then quite frank when he also included financial reward:

“As long as you’re not cheating people or doing something dishonest, if you’re providing real value, the way people indicate that you’re providing real value to them is by paying you. So the more that they pay you, the more value you’re providing...So I know that might sound crude, and
maybe I should be more noble, ... but I always realize at the end of the day, I gotta make payroll” (P10).

I observed that few mentioned financial reward, perhaps due in part to participants viewing its mention as socially undesirable within the context of the interviews. Therefore, there is a possibility that awards and monetary compensation play a larger motivational role than discovered in this interview study.

4.3 Chapter Summary

This chapter lays the foundation for defining the cybersecurity advocate role by describing characteristics and motivations of those performing this type of work. I found that technical literacy is viewed as a requirement of advocacy work but, surprisingly, is regarded as less important than non-technical skills, such as interpersonal and communication, due to a recognition of the social component of the job. These individuals were deeply service-oriented and passionate about the work as they saw cybersecurity having the potential for significant negative or positive impacts to society. They are motivated by a love of and aptitude with technology, the enjoyment of working with others in the field, and, most significantly, by seeing their efforts are making a positive impact on their audience.

Chapter 5 continues the discovery of the role by describing how advocates leverage their skills and display their characteristics in their routine work practices. In addition, the self-reports by experts outlined in this chapter are further explored via observable characteristics in context within the case study as presented in Chapter 8.
5 Interview Study: Overcoming Negative Perceptions of Security

This chapter describes interview study findings related to cybersecurity advocacy approaches in the context of how they overcome negative perceptions of security first reported in Haney and Lutters (2018a). The following research questions are addressed:

RQ1 (partially): What are the motivations, **professional characteristics, and skills** of cybersecurity advocates?

RQ2: What techniques do cybersecurity advocates use to encourage security adoption?

RQ3 (partially): What are the rewards and **challenges** experienced by cybersecurity advocates?

Analysis of the interview data reveals ways in which advocates attempt to overcome users’ widely-held negative views of security. An overview of the framework is provided pictorially in Figure 1. Participant interview responses revealed that, as a foundation, advocates must first establish trust with their audience. To overcome perceptions of security being fear-invoking, advocates are honest, yet discerning, about the risks they communicate. They also attempt to empower their audience by engendering a feeling of hope and self-efficacy. Advocates address feelings that security is confusing, complex, and difficult by “bridging the gap,” that is establishing common ground between security experts and non-experts. They do this by serving as security educators who promote recommendations that can be realistically accomplished with usable security solutions. Finally, to overcome perceptions that security is irrelevant and boring, advocates create interest by incentivizing and employing engaging rhetorical techniques.
5.1 Establishing Trust

Before advocates can overcome negative perceptions of security, they must first establish trust, which is a foundational aspect of risk communication. A security engineer who provides consultation to government customers spoke of this trust: “To me, trust is the most important thing that I have. If they trust that what I’m telling them and what I’m doing is the right thing, then I am much more successful” (P12).

Advocates gain audience trust by relying on organizational reputation, demonstrating technical knowledge, building relationships, and leveraging insider access.

5.1.1 Relying on Organization Reputation

As noted in four interviews, organizational reputation may help to establish credibility, at least initially. One participant suggested that the most effective advocates are sometimes “people who have the credentials and are associated with organizations...
that are viewed as having some authority” (P07). This reputation can especially be helpful when advocating to general public audiences via online channels, since personal interactions with these audiences may be rare. However, when interacting directly with an audience, organizational reputation only goes so far, and must ultimately be upheld on an individual basis. A government security analyst discussed this external bump versus sustained personal reputation: “Our agency...carries with it a great deal of credibility...And I think that helps out a lot. But [individuals have] to be able to exhibit and illustrate the qualities that go along with the respect they bring into the door” (P01).

5.1.2 Demonstrating Technical Knowledge

One way that advocates establish individual credibility is by demonstrating technical knowledge, as suggested as an important characteristic by 19 participants. When asked what makes people successful at promoting security, one participant remarked, “First and foremost, you really do need to understand the technology...This stuff’s tricky, and you don’t just guess your way out of it” (P08). Advocates that work with technical staff are particularly held to high standards with respect to technical acumen. A participant with over 30 years in the security field emphasized this:

“This is a business that is very technology oriented, and full of people...who want to one-up you. So if you can’t kind of deal with that, it’s going to be hard for you to be an effective advocate because people will kind of eat you up” (P04).
5.1.3 Building Relationships

Whereas technical skill may be an important component in building credibility and trust, our findings support previous risk communication research that emphasizes the importance of exercising interpersonal skills to build relationships and foster trust. A security usability specialist emphasized the value of these non-technical skills: “If you’re a computer scientist, and all you know is the computer science, and you don’t have the empathy, you don’t have the skills to listen,...you don’t have that psychological side, I don’t think you can make it work” (P03).

Relationship building is facilitated by demonstrating empathy (mentioned by four participants) and listening skills (6). A participant suggested, “The most important part is to go in and listen...to what their challenges are, what their problems are” (P05). A technical executive at a higher education institution expressed the importance of empathy:

“I think people have to have a high emotional intelligence and especially empathy. Part of being successful in this is being able to have a conversation and put yourself in the place of the person that you’re working with, and then be able to give effective advice that is not preaching, is trying to be helpful, and is letting them know that they’re not stupid because they may not know how to do certain things” (P18).

Humility was mentioned by five participants as another interpersonal skill important for trust-building. Several noted that those advocates who approach a situation with an attitude of “I’m in charge. I know best. You must listen to me” (P02) are not generally very effective in enacting security behavior change because they put their audience on the defensive. A deputy CIO with a strong technical background remarked on the
importance of not being arrogant because “You’ll never have all the answers” (P25). A security consultant discussed his personal philosophy of humility: “Whenever I walk in the room, I assume I’m the stupidest one there, and everything works out great” (P10).

Participants believed that trust is also created by being open to multiple viewpoints and building consensus. Consensus was especially important for the participants from non-profit organizations that relied on volunteers to inform their advocacy efforts. A founder of a non-profit group discussed their commitment to consensus building: “We prioritize and cherish a multi-stakeholder approach. There [are] lots of voices...The goal is to surface beliefs, combine them with other beliefs, come to a set of shared beliefs” (P11). Another participant described her collaborative role with members of her non-profit organization as “an uber-facilitator. Our job is to get these people together and make them work for the common good” (P15).

Interpersonal skills do not only apply to advocates who have in-person interactions with their audience; others must utilize these skills for any security guidance that reaches their audiences. For example, P24’s non-profit conducts extensive anonymous consumer research prior to publishing security guidance to ensure they address their audience’s concerns and use language that will be easily understood. This attention to their audience’s needs, in effect, demonstrates listening skills and empathy.

5.1.4 Leveraging Insider Access

Nine participants gained credibility due to their past experience in the professional communities to which they advocated security. This experience helped them to be portrayed as “insiders.” For example, one participant with a law background began her career in security advocacy when a legal organization recruited her to help with
security compliance: “They needed a translator to translate law to geek...And I learned that I sort of have a unique aptitude in this area where law and information security policy intersect” (P15). Another participant remarked, “It’s very difficult to integrate yourself into someone else’s daily work when you don’t know what the daily work is” (P17).

However, gaining credibility can be challenging when the advocate is perceived as an outsider. To overcome this, six mentioned the value of enlisting the support of opinion leaders and decision-makers within the target community. One participant talked about this value: “You need to find whoever it is that you think is a change maker and make sure they have that data, that they’re excited by that data, and they can use it to their benefit to make a difference” (P03).

5.2 Overcoming Perceptions that Security is Scary

The interviewed advocates felt that the consequences of poor security can be catastrophic personally, organizationally, and societally. The participants had a solid understanding of the current state of security and potential consequences of poor security practices. One participant believed the internet is “getting more insecure constantly...The bad guys are getting better” (P06). Another was concerned with global consequences, saying, “It is so easy to imagine a really big cyber incident. And the barrier to entry is really, really low” (P16).

Security risks are real, but several participants believed that, in some cases, these risks are sensationalized. Two participants partially blamed other security professionals, with one advocate noting, “We’re just really a fear-mongering industry” (P21). Another who came into the security field with a humanities background observed security
professionals “tend to be really negative and really fatalistic. Everything’s awful, everything’s burning, everything’s dead” (P23).

Three participants also blamed media portrayals of security incidents for creating perceptions of fear, particularly among non-technical audiences. A security consultant reflected that when people see depictions of cyber incidents on television and in the movies, “the computer looks like some kind of magic box where somebody touches it, and zing! They attacked our network and taken our children, and look, they’ve wilted our lettuce!” (P08). Another commented on how media portrayals can build fear around concepts that are unfamiliar: “People are afraid of what they don’t understand or don’t want to learn...Their consciousness is kind of framed in this Hollywood...sort of approach where it’s this evildoer. And that terrifies people” (P02).

It is not surprising, then, that some people view cybersecurity with fear. To address this perception of security being scary, cybersecurity advocates must strike a careful balance between being candid about security risks while being hopeful and encouraging. The latter are essential for developing a sense of empowerment in the audience.

5.2.1 Being Honest, Yet Discerning, About Risk

To convey a sense of importance and urgency to their audience, participants said that they must be forthcoming about risks. One participant remarked, “You can’t appreciate the importance of security without first understanding what’s at stake, what’s at risk” (P14). Another recommended, “In terms of it being scary...take that head on. Here are all the terrible things that can happen” (P08).
However, six participants noted the importance of being discerning: not “crying wolf” (being an unnecessary alarmist) over every little security issue, lest their audience become overwhelmed, disinterested, or skeptical. One said a mistake in security advocacy is “being more sensational, and theoretical, and hypothetical than practical and rational...Focusing on the possibility is a very easy way to get known as crying wolf” (P02).

In some cases, advocates may only want to engage a select group with the authority to address a security issue, especially when dealing with issues that have broader-reaching organizational or national consequences. An advocate who promotes security to industries that build safety-critical products, such as medical devices, commented, “If I told everybody what I know, they’d freak out. I want to tell a smaller list of people I know so that we can quietly fix it” (P11).

5.2.2 Empowering

For many users, an overabundance of fear may result in a feeling of futility regarding their security situation. This can lead to paralysis and inaction. This was echoed by one participant when she said, “If you have a little bit of fear, it’s actionable. But if you have too much fear, it becomes so overwhelming that you give up on it” (P21).

Feelings of helplessness can be perpetuated by security professionals who regularly express their belief that users are unable to comprehend and practice good security behaviors (mentioned by six). An advocate who had led her company’s security awareness program expressed her frustration with these professionals: “I feel like there’s just a lot of people saying, ‘Oh humans are the weakest link. They’re always hopeless...They haven’t changed their behaviors, so what’s the point?’” (P21). Another
commented on the harsh way non-experts are treated by security experts in online forums, remarking, “smashing them and telling them they’re stupid, that’s not going to help. Instead, we need to be more encouraging, more open-armed in the industry” (P10).

To overcome feelings of fear and helplessness, advocates must empower their audience to take action. Empowerment was a concept mentioned by 16 participants, mostly in the context of non-technical users. A prerequisite of empowerment seemed to be a sense of hope, as noted by eight advocates. One participant reflected:

“You can’t last for decades in this cybersecurity business without being one of two personality types: the hopeless cynic or the hopeless optimist...You can make an entire living just pointing out other people’s problems or mistakes...But I just don’t find that satisfying. I’m much more interested in creating positive change” (P04).

Advocates then use this hope to foster self-efficacy in their audience. Self-efficacy is the cornerstone of independence, which was expressed by one advocate when he said, “we have to be able to get to a point at which they can do a lot of it themselves” (P01).

The interviews suggested that self-efficacy can be encouraged by providing people with basic, concrete actions that will empower them to take control of their security situation. Instead of simply raising an alarm, a security technologist believed:

“it’s really important to tell people what they can do so they that don’t just go, ‘Oh my gosh. The world is a scary place, but there’s nothing I can do about it, so I guess I just won’t worry about it’ ” (P07).

Another commented:
“I love empowering people and seeing their lightbulbs go off in the moment that they understand why they are a target and what they can do about it. So, it’s not a place of fear. You have to start with fear to get them to understand that there’s a problem, but then you also give them the tools” (P21).

Framing messages in a positive light and comparing security measures to more familiar, accessible protective mechanisms was also viewed as being helpful in alleviating fear and empowering. A security advocate talked about how she chooses to frame her communications during her work with senior citizens:

“You slip that message of ‘You’re going to get attacked and everything’s going to get stolen’ to ‘Well, it’s kind of like home improvement when you put a better deadbolt on your door or you decide that you’re going to shore up your foundation’ ” (P23).

5.3 Overcoming Perceptions that Security is Confusing

Few security non-experts have the technical know-how to address security issues, so “security is mysterious to most people” (P07). A participant underscored the impact of this knowledge deficiency when she commented, “people don’t actually know what the names of the tools they need are. They don’t know the proper technical words that are going to lead them to a solution” (P23). This lack of understanding leads to the perception that security solutions are confusing and difficult to implement, as noted by 20 participants.

The barrage of security messages and advice people receive at work, from the media, and from friends can create “a lot of uncertainty of what is the right thing to do”
One participant commented on this state of being overwhelmed: “You’re getting hit from every single side... We have almost an information overload happening, and it’s hard to sort through it” (P08).

Security can also be seen as a burden, “just one more thing to remember, one more rule” (P28) that gets in the way of doing other tasks. A participant observed, “there’s a complete misunderstanding that to be secure takes an immense amount of time. That’s a huge obstacle to get over” (P23).

To overcome the perception that security is confusing, advocates “bridge the gap” by establishing common ground between security experts and non-experts, educate people on how to practice good security, provide practical recommendations, and promote usable security solutions.

5.3.1 Bridging the Gap

The process of mediating between technical and non-technical audiences requires establishing common ground (Clark and Brennan, 1991), which necessitates advocates to have strong communication and translation skills and an awareness of audience context. A nonprofit director underscored the importance of communicating in a manner that is meaningful to the audience: “you can produce as many policies and processes as you like, if you cannot communicate them to people in a language that they understand, in a language that means they’re going to be receptive to your message, then they’re worthless” (P27).

Bridging the gap was a frequently discussed concept in the interviews. Participants described their connective roles in various terms, such as translators, boundary spanners, ambassadors, cross-pollinators, and information carriers.
5.3.1.1 Translating

Based on their own experiences, participants believed that highly technical security experts often unwittingly make security seem more elusive as they rely heavily on disciplinary jargon. One participant remarked, “There’s also, I think, a big language issue...it is a highly technical field with a very specialized language” (P04). A lack of understanding of the skill level of their audience also results in confusion, as described by a security awareness educator: “It’s not that people are stupid, it’s that we need to communicate in their language” (P09).

To overcome the language difference, advocates act as “translators,” reframing highly technical concepts using terms their audience can understand. Twenty-three participants commented that the underlying communication skills required for translation were important for security advocacy. In fact, despite being a highly technical person, when asked about the characteristics of successful security advocates, a security consultant said, “communication skills I think are number one” (P10).

While describing the importance of effective communication in his work, a participant asserted, “Being able to translate complicated things very simply is crucial to...advocating security” (P02). A security consultant described his role as a connector between groups: “I’m sort of the in-between person, between the business interests of the company and the technical interests because they don’t talk to each other very well. I can translate both languages” (P08).

5.3.1.2 Being Context Aware

Context awareness was viewed as critical for effective security advocacy, as expressed by 22 participants. As much as possible, they need to be aware of the
operational environment of their audience, including technology, roles, social structures, constraints, and goals. One participant commented, “Understanding your environment, and the different, unique threats and vulnerabilities in your environment is hugely important” (P14). A non-profit organizer used a metaphor to convey this necessity:

“This is more of an ambassador role where you’re going to a foreign country. You need to represent your own country, but you have to assimilate to and acclimate to the language and the beliefs and the culture that you are trying to affect” (P11).

Advocates also discussed using their knowledge of context to tailor the security message to the skill level and concerns of the audience. When appealing to non-technical audiences, a veteran security evangelist realized, “You have to change your language, which means in the non-techno speak figure out how to translate what you know into concerns people have about economic and social issues” (P04). A security engineer who advocates to a wide swath of people within his organization remarked, “The message, even though it’s going to be the same, it’s going to be delivered differently depending on the level of person that you’re talking to” (P13).

5.3.2 Educating

Participants thought that a greater understanding of security helps to overcome confusion and leads to empowerment, as discussed earlier. To that end, advocates saw themselves as security educators. Eleven participants had served at one point in a formal educator role, but all discussed the educational component of their jobs. A security awareness director at a large university saw his role as foundational: “The only way you
can fully understand what’s at risk and what’s at stake is through education and awareness. So, it’s the starting point for everyone. I’m ground zero in security” (P14).

Eleven participants mainly educated non-technical audiences. Their goal was to provide simple, straightforward instruction and help people make informed decisions about their security behaviors: “I think it’s a lot like knowing when you see power lines are down, not to touch the power lines. It’s just a basic level of knowledge you need to know for self-preservation purposes” (P15). For example, P08 created “security awareness basics” videos targeted at the general public. For his other audiences of non-technical professionals in the legal, healthcare, and finance industries, he did both video and in-person presentations on security topics of interest to those communities. He commented on the value of his security education courses: “I’m not going to make you into a security expert in three hours ...But I want you to be able to have a conversation with one where you can be able to follow each other” (P08).

In contrast, others educated technical audiences. Fifteen participants had a role in educating developers, IT specialists, college students, and other security professionals on issues such as secure products and network security. For example, P22 educated product teams within his organization on secure development practices. Five mentioned that it was important to educate the next generation of security professionals “so that they don’t make or sustain the same mistakes...that got us into the mess that we’re in with cybersecurity” (P02). One participant often does presentations for high school students at cybersecurity summer camps, “just talking about information security, and just having fun and making them laugh. And talking about how meaningful this is” (P10).
5.3.3 Providing Practical Recommendations

The participants agreed that the amount of security information to be aware of can be overwhelming, even for them. To counter this, 16 participants discussed providing practical, prioritized recommendations. Six mentioned condensing security information into more manageable chunks containing the most important security actions to take. P11 mentioned how his advocacy group had developed a set of “first principles,” which are foundational security measures that should be in place within an organization before anything else.

While some security guidance is universal, other recommendations are dependent on the audience’s environment. Several participants spoke out against “one-size-fits all” solutions, emphasizing the importance of context. A non-profit organization approached this issue by producing general guidance that can be customized and disseminated by others: “Our goal is to create non-proprietary resources so that our local partners can take those and tailor them for their community...because it could mean different consequences for different people” (P24). Others felt the responsibility to directly provide tailored security guidance that is based on the actual risk within a given situation. One participant was a proponent of this approach within organizations:

“I think in the security area there’s a lot of mythology and a lot of things we do because we heard it’s the right thing to do, and we have no idea why, but everybody else seems to be doing it, so we should do it, too. And so, trying to get people to stop and think it through, and figure out what’s actually going to be effective” (P07).

To ensure guidance was practical to their audience, an advocate in higher education described her organization’s efforts to regularly poll members on their biggest security
risks and challenges. These risks then became the cornerstone of their annual “top 10 list” of security recommendations:

“You’re never going to be able to remediate or mitigate every single information security risk that you have, but you should be able to identify the ones that are the most likely and the ones that would be the most devastating to your environment and take steps to mitigate those” (P15).

5.3.4 Promoting Usability

Security technologies and policies are not generally known for usability, leading to feelings of frustration and confusion (Garfinkel & Lipford, 2014; Zurko & Simon, 1996). One participant felt that security professionals are “putting too much pressure on the user, and the user doesn’t have the knowledge” (P03). She also observed that the volume of security-related tasks a user must perform on a daily basis (e.g., multiple logins) can be overwhelming when viewed as a whole: “In isolation, none of these security things are that big of a hardship or have significant usability concerns. The aggregation of them is what causes the usability concerns” (P03).

To alleviate the complexity and burden of security, nine participants emphasized the need to advocate for systems and security policies that are usable, minimize required knowledge, and compensate for the inevitability of user error. Three participants conducted usability research and shared the results to directly influence vendor products as well as organizational and national policies. One of these participants explained her motivation metaphorically: “Most of us drive a car, but don’t know how to fix cars. We shouldn’t have to know how to fix cars in order to drive them. And I think that should be true about computers, too” (P07). Another participant, who had been a champion for
usable security both internally and externally to his organization, stated that the usable security challenge must address the question of “How do we build and deploy systems that are easy to use, easy to manage, that result in cost savings?” (P16).

5.4 Overcoming Perceptions that Security is Dull and Not Relevant

Another negative perception, voiced by 19 participants, is that security is boring, not relevant, not of concern, or not worth the investment. This drives apathy in users adopting good security behaviors.

Participants expressed that security can be boring to less technical audiences, especially when a technologist fails to frame it in terms the audience can understand. This impression is exacerbated by security professionals who present material in a lackluster fashion that risks losing the attention of their audience, even if the material is valuable. One participant had observed “presentations where the speaker’s doing monotone and talking security. If you really love it, you can get through those, but for normal people, they’re torture” (P08). Additionally, security can be viewed negatively after exposure to typically uninteresting organizational annual security awareness training as described later in Chapter 6.

Besides disinterest, people may be apathetic towards security because of not understanding their personal vulnerability and responsibility. A security awareness director expanded on this: “if people don’t understand why and how this affects them, they’re simply not going to comply with whatever initiative it is you’re trying to roll out” (P14). Another participant discussed how security is not something most people take under consideration when acquiring a computing device: “We don’t want secure,...we don’t even want to think about it. [We want] pretty, functional, cheap”
Lack of concern may be partially due to a “belief of it won’t happen to me. It’s like I’m a great driver, so I can text while driving because it won’t ever happen to me, so I don’t have to worry about it” (P21).

Security may also be seen as an unwelcome, unnecessary inconvenience. For example, one participant lamented password policies: “You force them to change their password. We all hate that” (P28). Another commented on the lack of desire to dedicate time to security practices: “I think for end users, it’s just nobody wants to spend their time doing security. That’s not what they signed up for when they bought a computer” (P07).

Advocates commented that organizations may also be apathetic to security because it can be hard to show clear return on any investment. Security measures are preventive in that they are implemented to lower the likelihood of some unwanted event occurring in the future (Rogers, 2003). Therefore, it is hard to measure prevented events because they typically cannot be observed. A participant discussed this challenge, remarking, “It’s hard to prove that it’s working for you. Is it working because you’ve done such a good job and you’ve invested in all the right places, or is it working because you’re just not the target today?” (P05). An advocate working at a non-profit observed:

“One of the other trends that we see…is that of cyber fatigue in the boardroom: people constantly asking for more resources, yet they can’t guarantee any form of security. There’s no real return on investment, and it seems to be a black hole that we pour money constantly into” (P27).

Cybersecurity advocates attempt to overcome boredom and apathy by incentivizing security behaviors and using engaging communication techniques.
5.4.1 Incentivizing Security Behaviors

Seventeen participants mentioned that successful advocates must be able to persuade their audience to practice good security behaviors by appealing to both intrinsic and extrinsic motivations. A former security awareness director reflected, “I really want to get people to want to do security instead of having to” (P21).

5.4.1.1 Selling Security

Advocates believed, in effect, that they must market security in order to motivate people to take appropriate security actions. A participant commented on the importance of marketing skills: “you have to be able to make a...good case...that’s based on good data, that the dollar figures support, and that you can get excited and get them excited about. And if you can’t...market that, you can forget it” (P03). One advocate had an interesting and honest perspective on his use of persuasion: “I am trying to drive them to make themselves more secure by using various argumentative techniques, and, in some way, that’s manipulating them. But if you’re manipulating somebody for their own good, that’s not wrong” (P10).

As discussed earlier, having context awareness was viewed as critical to being able to sell security in terms that the audience understands and cares about. One advocate observed, “you need to be able to be flexible in terms of adapting your argument to their particular needs” (P06). Another commented: “It’s not a one-size-fits-all approach. You could take a given security concern and have to frame it four or five different ways depending on who you’re talking to” (P02). As an example, a security consultant was having a difficult time convincing an executive to spend resources to implement HTTPS for his company’s website. However, when the consultant mentioned that Google ranks
websites using HTTPS higher in its search results, the executive immediately changed his mind since “Their biggest business risk was not being on the first page of Google” (P10).

Ten participants said that they must also be able to communicate the reasons behind their security recommendations in order to convince their audience of potential benefits. An advocate stressed the importance of providing concrete reasoning: “We gotta stop leading with ‘what’ and start leading with ‘why.’ Like why does this matter? If you get someone to care why, they’ll seek the what and the how” (P11). Along this vein, for those advocating within an organizational context, establishing the business drivers for security is essential. A participant with past experience as a business executive believed, “we should be concerned with selling security as mission assurance, revenue assurance, reputation assurance” (P02).

Interestingly, three participants thought that lessons learned from persuasion within the public health field could inform the security advocacy field. An IT executive commented:

“It has struck me that we have not leveraged the hundred plus years of research in public health to really garner how to change people’s behavior effectively. How do you teach people to wash their hands? How do you teach people to do the handful of basic things that we know will solve 80% of the problems is the hard part of this” (P18).

A non-profit security evangelist echoed this thought, saying that public health is “well-defined, it’s a social expectation, and you know that it provides value even though you
probably can’t quote the actually medical studies...You should just do it. We’re not to that stage yet [in security]” (P04).

5.4.1.2 Creating Reward (and Consequence) Systems

My results suggest that advocates encourage a culture that incentivizes security adoption. As mentioned earlier, advocates discussed that showing return on investment in security can be a challenge. A non-profit director saw his role influencing public policy as critical to creating an economic reward structure for organizations to practice good security: “Most of these people are not doing what they ought to be doing with cybersecurity for economic reasons. And so we need to find ways to make cybersecurity more economically attractive to these people.” (P06).

Several participants saw economic incentives as only part of the solution in that they need to be coupled with appeals to the values of the audience. For example, one participant discussed motivating secure development practices, not by framing in security terms, but in terms developers care about, such as “you can avoid unplanned, unscheduled work, you’ll be on time, on budget, you’ll reclaim 20% boost in developer productivity across the calendar year. You’ll get your bonus, you’ll crush your competitors” (P11).

Analysis uncovered a tension regarding negative reinforcement strategies based on audience type. Three participants pushed for more accountability with negative consequences for organizations that experience serious security breaches that result in the loss of sensitive, personal information. However, three others believed that negative incentives were not useful from an end user perspective. A security awareness director at a large university opined that these kind of incentives are “completely the wrong way to
approach things in security. It’s all about education. It’s all about driving awareness, raising awareness, and getting people to understand the importance of security through non-punitive measures” (P14). Another participant felt that simple, positive incentives could be effective, but observed:

“security teams generally have a lot of history and best practice in negative behaviors...We have very few examples where, ‘Here are the compliance requirements. When you meet or exceed this, we will reward and recognize you as being a champion’...It doesn’t have to be monetary, it can be a thank you” (P21).

5.4.2 Using Engaging Communication Techniques

To overcome feelings that security is boring and irrelevant, advocates attempt to make their communications engaging and relatable while varying communication channels.

5.4.2.1 Exhibiting Enthusiasm

To overcome disinterest, participants felt that modeling enthusiasm for security to their audience captures their attention and promotes greater engagement. This was not difficult for the participants, considering 18 expressed passion for their role as advocates. The director of a non-profit commented about his passion: “I believe in what we’re doing” (P06). When asked about effective security advocates he had encountered in his career, a security engineer mentioned those for whom “you can really feel the energy that they believe in it” (P12). Another participant expressed the importance of having passion for her work when she remarked, “I can’t sell something I don’t believe in. I
can’t sell something I don’t like. I mean, I’m not going to sit and lie to you. And so, I am passionate about it” (P03).

5.4.2.2 Making Security Relatable

Findings reveal that advocates also overcome apathy by making security relatable, described by one participant as putting “the personal use and behavior in it so that people own what you’re telling them” (P28). To do so, they often used rhetorical devices in both written and oral communications to convey meaning and persuade people to take action. Among the rhetorical devices mentioned were anecdotes and narratives (8), analogies and metaphors (4), imagery (3), alliteration (2), and pop culture references (2).

Narratives might involve stories about hypothetical, but plausible scenarios, or actual occurrences of security-related incidents. One advocate liked to share stories about her own experiences since she believed, “Personalizing the message is useful, seeing that this happens to real people” (P07). Another discussed how he shares stories of things that have happened to others, for example “a person whose money might have been stolen out of their bank account because of the poor security they did at home, not because of what the bank did, but because of what they did” (P05). Four advocates mentioned how leveraging narratives of current events can serve as “an opportunity because [the audience’s] awareness is already heightened” (P24).

Advocates also use analogies and metaphors to relate security to situations and phenomena that are more familiar to their audience. For example, the analogy to public health and basic hygiene (e.g., washing your hands, brushing your teeth) was mentioned several times to explain the concept of cyber hygiene (basic, fundamental security practices). This was described by one participant:
“Do you tell someone to exercise and get enough sleep, or do you wait until they are having some serious problems and then you’re going to bring them in for surgery? Which route would you rather go? It’s not exactly the same, but it’s kind of analogous to what’s going on there [with security]. And it’s getting people to understand, OK, here’s your basic network health hygiene” (P08).

Even though analogies and metaphors can be useful, two participants cautioned that these must be meaningful and tailored to the audience. One participant thought that oversimplifying these “can be dangerous. You can be too glib, and it’s superficial” (P06). P08 provided a critique of a security training video that depicted someone fishing to explain the concept of phishing. He felt that such a metaphor was “cornball” (trite and unsophisticated) and wouldn’t resonate with his audience of attorneys.

Imagery and visual representations were also regarded as valuable in making complex topics more relatable and memorable. For example, after the Heartbleed vulnerability (US-CERT, 2014) was announced, one participant said, “I was trying to explain that and ended up using a cartoon to explain a very complex topic to people” (P25). Another revealed, “When I start talking about two-factor authentication, I like to call it two-raptor authentication. I like dinosaurs. It’s more fun when you imagine that they’re going to eat someone’s face off. People will remember the name of the feature” (P23).

The participants used a variety of platforms to peak interest and advocate for security. The most mentioned communication channels were: written materials (e.g.,
books, papers, frameworks, newsletters) (18); small group/individual face-to-face interactions (17); large forum and conference presentations (16); social media (12); and formal classroom training (9). A few participants utilized particularly unique communication channels. For example, three had developed or used games to teach security concepts. One organization sponsored a food truck event for their employees during which people standing in line for their lunch were engaged with security trivia. Another creative idea was putting a vinyl security-themed wrap on a public bus: “it becomes essentially...a traveling billboard” (P26).

5.5 Chapter Summary

This chapter begins to uncover cybersecurity advocates’ work practices related to how they motivate their audiences to engage in beneficial security behaviors by overcoming people’s negative perceptions that security is scary, confusing, and dull. My research findings revealed that advocates must first establish trust with their audience and address concerns by being honest about risks, while striving to be empowering. They address confusion by establishing common ground between security experts and non-experts, educating, providing practical recommendations, and promoting usable security solutions. Finally, to overcome perceptions that security is uninteresting, advocates incentivize behaviors and employ engaging communication techniques via multiple communication channels.

The negative perceptions discussed in this chapter are primarily personally-held challenges that advocates encounter when working with individuals inside and outside of organizational contexts. Chapter 6 continues to enumerate challenges to security advocacy identified in the interview study but from an organizational perspective.
6 Interview Study: Organizational Challenges to Cybersecurity Adoption

The majority of interview participants worked to enable positive security behavior change within organizations. Participants suggested that this is not a trivial task, especially when considering the many facets of organizations. Prior work, such as Oltsik (2016), identified challenges organizations face regarding cybersecurity, for example, shortage of security staff, lack of resources, and ineffective employee security training. A survey of company executives identified additional challenges such as the isolation of cybersecurity functions, failure to incorporate cybersecurity into business strategies, and executive board members not taking responsibility for cybersecurity (EY, 2018).

These investigations, although valuable, have not identified the specific challenges identified by those performing the cybersecurity advocate role, who have a different perspective than most cybersecurity professionals. To be successful, advocates must be deeply attuned with organizational relationships and contexts, including culture, people, and external influences. Therefore, they are in a unique position to observe where and why their efforts receive resistance.

In this chapter, I first describe organizational barriers to cybersecurity adoption as expressed by the interview participants. I then discuss ways in which advocates attempt to overcome those barriers. This chapter addresses the following research questions:

RQ2: What techniques do cybersecurity advocates use to encourage security adoption?

RQ3 (partially): What are the rewards and challenges experienced by cybersecurity advocates?
6.1 Challenges

The following do not represent a comprehensive list of all challenges to cybersecurity adoption, but rather those mentioned in the interview study as those viewed by participants as being significant obstacles to the work of cybersecurity advocates.

6.1.1 Weak Security Culture

Lack of a strong organizational security culture may serve as a barrier to organizations implementing security measures. Several differences in challenges related to security culture and mindset were observed by participants dependent on the sector (higher education, government, or commercial) described by participants. Exploration of culture in each sector illuminates context-specific incentives that must be considered by advocates depending on their target audience.

The environment of higher education poses a special challenge to cybersecurity advocates who must balance security restrictions with support for open collaboration. A CIO of a large university described how the academic research culture was sometimes at odds with the security team:

“*We have a history of not wanting to do anything that would impinge upon academic freedom. And so there are some issues around collection and preservation of log files and things like that where we gotta be thinking about what’s our values and what would we do or not do*” (P18).

Quite differently, government organizations are more formally structured and controlled. Organizations that deal with highly sensitive information naturally tend to be more security-conscious. However, other agencies that handle unclassified data or have
time-sensitive missions may see security as an impediment to day-to-day operations, failing to recognize that security can be an important enabler. Their focus is on successfully executing their mission, while supporting functions, such as IT and cybersecurity, may be seen as lower priorities. A cybersecurity expert who routinely worked with government agencies expressed this as “operations trump security all the time” (P01). Another commented about his efforts trying to communicate security concerns to senior government officials:

“I found them to be more dismissive of the problem. ‘Well, we have to get the job done. We have the mission.’ Or... ‘it’s unclassified information, so why do I need to protect it?’ And not always understanding that taking those bits of information from different places can paint a pretty enriched picture of what our government’s trying to do” (P05).

Conversely, the commercial sector is largely focused on profit, with security considerations sometimes yielding to time-to-market schedules. An advocate who worked with corporations noted that the mindset of most companies is that security is a hindrance to profit, and not yet seen as a “competitive advantage” (P27). A consultant commented on cybersecurity being an afterthought: “The economics make us push solutions faster so that we can get them out there, get market share faster, and then we’ll figure out security later” (P10).

Participants also discussed how organizational structure can negatively impact security culture. Of particular interest, several noted that an organization’s view of security can detrimentally influence how organizations position security tasks and personnel within the organization’s structure. For example, a security awareness
professional said that “segmentation is...death” (P09) because it interferes with the
“communication, collaboration, and culture” that are necessary to form a strong security
culture. Another participant who often conversed with company board of directors
commented:

“If you’re a business, you got a legal department, you got a marketing
department, you got a finance department, you got a human resources
department, executive suites. Cybersecurity cuts through all these things.
But in most organization...they still think of cybersecurity as IT. So, the IT
guy is in charge. And so people for the most part don’t own their own
security” (P06).

6.1.2 Economic Barriers

Economic reasons, including unclear return on investment (also discussed in
Chapter 5) and lack of budget/resources, were the most mentioned organizational barriers
to cybersecurity adoption (19 participants). Said one participant:

“most of these people are not doing what they ought to be doing with
cybersecurity for economic reasons. And so we need to find ways to make
cybersecurity more economically attractive to these people. And that’s
complicated because the economics of cybersecurity are so upside-down
and so poorly understood” (P06).

Participants noted that some organizations, especially small businesses, are
constrained by lack of resources to purchase security technologies and hire qualified
security professionals. Public-sector (government) and non-profits can be especially
constrained by budget. A CISO of a U.S. state government discussed this challenge: “it’s
easy to say, ‘I need more money’ or ‘I need more people.’... And maybe in the private sector people...get the extra people, get the extra dollars. But we just can’t do that easily in our space” (P26).

Even when funds may be available, organizations may be reluctant to allocate resources to cybersecurity because it can be hard to show value. Because security technologies are preventive, it can be difficult to measure their impact. One participant described this challenge from the perspective of organizational decision-makers: “How do I know that I’m getting a good return for what I’ve spent maybe millions of dollars on? That’s a really hard problem for today because, you know, in a perfect world, if you’re doing security well, nothing’s happening” (P05)

Even if the importance of cybersecurity is understood, there is a point at which investing in security does not make sense from an economic perspective. This was expressed by a non-profit advocate when he mentioned his experiences with executives who say, “I care about security, but I’m not going to bankrupt my company” (P04). Another participant described a conversation he once had with executives about security weaknesses in their company’s network:

“Their perspective was, ‘Well, what you’re telling me is that this is going to cost me probably 10 million dollars to address all the problems that you found...But, if I lose the information, it’s going to cost me one million dollars. For me, that’s a pretty easy return on my investment and the decision for me to make.’” (P05)

He continued about how this perspective was one that cybersecurity professionals often do not share, but should be aware of: “We tend to think about it very much from the
purist perspective…Very different than a CEO running a company who really thinks about it from that what’s the return on my investment here?” (P05).

6.1.3 Cybersecurity Workforce

The cybersecurity workforce within an organization can pose a challenge to security adoption. Skilled security staff may be in short supply, leaving organizations struggling to keep up with security demands. Study participants lamented that the existing workforce may lack the skills necessary to implement security correctly and to communicate the importance of security to all layers of the organization. Advocates also observed that many security professionals hold strong-held negative biases against end users in their organizations, which results in an “us versus them” mentality.

6.1.3.1 Skilled Workforce Shortfall

Just under half of the participants noted that the lack of skilled security professionals, including those competent in advocacy, creates security adoption challenges for organizations. These organizations often have trouble finding enough qualified professionals to address the myriad security issues they face. One participant noted, “small organizations may not even have full-time security staff and people who know what they’re doing” (P07).

Participants thought that even the current workforce may be lacking in the skills needed to be successful. Security professionals require competencies beyond knowing the typical “laundry list” of technical skills present in much of today’s cybersecurity curricula (Dawson & Thomson, 2018). A government security expert discussed his opinion that the current paradigm for cybersecurity education is deficient in fostering strong critical thinking skills and foundational understanding of security mechanisms. This deficiency
leaves professionals vulnerable to their skills becoming obsolete when technologies and threats inevitably change:

“There’s this desire to train up people and give them lots of rules, but a lot of the people who are just trained up don’t understand the reasons for the rules. So they’re not able to evaluate what needs to be changed and what doesn’t need to be changed…I think that a lot of the problems that we have with the security professionals is that it’s really hard to stay up-to-date. And it’s harder to stay-up-date if you’ve learned a series of things to do rather than learn underlying principles for making decisions” (P16)

Being a cybersecurity advocate capable of facilitating real change requires an even more nuanced skillset that includes not only technical skills, but also non-technical, “soft” skills, as discussed earlier in Chapter 4. However, participants observed a lack of these non-technical skills within the security community as a whole. One advocate remarked, “We’re terrible at empathy. If you broaden that, we’re terrible at soft skills. We’re very mono-cultured and bring technical solutions” (P11). A security awareness advocate observed that many professionals “struggle with something called ‘curse of knowledge.’ So, they understand technology and problems so well, they have this assumption other people must understand it also. They project that assumption. And as a result, they communicate in rather confusing terms” (P09). Another participant lamented the dearth of people prepared to do advocacy work and recommended:

“We have to have a whole army of advocates...who are skilled enough in the organizations themselves, with the right amount of responsibility and
authority to be able to carry it off. It’s one thing to talk a good ballgame.

It’s yet another to be able to pull it off” (P01).

Lack of gender and racial diversity has often been cited as a contributor to the cybersecurity workforce shortage as discussed in section 2.4.1. Several participants did indeed mention lack of diversity as a challenge to organizations employing enough skilled professionals. However, surprisingly, only one participant (a male) explicitly expressed concern about the lack of women in the workforce: “the gender imbalance is a concern...And that’s because we need the help. There’s just not enough information security practitioners” (P10).

The remaining participants who commented on diversity instead spoke about lack of diversity of thought. For example, P23 commented on the need to bring in people with more economic and life experience diversity to help design security technologies that are usable to a larger population of users. Another participant expressed, “I also feel like the security industry as a whole just needs more input from outside...We don’t have enough diversity of thinking,...different specialties and backgrounds coming into this space” (P21).

6.1.3.2 Failure to Consider the Human Element

Participants believed that many security professionals are out of touch with the human element of security. As one participant reflected, “I think security’s a human problem...And we’ve just forgotten about that. We just think it’s just widgets and viruses, and the widgets defending against viruses” (P21).

Interviewed advocates spoke about security professionals sometimes having negative perceptions that non-technical employees in the organization (end users) are the
weakest link. These perceptions may result in an adversarial relationship between organizational employees and security staff which hinders, rather than motivates, employees adopting security best practices. One participant observed that when cybersecurity is deficient in an organization, security workers “have to blame somebody, so they’re going to blame the lowest common denominator – the user” (P03).

Security staff may fail to account for the context of employee users -- their limitations, skill levels, biases, constraints, and needs -- when developing security technologies or procedures, implementing security solutions, or educating about security. The lack of context awareness may result in solutions that place undue burden on users or assume unrealistic expectations that employees are equipped to anticipate, understand, and act wisely when faced with security decisions, when, in reality, they are often at a loss. A usable security champion remarked that security professionals “need to understand the user and that the user’s on their side, but they’re just putting too much pressure on the user, and the user doesn’t have the knowledge” (P03). A former security awareness professional commented:

“Security people as a whole have a tendency to be very arrogant and shield the knowledge to themselves and say, ‘You couldn’t possibly understand that. And when you choose not to do security, how dare you’ without spending the time to understand, ‘Let me understand the other things you’re balancing in your life so that I can try to find a way to make security more usable for you’...Security people will always know security better, but it is wrong for us expect that other people will be security experts as well” (P21).
Another participant thought that security professionals should be doing more to relieve user burden “behind the scenes” by adding other layers of defense:

“*When you start figuring out why people on the security team don’t respect users, you tend to also get into this really deep security therapy session where you figure out that they’ve actually set up...unwittingly set up the end user as their own line of defense. And they get really frustrated when that line of defense fails. And it’s like, ‘Well, wait a second. You had other options. There were other options that you could put between that layer and the person.’ And being able to really illustrate that tends to get people to wake up and stop talking crappy about users, which I think is one of the more dangerous problems that we have”* (P23).

Interview participants also acknowledged that security professionals may not be adept at communicating security information in ways that resonate with users or in a language they understand. A non-profit program director discussed less effective security advocates as being those who get “*really frustrated perhaps with the end user, saying, ‘What’s wrong with you? You need to understand this.’ Well that’s because you’re speaking a foreign language or doing something that doesn’t make sense to them*” (P24).

Another advocate believed that ineffective security awareness training is partially to blame for employees being ill-prepared to make good security decisions:

“*We give employees really terrible training, very compliance-based training that doesn’t respect their time or their intelligence, then we expect that stand up against sophisticated attackers that have all the motivation and resources. And when they do fail, like 95% of the time, we...*
say, ‘Oh, how stupid you are.’ And ‘Security awareness programs don’t work.’ And I think that’s fundamentally wrong” (P21).

6.1.4 Policies and Regulations

Cybersecurity regulations attempt to force organizations to protect their assets and data from unauthorized access or modification. For example, overarching regulations and frameworks within the U.S. Government include the Federal Information Security Management Act (FISMA) (DHS, 2019), the NIST Cybersecurity Framework (2018), and numerous government agency-specific policies and standards. Industry sectors also have standards and policies related to cybersecurity, such as the Health Insurance Portability and Accountability Act (HIPAA) (Department of Health and Human Services, 2019) and the retail sector’s Payment Card Industry Data Security Standard (2019).

The sheer number of regulations, standards, and frameworks can be overwhelming for organizations. The one-size-fits-all approach taken by regulating organizations when creating policies can cause issues for organizations with unique concerns. In addition, these policies may not provide the robust cybersecurity posture they seem to promise.

6.1.4.1 Lack of Relevance

Because of the constant flux of technology change and cyber threats, participants thought that it can be hard for policies to remain relevant, especially those at national levels. One participant commented, “policy moves glacially. The law moves glacially. Technology will always leapfrog over policy and laws” (P02). Another participant remarked:
“the traditional regulatory model is ill-suited to dealing with cybersecurity for a lot of reasons that have to do with the nature of the cybersecurity problem itself – the speed with which it happens, active attackers, international jurisdiction, all these kinds of things” (P06).

Many regulations are wide-reaching, so are unable to account for individual differences in organizations. This generalized approach can create problems:

“I think in the government in particular, they err on the side of too much security, the central planning model of security, the one-size-fits-all cookie cutter approach because it’s easier to administer up top. But the lower down you get on the totem pole, you know, various locations and groups have their own unique requirements” (P02).

Another problem with policies identified in the study is that regulators may lack cybersecurity savvy, especially those at the highest levels of government. One participant observed:

“I think too many times security is driven by regulators who don’t understand the true problems...that we’re facing. So we chase the shiny object, whether it be a particular intrusion that got a lot of publicity...And then the regulations pile on...So, they don’t focus on some of the things that can really, truly make a difference” (P05).

Another advocate spoke from personal experience about the lack of involvement of knowledgeable practitioners in U.S. cybersecurity laws:

“just seeing what it takes to get something done, how it’s influenced from outside where your practitioners really don’t get a say. You have your
special interests and lobbyists and stuff...I thought that was a real shame.

And that’s one of the things I’d love to change is to really get folks who
actually do security to put some influence on how laws are made” (P25).

6.1.4.2 Compliance-driven Cybersecurity

Participants felt that organizations spent too much time trying to decipher and
adhere to various regulations, some of which may overlap or conflict. A participant
discussed this difficulty: “There’s a gazillion different standards bodies and frameworks,
and compliance standards, and every auditor has a different opinion. So even if you had
the resources and the management will, it’s not really clear what you should be doing”
(P04). Another lamented the resources consumed by compliance activities: “We’ve got
all of our cybersecurity people over there doing regulatory compliance, they don’t have
enough time to be over here doing security. So, this is actually anti-security. This is
counter-productive” (P06).

Several participants mentioned the dangers of compliance-driven security
programs and the misguided belief that conforming with a regulation means that strong
cybersecurity has been achieved. One participant expressed his concern, likening
compliance to “driving your car using the rearview mirror because compliance is always
based on what happened yesterday” (P27). He continued:

“But if you only ever drive the car using the rearview mirror, you’re going
to miss the red Ferrari that suddenly comes out of left field. So you’re not
going to be able to avoid it...Cyber is full of red Ferraris moving,
screaming around the roads at huge speeds. Unless you have very active
situational awareness, looking forward, trying to anticipate, predict
what’s what going on, you will never avoid them. And what government seems to be doing is, I think, imposing more and more regulation, some of which isn’t bad, but some of which is probably over-stretching organizations. And I’m concerned about an increased focus on compliance” (P27).

Despite the focus on compliance, the current regulatory structure does not always hold organizational decision makers accountable for poor cybersecurity practices. One advocate said, “Some of the cybersecurity laws that have been passed in recent years were done in a way that would give blanket indemnification to a company reporting cybersecurity concerns to the government regardless of whether or not they fixed the problem” (P02).

The compliance mentality can especially be observed with employee mandatory security awareness training, which several participants deemed to be largely ineffective. Advocates observed that many organizations focus on the number of employees trained, and not on how well the training positively impacts security behaviors. A participant working in the security awareness field said that most training is “developed by auditors to be compliant, to check the box. So that’s where you got death by PowerPoint once a year” (P09). This same advocate continued, “What we have done in the past has been traditionally very compliance driven. Very little has been focused on let’s actually change behavior” (P09). An advocate who consulted with higher education institutions commented, “Even though they’re training more faculty and staff on information security issues because of compliance requirements, ...it’s hard to always be sure that your message is being heard” (P15).
Annual security awareness training tends to be computer-based, where employees watch a video or click through slides. A security engineer who had once been tasked with refreshing an organization’s security training noted that the original training “was boring...there [was] absolutely nothing to get the user to buy into security thinking” (P12). A participant who worked with security awareness professionals said, “Awareness can have a bad reputation...Developed by auditors to be compliant, to check the box. So that’s where you got death by PowerPoint once a year” (P09). An advocate who had led once led the security awareness program at a large corporation commented:

“Security awareness programs as they exist right now are one of the things that make working for a large corporation suck...It’s got to be a layer of Dante’s Hell - compliance training...I also feel like people could really benefit from having a fully capable awareness program. Because security’s something that affects everybody inside or outside of work. And we’re doing everybody a disservice by just doing it out of compliance” (P21).

6.2 Mitigation Strategies

Some organizational challenges may be viewed as insurmountable for a cybersecurity advocate. In those cases, advocates attempt to mitigate or work around the challenges as best they can. For example, a small business may likely never have the personnel and monetary resources to dedicate a substantial amount of effort towards advanced cybersecurity solutions. However, advocates can recommend tailored solutions that address an organization’s biggest risks within existing constraints. In this section, I describe how advocates attempt to mitigate the challenges they face in their work. Table
4 maps the challenges described in section 6.1 with the strategies presented in this section. Note that a mitigation strategy may address multiple challenges.

Table 4

Mapping organizational challenges to advocate mitigation strategies

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Mitigation Strategy</th>
</tr>
</thead>
</table>
| Weak security culture | 6.2.2 Making a business case (all strategies)  
|  | 6.2.3 Targeting multiple levels (all strategies) |
| Economic barriers | 6.2.1 Bolstering the cybersecurity workforce (all strategies)  
|  | 6.2.2 Making a business case (all strategies)  
|  | 6.2.3 Targeting multiple levels  
|  | 6.2.3.1 Influencing management  
|  | 6.2.3.3 Leveraging opinion leaders and champions |
| Cybersecurity workforce – Skilled workforce shortfall | 6.2.1 Bolstering the cybersecurity workforce (all strategies) |
| Cybersecurity workforce – Failure to consider the human element | 6.2.1 Bolstering the cybersecurity workforce  
|  | 6.2.1.1 Developing professionals  
|  | 6.2.1.2 Encouraging a multi-disciplinary approach  
|  | 6.2.2 Making a business case  
|  | 6.2.2.2 Tailoring guidance  
|  | 6.2.3 Targeting multiple levels  
|  | 6.2.3.2 Engaging end users |
| Policies and regulations – Lack of relevance | 6.2.1 Bolstering the cybersecurity workforce  
|  | 6.2.1.3 Building partnerships and professional networks  
|  | 6.2.2 Making a business case  
|  | 6.2.2.2 Tailoring guidance  
|  | 6.2.3 Targeting multiple levels  
|  | 6.2.3.1 Influencing management  
|  | 6.2.3.3 Engaging end users  
|  | 6.2.4 Contributing to policies and regulations (all strategies) |
| Policies and regulations – Compliance-driven cybersecurity | 6.2.2 Making a business case (all strategies)  
|  | 6.2.3 Targeting multiple levels  
|  | 6.2.3.1 Influencing management  
|  | 6.2.3.3 Engaging end users  
|  | 6.2.4 Contributing to policies and regulations (all strategies) |
6.2.1 Bolstering the Cybersecurity Workforce

Cybersecurity advocates attempt to build up the quality of the security workforce within organizations and attempt to compensate for current deficiencies by leveraging partnerships and technologies.

6.2.1.1 Developing Professionals

To build the technical skills of the current workforce, some participants actively educated security professionals by teaching higher education or professional development courses as described in section 5.2.3. Several veteran advocates saw themselves in a mentoring role. For example, a veteran advocate talked about his role guiding the new generation of security professionals:

“I’m really conscious of my role as an old guy in this, a pioneer, someone who’s got a lot of history. And so there’s an excitement to that, to feel that you’ve seen a lot of things happen, made a lot of mistakes you get to convey to other people...So, feeling responsible. I feel the role there. It feels like I’m supposed to be doing this” (P04).

Interview participants also attempted to foster non-technical skills among organizational security professionals by both modeling those skills themselves (as described in section 4.1.2) and by educating others. One participant (P09) worked with security awareness professionals to teach important skills about understanding users and developing effective training programs. Another (P23) consulted with security professionals, such as red and blue vulnerability assessment teams, on how to advocate for their own work to organizational leaders. Other participants worked in the usable
security area and tried to educate security professionals on human aspects of security so they could better understand end users (described in section 5.3.4).

6.2.1.2 Encouraging a Multi-Disciplinary Approach

Whereas interview participants lamented the dearth of non-technical skills within the security community, they encouraged the formation of multi-disciplinary teams possessing those skills to work on security advocacy within organizations and to facilitate the development more usable security solutions for end users. For example, a security educator said, “Folks who maybe have an education background, or a marketing background can find clever ways to get folks interested in learning more about security practice and perceive threats and vulnerabilities on their own” (P02). Another participant commented:

“Security people aren’t people people, but there are whole industries that are people people: marketing, advertising, psychology, game theory...So we need to be bringing in a lot more people who have expertise in other areas and start cross-collaborating and cross-pollinating and cross-hybriding our skillsets to solve the security problem” (P21).

A non-profit program manager that worked with higher education institutions agreed:

“The people who do information security or cybersecurity awareness training, they come from all over the place...They are communication professionals, or marketing professionals, or teachers. And they just come to this area and they flourish because they have a unique set of skills to do well” (P15).
A participant described the diversity of his volunteer advocacy community:

“We happen to have the most diverse participants of any cross-section you might see in cybersecurity... We have psychologists, data scientists, social work background, PR communications experts... And I don't think we succeeded in spite of those, I think we probably have been successful because of those” (P11).

Other advocates championed multi-disciplinary cybersecurity approaches that incorporate technology, business, and policy. A non-profit director who worked with corporations discussed the need to have appropriately prepared advocates in senior executive positions within organizations:

“One of the ways that we can address this shortfall in skillsets at the highest level is really to try to encourage people from outside of that security space to come into it. And they can pick up the technical skills very quickly...It’s much more, I think, today, how you can position security within the business context and ensure that you’re delivering value and, of course, gaining the trust of your board of directors to be able to do the right thing” (P27).

Another participant, who advocated for cybersecurity policy at the national level, said, “We see [cybersecurity] really as a three-legged stool that involves, obviously technology, but also involves economics, and also involves public policy. You need to weave these three things together” (P06).
6.2.1.3 Building Partnerships and Professional Networks

As mentioned briefly in Chapter 4, professional networking and drawing knowledge from the security community was viewed as vital for advocates to stay updated on the latest security happenings. In doing so, they augment the cybersecurity workforce within their organization. Participants also discussed how they facilitate information sharing, which benefits not just their own organization but also advocates’ audience organizations which may not have the security workforce to develop their own security plans and policies. For example, one advocate talked about her non-profit security advocacy group:

“We bring information security professionals in higher education together, both virtually and in face-to-face meetings to discuss current information security issues, how they conduct information security awareness at their own institutions. And we bring them together to create resources and thought leadership that can then be shared back out amongst all higher education information security practitioners” (P15).

Advocates also foster consensus building when developing relevant advocacy approaches and best practice guidance for organizations by involving external stakeholders who bring different perspectives and areas of expertise (see also section 5.1.3). One participant discussed his interactions with others in the security community: “I cross-pollinate…I move ideas around. I help to find those smart ideas, and then I try to tell other people about them. And then combine them together in different ways” (P10).
6.2.2 Making a Business Case

Participants often mentioned the need to make a business case for cybersecurity adoption, which they accomplish by “selling” the value of security, tailoring guidance to an organization’s needs, and providing empirical evidence to bolster the case. Items in this section are also described briefly for broader advocacy audiences (not just including organizations) in Chapter 5.

6.2.2.1 Selling and Incentivizing Cybersecurity

Advocates discussed the need to market cybersecurity as an enabler for the target organization’s primary mission. Framing the message was particularly viewed as critical for success. This requires an understanding of the organization and what they care about. When talking to the company board, a participant would promote cybersecurity “as mission assurance, revenue assurance, reputation assurance. We’re not always here to say no” (P02). An advocate at a non-profit commented on the importance of reframing how organizations think of cybersecurity:

“…what I always tell organizations is information security, to be successful, needs to move out of what I always call the cost bucket. So, it needs to be stopped being viewed as a cost. Because if it’s a cost, then the message that is sent to the business is that it is something to be reduced. It...needs to move into being a strategic support arm for the business. If it can do that, barriers suddenly vanish overnight, resources miraculously appear” (P27).

To sell cybersecurity, advocates attempt to incentivize cybersecurity adoption by appealing to organizational values, which for industry organizations is typically profit and
reputation, and how cybersecurity could protect those values. They may also try to incentivize by placing a monetary value on how much cybersecurity measures could save an organization. A participant who taught security teams how to advocate for themselves encouraged her clients to

“start looking at it from an incentive perspective...If you are having a specific problem where passwords and credentials are causing a huge number of attacks, you either have to talk about how much those attacks are costing you and how many more resources you’re going to need, or you’re going to have to look at the solution and say, yes, it’s going to cost what we would spend on two people to manage this problem full time, but in the next 2-3 years it would save us this much money” (P23).

6.2.2.2 Tailoring Guidance

When making a business case, context awareness was seen as being key. Advocates thought it was important to be attuned to the unique environment of the organization and realistic about what can be done within an organization’s resource constraints. This awareness then translates into the development of practical, prioritized guidance. The guidance must be achievable, useful, and perceived as reasonable by security staff and employees. One advocate expressed her philosophy:

“You’re never going to be able to remediate or mitigate every single information security risk that you have, but you should be able to identify the ones that are the most likely and the ones that would be the most devastating to your environment, and take steps to mitigate those risks” (P15).
Tailoring was seen as especially important when applying broad policies at the government or national level within organizations. For example, when discussing overarching, one-size-fits-all policies, one participant remarked, “You’ve got to tailor security and sell security in a way that recognizes the variations between locations or entities or mission goals” (P02).

6.2.2.3 Providing Empirical Evidence

As discussed earlier, participants expressed that good measures of effectiveness can be difficult to develop but are critical for demonstrating an organization’s current security posture, identifying security needs, tracking progress over time, and demonstrating success. A CISO of a state government discussed the value of data when meeting with high-level local government officials who ultimately make decisions on where to allocate security resources: “We can show up to those meetings with some data in hand to help them understand where their greatest risks are and work together to help them mitigate those risks” (P26).

Reliable measures of effectiveness to gauge the success of security advocacy efforts may be even more elusive yet advocates still must look for opportunities to obtain these. For example, advocates who run security awareness programs within their organizations may test their staff members’ security behaviors via phishing exercises. Participants thought that the metrics from these exercises can provide some marker of improvement or problem areas on which to focus. Believing that organizational security culture can take years to change, one participant discussed how an organization’s security incident data, such as “exposing of sensitive data, use of ID badges” (P09), can be tracked as a preliminary way to start measuring success. Other metrics, such as
attendance numbers and views of videos, can also be an indicator of reach. Metrics are also discussed in the context of advocate motivation in section 4.2.

Demonstrations of vulnerabilities via in-house or third-party penetration testing are also viewed as powerful tools for cybersecurity advocates. Penetration testing involves finding and often exploiting vulnerabilities within an organization’s network or products. The identification of vulnerabilities can be an indicator of the need for greater security adoption or can measure improvement in security posture over time. One participant discussed how, even after other attempts at convincing company leaders to implement certain security measures failed, “the trump card has always been a successful penetration test” (P19).

6.2.3 Targeting Multiple Levels

Participants believed that obtaining cybersecurity buy-in at all levels of the organization is necessary for sustained success. Interview participants discussed ways in which they enlist the support of organizational leaders (managers and opinion leaders) as well as employees.

6.2.3.1 Influencing Management

Sixteen participants discussed the necessity of gaining management buy-in. This top-down approach is critical for establishing security culture, allocating needed resources, and enforcing security policies. Said one advocate, “if you don’t get some senior buy-in ... then it won’t sustain over time because the technologists move on, things will change, pressures will come” (P05). Advocates expressed that being successful requires convincing organizational leaders of the business case (section 6.2.2) and their
responsibility for cybersecurity. One participant often presented at leadership training courses about

“why security and understanding risk was a key part to being a successful executive in the company because you need to be able to balance growth and employee happiness as well as risk…it’s about the risk you choose to accept on behalf of the company” (P21).

Another advocate discussed his non-profit’s approach when working with corporate boards:

“Corporate directors don’t want to learn about IT...They talk about mergers and acquisitions and new product developments and things. So what we did was we embedded cybersecurity in those conversations. So the approach we took was, if you’re considering a merger or acquisition, what are the cybersecurity questions you need to be asking? When you’re launching a new product and developing a new supply chain, what are the cybersecurity issues?” (P06).

6.2.3.2 Leveraging Opinion Leaders and Champions

Interviewed advocates felt that, while gaining management buy-in is important, it may be initially difficult to do so because of lack of access or cybersecurity/IT literacy.

Therefore, advocates may need to leverage opinion leaders and champions within organizations to obtain broader buy-in from both employees and organizational leaders (also mentioned briefly in section 5.1.4). Diffusion of Innovations Theory observes that adoption within organizations is often facilitated through internal opinion leaders (well-respected individuals) and idea champions (Rogers, 2003). This observation was
supported in the advocate interviews. Engaging opinion leaders and champions can be particularly helpful when the advocate is an outsider to the organization. One participant discussed his reasoning for trying this bottom-up approach:

“There’s times where we tried to influence by hitting the senior level decision makers, but they don’t understand the problem. So, you might try coming in at a lower level where...the technologists can understand, and they can help drive up instead of it being driven down” (P05).

Another talked about how she identifies champions:

“I think we tend to go by we need to talk to somebody with a title, and I don’t think that’s always the case. I think you got to find the person who’s excited about it, who’s passionate about it, who’s connected” (P03).

6.2.3.3 Engaging End Users

Participants spoke about the need to treat employees (end users) as partners, rather than adversaries, in cybersecurity. Therefore, advocates attempt to empower users to make informed security decisions via awareness and education efforts aimed at influencing attitudes and behaviors, not just meeting compliance requirements. They also advocate for users’ needs by first practicing active listening to collect and better understand user challenges and concerns. Advocates then take these needs under consideration when developing and promoting usable security solutions and processes. Chapter 5 contains a detailed discussion of advocacy techniques used to educate and empower individuals – in this case, organizational employees.
In addition, from an organizational perspective, three participants discussed tying work security behaviors to home behaviors in an effort to make security more personally relevant. This approach was described by a security communications consultant:

“The focus tends to be really about protecting the corporation where I think, given the fact we have no space in public school curriculum or even college where people learn about how all of this stuff works, it would be a lot better if the focus was on the personal part because, for one, it would improve people’s lives no matter where they go...if you have the bandwidth from a corporate perspective, why not make sure you are encouraging people to make better decisions in their time off and make it not about the company at all” (P23).

6.2.4 Contributing to Policies & Regulations

To counter obsolete, restrictive, or complex regulations, several participants talked about how they contribute to policy creation (also mentioned in section 4.2). Influencing policy can be a force-multiplier for advocates’ efforts since policies often reach a broader audience. P06’s non-profit lobbying group affected large-scale U.S. government cybersecurity strategy: “We needed to change the economics of the system through public policy so that we could incentivize appropriate cybersecurity” (P06). Another participant worked to influence regulations for life-critical products (e.g., medical devices):

“...we’ve been using those ambassador muscles to drive pretty substantive change in [U.S. regulatory organizations], other pockets of government domestically, internationally...We wanted more bandwidth and more lift
and thrust than just a grassroots, 100% volunteer thing. Idea was an international policy accelerant to the grassroots might be necessary” (P11).

Three advocates talked about their work trying to influence the auditor population to think about compliance in a different way. One participant commented about her efforts:

“auditors have driven the way the programs exist today because they ask, ‘How many people have completed training?’ as opposed to, ‘Show me what has happened since you’ve done this training.’ And if I can influence those people to ask a different question, the downstream impact in the community will be different” (P21).

6.3 Chapter Summary

This chapter describes organizational challenges to cybersecurity advocacy and the strategies advocates use to mitigate those. Challenges identified in the interview study include weak security culture; economic barriers such as lack of resources and difficulty showing return on investment for security; cybersecurity workforce shortfalls and security professionals failing to consider the human element when implementing and recommending security solutions; and policy issues pertaining to relevance and compliance-driven security. Advocates attempted to mitigate these challenges by leveraging their technical and non-technical skills to educate others, build consensus, and develop professional networks. They tailored their approaches to multiple levels of staff within the organization and incentivized their audience by making a strong business case for security adoption.
The identification of organizational challenges in the broader interview study lays a foundation for comparison for challenges encountered by the security awareness team in the case study as discussed in Chapter 8.
7 Case Study: Context

As a foundation for examining cybersecurity advocacy in Agency A, this section provides descriptions of the organizational environment, security awareness team, and security awareness approaches. Details of approaches are provided in Chapter 8 as evidence of how the security awareness team is practicing cybersecurity advocacy and transforming the security awareness program.

7.1 Agency Description

A high-level, rather than a detailed, organizational description is offered in this section in order to protect the anonymity of Agency A.

7.1.1 Structure

Agency A is a medium-sized federal government agency of approximately 4000 employees (federal and contract employees). Most employees are stationed at Agency A headquarters in the Mid-Atlantic region, with smaller contingents located in several regional offices throughout the continental United States. Staff at these remote sites serve as liaisons to regional stakeholders and local governments.

The agency headquarters consists of multiple operational mission offices along with several staff offices (e.g., Office of the Chief Information Officer, business office, public affairs). The agency is outward-facing; its mission involves producing guidance for and regulating external stakeholders operating critical infrastructure. Sensitive information is often produced, disseminated, and stored by agency employees.
7.1.2 Security Culture Expectations

Security culture is “the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security” (Centre for the Protection of National Infrastructure, 2019). An overview of the security culture, including what the organization expects of employees, was gleaned through interviews of security awareness team members, managers, and employees. Note that these are the perceptions of a small sample of agency employees and may not represent the overall culture. An in-depth analysis of the security culture is out of scope for this research. However, perceptions are useful in framing how security awareness efforts are received by employees.

Participants generally believe that the agency views cybersecurity as a high priority. An attorney commented that Agency A “puts cybersecurity pretty high on its list” (E5). Another believed that security is

“valued because it is absolutely necessary that the information that is contained within our organization, as well as in the federal government, is maintained in a manner that is appropriate and secure. And that’s to protect not only the information that is needed by the federal government to do its work, but also to protect members of the public” (E3).

The interviewed managers, both of which work within the CIO office, voiced similar opinions: “I think because of our industry, people are security-conscious” (M2).

When employees were asked about the expectations placed on them by the organization with respect to security, all felt that they have at least some responsibility for security. General statements about security expectations included “being aware of
your surroundings, being aware of what you're clicking on. It's everybody's responsibility” (E7) and “protect information consistently” (E5). A research librarian said, “They expect us to recognize the spam email and not to click if it’s a suspicious email” (E1). An attorney believed that agency workers were expected to be aware of “what we're sending out in terms of emails and attachments and opening attachments” (E6). The leader of a research resource team held a more comprehensive view of employee expectations:

“Each employee is responsible for ensuring that the information that we have access to is protected in the manner that it's governed. And whether that means just powering down our computers so that someone can't accidentally view something they shouldn't, protecting written work, whatever the case may be. Or just being aware of the attacks that could be coming in through the electronic devices that we use and making sure that we're alerted to that, that we're educated, and can participate in a good manner, and question when we're not sure. And question those that know more, that can provide us with a good answer even if we're erring on the side of caution. So, everyone that is a member of federal government has that role. And I know that we take that role seriously” (E3).

However, some participants voiced concerns with respect to how advertised security culture expectations match up to reality. These concerns are discussed in greater detail in the context of the agency’s organizational challenges as described in section 7.5.
7.2 Security Awareness Team

This section contains a description of the security awareness team and program at Agency A, including placement within the agency, mission, team composition, how the team stays relevant, and general approaches to security awareness.

7.2.1 Placement within the Agency

The security awareness team is housed in a cybersecurity oversight organization under the Office of the CIO. The organization is responsible for developing cybersecurity policy implementation procedures and guidance and often serves as a liaison to other organizations in the agency by answering cybersecurity questions and helping programs be compliant with government cybersecurity requirements, such as FISMA (DHS, 2019).

7.2.2 History

There was little record of the history of the security awareness program beyond what was captured in the case study interviews with managers and the security awareness lead. However, the program appears to date back to at least 2009. Back then, the program focused mainly on training compliance, for example ensuring annual cybersecurity awareness training was completed by agency employees and additional classroom training requirements were met for those employees with a cyber role. The previous security awareness lead retired about three years prior to the case study. At that time, the current lead took on this role. Further discussion on how the program has undergone a transformation during the past three years can be found in Chapter 8.

7.2.3 Mission

The security awareness team has three primary responsibilities. First, the team implements and tracks the completion of annual security training for the entire
organization. This security training is mandatory for all agency employees and contractors per FISMA and other U.S. government directives. The online, computer-based training typically is interactive and walks employees through different security scenarios and how to respond appropriately.

The team also plans and executes security awareness initiatives (the focus of the case study) throughout the agency to increase employee awareness of security issues and educate them on appropriate security actions. Approaches include phishing exercises, handouts, events, and other avenues such as agency-wide campaigns. Team members are responsible for developing security awareness themes and coordinating logistics.

Finally, the team manages, coordinates, and tracks role-based training. Role-based training is required for any employee with a cybersecurity role (e.g., IT security specialists and information systems security officers) as well as senior executives. Role-based training tracks follow a repeating three-year cycle. During year one, role holders attend cybersecurity classroom training taught by a contractor and customized for specific roles. During years two and three, role holders are required to attend vendor or external training. This type of training can also be fulfilled by attending various agency security awareness events:

“We give people credit towards their annual computer security awareness training, to their role-based security training requirements, for getting out and listening to things that they should be doing as part of their job.

Going to a classroom where you’re hearing something theoretical or about a specific product, we feel, isn’t as beneficial as getting out there
and understanding why it's important to secure things and how to get that mode of thinking into your everyday activities” (M1).

The tasks of managing the annual security training and role-based training programs are baseline operational activities executed by federal organizations and represent the emphasis of compliance within the government. These programs are important because they are the source of the security awareness team’s legitimacy and funding. However, they do not represent the advocacy function. I captured information about these activities in order to put the team’s advocacy efforts in context; mandatory training was never the focus of my analysis.

7.2.4 Team Composition

The security awareness lead (S1) is the primary cybersecurity advocate within the team, serving as the driver, decision-maker, and public face of the program. Two contractors (S2 and S3) support the program on a full-time basis. Government staff and contractors working together cannot officially be called a “team,” although S1 views them as such since “it helps build ownership in the process” (S1). For simplicity, the three individuals performing security awareness tasks will be referred to as the security awareness team throughout this document.

The team lead has over 30 years of IT and cybersecurity experience with a formal degree in business administration and computer programming. He has been at Agency A for about 20 years, the first five as a contractor. He spends about 50% of his time leading the security training and awareness program, a role which he views as “the most important thing I’m doing right now” (S1). Upon taking the lead role for the program three years prior, S1 took immediate ownership and steered the program in new
directions even though he was new to training and awareness: “if you’re going to put me in charge, I’m going to take command and I’m going to make it successful” (S1). In addition to his awareness and training duties, S1 also works with information system owners on system authorizations and serves as the agency subject matter expert for government cloud services and data analytics.

S2 and S3 are contractors supporting the awareness and training program on a full-time basis. They are heavily involved in the creative process of event planning. These team members also handle logistical and administrative tasks such as tracking security training requirements and completion, securing space for events and classroom training, inviting speakers, coordinating with other departments (e.g., audio-visual and graphics), marketing the events, tracking attendance, and broadcasting events to remote sites.

Other agency staff within the organization support the team on a limited basis. Contractors conduct phishing exercises, create dashboards, and serve as instructors for role-based security training. Although not officially resourced to the security awareness program, several government security personnel are embedded into different agency mission elements and help to promulgate security awareness information during monthly or quarterly meetings with element staff.

7.3 Security Awareness Events

The team regularly holds three types of security awareness events throughout the year: lunchtime events, security officer forums, and security days. As part of the case study, I observed three lunchtime events, one security officer forum, and two security days. Table 5 provides an overview of observed events.
<table>
<thead>
<tr>
<th>Event</th>
<th>Theme</th>
<th>Attendance</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lunchtime #1</td>
<td>Holiday Security</td>
<td>100+ (in-person)</td>
<td>The event was in the information fair format typical of most agency lunchtime events. Five stations (plus an unmanned CIO table) featured topics related to holiday cyber and physical security and safety: cyber and holiday trivia; internet of things; safe online shopping; fire safety; and credit card skimming.</td>
</tr>
<tr>
<td>Lunchtime #2</td>
<td>To Send or Not to Send</td>
<td>50+ (in-person)</td>
<td>The event involved two performances of adaptations of popular Shakespeare plays to address cybersecurity concerns. The team lead read through three “acts” based off plays but re-written by the team to incorporate security themes. Accompanying presentation slides were displayed on a large video screen.</td>
</tr>
<tr>
<td>Lunchtime #3</td>
<td>Late Night Cyberside Chat</td>
<td>30+ (in-person)</td>
<td>The event spoofed a late night TV show complete with a show “set.” The team lead served as the host. Several guests from inside and outside the agency talked about IT and security topics such as the new agency Wi-Fi service, staying safe online during the holidays, and internal agency investigative services. The event also included a comedy monologue and a comedy sketch similar to Johnny Carson’s “Carnac the Magnificent.”</td>
</tr>
<tr>
<td>Security Officer Forum</td>
<td>Stop, Drop, and Lock</td>
<td>70+ (in-person and remote)</td>
<td>Followed by opening remarks from the security awareness lead and CIO, an external speaker provided an overview of the NIST Risk Management Framework and why it matters to security officers. The security awareness lead then talked about Personal Identity Verification (PIV) card security vulnerabilities and provided recommendations for mitigating those. An agency contractor demonstrated a recent security exploit and suggested mitigation actions. Finally, the team lead talked about cybersecurity role-based training.</td>
</tr>
<tr>
<td>Security Day #1</td>
<td>Cybersecurity and You</td>
<td>230+ (in-person and remote)</td>
<td>Following opening remarks by the security awareness lead and agency CIO, talks were presented by four external speakers from government and academia. Topics included privacy policies, artificial intelligence application to critical infrastructure, supply chain risk management, and assessing cyber risk.</td>
</tr>
<tr>
<td>Security Day #2</td>
<td>National Cybersecurity Awareness Month</td>
<td>200+ (in-person and remote)</td>
<td>Following opening remarks by the team lead and agency CIO, external speakers from two cybersecurity-focused government organizations spoke about their missions and how they could aid Agency A. A former FBI agent talked about cybercrime and digital forensics, telling a story about how cyber activity led to cracking a difficult case.</td>
</tr>
</tbody>
</table>
Note that, although the security awareness team has branded each type of event, to protect the organization’s anonymity, the branded event names will not be referenced. This section includes overviews of each event type.

7.3.1 Lunchtime Events

Lunchtime events are held 4-5 times a year and are aimed at the general Agency A population. These are informal, drop-in events held between 11:00 am and 1:00 pm in an exhibit area located in a main thoroughfare between agency buildings and close to a cafeteria. In the past two years, most of these events have been attended by over 100 agency employees each. Lunchtime events have a theme, which are usually related to the time of year or a topic of interest to the workforce. For example, a spring event had a “Clean Up Your Cyber Act” theme in line with the idea of “spring cleaning.” A “Safety Tech Check” event aimed to help attendees get the most out of their smartphones, laptops, and tablets while operating them safely and protecting personal information.

Typical lunchtime events involve multiple tables, or “stations,” arranged in a horseshoe configuration in an information fair atmosphere. An security awareness team member staffs a sign-in table at the opening of the horseshoe where people can get information about the event and sign in to receive role-based training credit if they have a cybersecurity role. There is also always an unmanned CIO table with a variety of security-related pamphlets and handouts available for people to take. The other stations feature topics related to the theme and are manned by agency employees or contractors, representatives from organizations in the surrounding community, or staff from other government agencies. The stations afford attendees an opportunity to speak one-on-one
with an expert to learn about that topic and gather additional information (e.g., via handouts). The team makes a point to include both cybersecurity and non-security stations as well as topics that can help employees at home and at work. The team also usually staffs a gamification table that combines the event theme and cybersecurity topics, for example, a trivia game. Small prizes (e.g., candy) are given out to attendees who “win” the game.

7.3.2 Security Officer Forums

Security officer forums are typically held twice a year and are geared towards Agency A staff with cybersecurity roles (although any agency employee can attend), particularly information system security officers (ISSOs) who are “assigned responsibility for maintaining the appropriate operational security posture for an information system or program” (NIST, n.d.). The 2.5-hour forums focus on providing updates to the ISSO community and presenting security information to help individuals grow in their role. Like the lunchtime events, security officer forums have themes that address topics of interest to those with cybersecurity roles.

Forums are held in a large conference room at Agency A headquarters and are broadcast live to the agency’s remote sites as well as to attendees wishing to view them from their offices. Security officer forums typically feature the CIO or CISO providing a brief agency security update and 4-5 talks by speakers internal or external to the organization. After the forum, recordings and presentations are posted to an internal web site for those who could not attend in-person. The past two years, forums have been experienced live by roughly 100 in-person and remote attendees per event. Attendees can receive credit towards their role-based training requirements.
7.3.3 Security Days

Security days are the largest events sponsored by the security awareness team, attracting between 200 and 300+ in-person and remote attendees per event over the past two years. The half-day events are located in a large auditorium and are aimed at all agency employees with a goal of providing the workforce with security and technology information that can help them both at home and at work. Security days are held twice a year: once in October during National Cyber Security Awareness Month (NCSAM) and once in the spring. October security days follow the NCSAM theme, and spring security days have a theme decided upon by the team. Examples of past themes include “Security from the Doorstep to the Desktop” and “How to Protect Yourself Online and Offline.” There are typically four talks (related to the theme) during the event, not including opening remarks from the team lead and the CIO or CISO. Like the security officer forums, security days are remotely broadcast with recordings and presentation slides posted for later viewing.

A number of exhibitor tables are set up in the main atrium outside the auditorium where representatives from industry vendors, other government organizations, and internal agency organizations are available to speak with attendees and provide technology and security information during breaks and after the event. At the observed security day events, exhibitor tables included an agency CIO table with security handouts, an agency representative talking about smart cards and their correct usage, another government agency with ties to Agency A, and various security and technology

---

vendors, many of whom gave out small trinkets (e.g., pens). Light refreshments are typically served in the atrium at the conclusion of the talks.

7.4 Other Security Awareness Approaches

The security awareness team utilizes other security awareness approaches, including campaigns and phishing exercises which are described here.

7.4.1 Campaigns

The team initiates focused campaigns and security awareness material distribution to address specific security issues emerging within Agency A challenges. For example, in a campaign to encourage employees to complete their annual security awareness training, the team posted reminders throughout the agency buildings. A “Click with Care” campaign encouraged safe email behaviors to address the ever-present phishing threat and an agency incident involving a sensitive email being sent to unintended recipients. The campaign sought to bring awareness and offer practical solutions to avoid “the three clicks of death: clicking on a link you shouldn’t, clicking on an attachment you shouldn’t, or clicking send when you shouldn’t” (S1). Branded campaign posters were displayed throughout agency buildings and colorful handouts outlining mitigative actions were distributed to the workforce.

7.4.2 Phishing exercises

Agency A fell prey to at least three different coordinated spear-phishing attacks several years prior to the study. The attacks resulted in about a dozen employees disclosing their agency account and password information and two other employees infecting their computers with malware. Given the sensitive nature of Agency A’s
mission, the attacks were taken very seriously. Since then, there’s been a concerted effort to educate the workforce on spotting phishing emails, not clicking on suspicious links, and appropriately using email. Agency A has quarterly phishing exercises to test the workforce’s susceptibility to phishing emails and raise awareness. The security awareness team sets the strategy for these exercises, but a contractor outside of the team constructs the phishing emails (called scenarios), sends them out via a phishing awareness and testing application, and collects statistics on click rates.

The phishing program has been in place for approximately eight years, although in different instantiations over that time. The current program, instituted in 2018, involves the entire agency population (including all contractors and remote site employees with an organizational email address) being phished each quarter. A control group of 300 people (different people each quarter) is sent a phish of the same known difficulty each quarter to gauge overall effectiveness of the program. The remaining employees are divided into two groups, with each group receiving a different email scenario. Employees who click on a phishing test email are taken to a landing web page and educated about phishing cues. Clickers have to take additional phishing awareness training in the agency learning management system within 30 days. If they do not take the training within that timeframe, they and their supervisor are sent a reminder email.

Employees are educated on how to report suspicious emails via information received in agency-wide emails, security awareness events, and campaigns. Currently, employees can attach suspicious email and send it to the agency security incident response center or help desk.
7.5 Challenges to Security Awareness Efforts

Interviews of security awareness team members, managers, and employees revealed personal and organizational challenges within Agency A that hinder security awareness efforts and the workforce’s willingness and ability to practice good security habits. The most frequently mentioned obstacles are described in this section.

7.5.1 Lack of Workforce Buy-in

The case study revealed contradictions between the agency’s advertised security culture/expectations of the workforce and employees’ actual attitudes and behaviors. Several case study employee interview participants observed inconsistencies in official security policies versus actions within the organization. For example, the manager of an information security organization remarked, “I don't know if they necessarily have a good follow through with looking at what is said in doctrine versus what is put into practice” (E2). The security awareness lead, who also has responsibility for system security authorizations, commented, “everybody says cybersecurity is the most important thing out there. Yet when it comes to something like a system authorization or system design or architecture, security is the last thing... It's not thought of in the beginning” (S1).

The team often must contend with staff that does not “buy into” (see the value of) security awareness training. This disregard may be the result of lack of awareness of security threats and how security applies to their jobs. Several interviewees believed that the older population at Agency A has not evolved in their security thinking. An employee commented, “There may be different offices and different people who have been here for quite a while where security wasn't primary” (E8). A manager remarked:
“We have a lot of folks that have been here for a very long time. They're used to dealing with the same information, the same processes. The world has changed. Security considerations have changed. The technology has changed. But a lot of our staff still fundamentally see things the way they were 30, 40 years ago, when it was a paper-based process” (M1).

The interviews revealed that those working in roles not related to IT or cybersecurity may not believe they have a responsibility for security. The security awareness lead discussed challenges convincing staff from mission offices to attend security awareness events because “we’re still in our silos. We’re only worried about what we’re worried about. We’re not looking at other things” (S1). An engineer said that security awareness event topics were not discussed among employees in his organization because “we don't do that for a living” (E4). When asked if the security awareness information has helped her to make security-related decisions at work, an attorney said, aside from recognizing phishing email, “No...it's not part of my role to do security things” (E5). Several interview participants discussed the need for better alignment between the security awareness program in the Office of the CIO (OCIO) and the mission elements of the agency in order for people to see the connection to cybersecurity:

“My opinion is that OCIO tends to look at things through that IT lens only. They don't necessarily know what the business is doing. So how that goes back to training: I think that they do a good job, but I don't necessarily believe that they're aligned completely with what the agency confronts” (E2).
Cognitive biases may also affect buy-in. Participants thought that employees may be overly optimistic in believing they would not be a victim of a security attack because “they’re just a cog in the wheel” (S1) and do not do anything important enough to be targeted. A security officer felt people may not “take it seriously until it personally affects them” (E7).

Lack of support for security training is especially problematic when leaders within the agency do not buy in and “see it as a nuisance” (S1) since they should be setting an example for the workforce. The team lead commented, “I just happened to have a training course with some leadership in the mission office. And they’re like ‘Why do I have to take this course? Why do I care about cybersecurity?’” (S1). A security awareness team member observed that some leaders think “Oh, I know everything. I’m fine. And then they go click on a link. You don’t know everything” (S3).

Because security awareness training is not viewed as valuable to their everyday duties, employees may feel it is not a priority since they are otherwise “busy doing their work...they're just trying to get their job done” (M2). Managers may not support employees attending events because they have the attitude that “I can’t afford to send my people there...They need to be here at their desk” (S1).

7.5.2 Human Error

Participants observed that, even if employees buy into the importance of cybersecurity, they are subject to emotions, distractions, and pressures that may negatively impact their security behaviors. Firstly, good security habits take time to solidify: “I’m a human just like anyone else, and if a new procedure or a new requirement comes along, it takes me a while to embrace that, to get that ingrained into
my head and my daily practices” (E2). However, even when habits are formed, errors occur. One employee acknowledged, “it’s just a matter of time before somebody makes a mistake. They’re too busy. They just woke up. They had a bad lunch. I don’t know, boss yelled at them” (E4). This same engineer doubted his own ability to make good security decisions due to his lack of expertise in that area: “I know I’m supposed to do a lot. And I do my best to do it. But I’m always kind of nervous about it. What if I make a mistake?” (E4). A manager described an instance in which the agency’s relatively low click rate during phishing exercises ballooned: “We threw out a phish that was, ‘You have a complaint lodged against you with OPM.’ And the emotional part of people kicked in, and…the click rate went through the roof on that one” (M2).

7.5.3 Compliance-driven Training

Compliance to federal cybersecurity mandates, such as those specific to employee security awareness and role-based training, is an important metric for government organizations, including Agency A. Unfortunately, as mentioned in Chapter 6, some federal agencies may possess a compliance mentality in which adherence to security directives that set a minimum standard is viewed as the attainment of a strong security posture. However, Agency A’s security awareness team recognizes that “just because you’re compliant doesn’t mean that it’s an effective program” (S1). They believe that compliance metrics tell little about how impactful the training is in teaching and changing workforce behavior: “Everyone will check the box saying ‘Yeah, we’re 100% trained.’ Prove it. And even if you are, what good is it if you don’t have people applying what they learned?” (S1). The security awareness lead further illustrated this point by discussing his experience with security training in his previous position:
“The old way version was ‘Well you have to spend X number of hours training’...I would spend days in class and got nothing out of it and go to a conference where I listen to one speaker, and it’s like a wealth of knowledge. So, it has nothing to do with the amount of time you spend. It has to do with the quality of that training” (S1).

Mandated annual cybersecurity awareness training is often computer-based, may be the same year after year, and, as described in the previous section, is viewed by employees as burdensome: “everybody’s frustrated with training” (E2). The agency CISO described:

“in the past, we have had very strict requirements on what constituted appropriate education for ongoing security awareness training and for role-based security training. And that caused us problems because we have so many requirements here for mandatory training, there is training fatigue” (M1).

Employees, therefore, were observed attempting to complete the training as quickly as possible, often paying little attention to the content. The security awareness lead commented, “People do it because they have to. You have the online training where it’s like ‘Click, click, click, click, done. That’s it, I’m done.’ Rather than paying attention to the words they’re seeing on the screen” (S1). The security awareness team thought that completion of mandatory training is viewed as an avoidance of punitive measures, rather than a learning opportunity. A team member discussed how completion is tracked in a spreadsheet and that many employees “just want to make sure the spreadsheet’s updated... and their supervisor will get off their back” (S3).
7.5.4 Resources

The security awareness team is faced with resource challenges. The program budget primarily consists of enough to pay for the two supporting contractors. Without additional budget or people, the team is not able to expand their efforts, as confirmed by the CISO: “I don't know how much more we can do to increase our activities with the budget pressure that we've got” (M1). The direct supervisor of the team commented that, due to a reorganization, “Where I was trying to get more people, we end up getting less people. So, we right now are just trying to do what we can do” (M2). The lack of resources also limits how much data from other groups the team can analyze to inform their security awareness efforts. However, the team perseveres despite the resource constraints, realizing that they must be more creative in delivering the message and recruiting “world-class” (S1) speakers to talk at events without compensation.

7.6 Chapter Summary

The case study was conducted with a small security awareness team at a mid-size government agency. In this chapter, I provide thick descriptions of the security awareness team, their mission, and how they are situated within their agency. I also describe the team’s general approaches to security advocacy, which include security awareness events in three different formats and other approaches such as campaigns and phishing exercises. Like the advocates from the interview study, the team encounters a number of challenges in their routine work, such as a lack of workforce buy-in for the importance of security and security awareness training, an organizational focus on security awareness training compliance rather than effectiveness, and resource constraints that limit how much the team can accomplish. The thick descriptions lay the foundation for Chapter 8,
which explores the progression of the security awareness team towards advocacy and audience empowerment.
8  Case Study: From Compliance to Advocacy and Empowerment

In the security awareness context, government agencies are federally mandated by the U.S. Office of Personnel Management (2019) to ensure all employees complete annual IT cybersecurity training in addition to other security-related training as dictated by their organizations. Success is often measured by number of employees completing a specified number of hours of training. However, participants in the case study interviews felt that measuring success simply via compliance metrics fails to address the intent of the mandate, which is protecting information and information systems by ensuring employees make appropriate security decisions.

To address the disconnect, the security awareness team has made a concerted effort to transform their program from being solely compliance-focused to being impact-focused. Their ultimate goal is “to be the best in federal government for an agency our size when it comes to training and awareness...To show how much we can accomplish with very little [budget] and to make a large impact” (S1). This transformation is evidenced by the team’s progression to cybersecurity advocacy with a renewed focus on engaging and empowering employees to make sound security decisions rather than simply on enforcing compliance. They also see the importance of gauging their success via meaningful measures of effectiveness. The team’s evolution is still a work-in-progress, so they strive for continuous improvement by trying new approaches and adjusting over time.

This chapter presents the case study findings which address all five of my original research questions:
RQ1: What are the motivations, professional characteristics, and skills of cybersecurity advocates?

RQ2: What techniques do cybersecurity advocates use to encourage security adoption?

RQ3: What are the rewards and challenges experienced by cybersecurity advocates?

RQ4: From where do cybersecurity advocates get their security information and knowledge?

RQ5: What techniques and attributes of cybersecurity advocates result in motivating their clients/audience to change behavior?

8.1 Evolving to a Cybersecurity Advocate Role

The Agency A security awareness lead position has transformed over the years from being a program manager to a cybersecurity advocate role. As the primary security advocate, the security awareness lead is the “face” of security awareness within the organization and is ultimately accountable for the program’s success. Although officially serving in support roles, the other security awareness team members (S2 and S3) are also integral contributors to building the program. In this section, cybersecurity advocate characteristics discovered in the prior interview study and found in the agency security awareness team are described.

8.1.1 Technical Knowledge and Relevance

Given the dynamic nature of cybersecurity threats and technologies, staying relevant and updated in the field can be challenging for security awareness professionals.
However, as also reflected in the advocate interview study, maintaining technical knowledge is critical for maintaining credibility with the intended audience. Recognizing this, Agency A’s security awareness team attempts to stay relevant with respect to security knowledge and security awareness approaches.

The security awareness lead is not complacent in relying on his previous technical experience. Instead, he recognizes the need to be knowledgeable about the latest technology and how it might impact the agency. This is especially important given his desire to appear credible during frequent interactions with others in the organization “because as soon as you mention something, there’s going to be somebody in that crowd that knows 13 other things that are similar and they’re going to throw it back” (S1). He continues to take formal training courses offered by external vendors and engages in self-study. Although the other team members had no prior cybersecurity experience, in their current roles, they “are on alert with current events or anything in the news” (S3) related to cybersecurity. Team members actively share this type of information with each other as “it kind of strikes up ideas” (S3). The team also subscribes to various community forum email lists to keep up with the latest security happenings.

When it comes to keeping abreast of the latest and most effective security awareness approaches, the security awareness team relies on learning from other organizations’ programs and customizing those approaches for Agency A. The security awareness lead described his approach as:

“just taking a look at what other people are doing and just using common sense, thinking ‘How would I do this? How are we doing it now and how
to make improvements.’ So, a little bit of critical thinking involved, and being creative, and having a good team” (S1).

He also regularly encourages the team members to attend other organization’s security conferences and forums, for example the FISSEA annual conference (NIST, 2019) which focuses on security awareness methods and challenges. S2 commented, “that’s really where we’re learning, like ‘OK, this is what people in industry are talking about it.’ Or ‘Oh, this is how somebody else runs a conference like ours.’ So, we’re kind of creating our training I guess” (S2). S3 further discussed the value of attendance of other events:

“We’ll pay attention to was it a good speaker, how was it run, is there anything we can do differently. It’s a lot of compare and contrast. I’ve kind of enjoyed that. Getting out of the office sometimes and seeing how other people run things, and how we can make ourselves better” (S3).

In risk communication, the credibility of both the risk communicator and the risk message is paramount. During interviews of agency employees, participants were asked about their perceptions of the security awareness team and the technical knowledge they communicated. Overall, employees trusted the technical information provided by the team. For example, a team leader said team members, “are knowledgeable...they’re the experts” (E3). An attorney remarked, “I'm pretty confident that they are providing reliable information, and that if they make requests to follow X, Y, and Z, that there's a good reason for it” (E6).
8.1.2 Service Orientation

While the security awareness lead, S1, is “very passionate about technology” (S1) as demonstrated by his long career history in the field, he is also professionally motivated by a keen service orientation:

“The one thing that’s motivated me my entire working career is to make a difference and have an impact, whether it’s anonymous or otherwise...I just feel that the cybersecurity training and awareness will make a difference not only for the agency and its mission but the people here as well when it comes to their outside life...And I feel that’s the best and most where we can increase the knowledge of the user so they can just be aware of what’s going on and what they can do to make their life easier and protect themselves” (S1).

The security awareness team lead is supported by contractors who also are service-oriented. When asked what motivates them to do security awareness work, S2 remarked, “the reason I wanted to get into training was to help people. And I really like having some sort of structure and plan and helping people develop that for themselves” (S2). S3 commented:

“It’s really cool to just see all our ideas and brainstorming and teamwork coming together helping the agency and people saying, ‘Oh, I saw your poster. Oh, I saw your event calendar. I want to come.’ When we hear stuff like that it makes us really happy that people are being aware and actually learning and seeing the content we’re putting out. That is great. And that’s what makes me really enjoy doing this” (S3).
As observed in the interview study, service orientation is often accompanied by a deep passion for the work, which was observed in the team by several employees. One remarked, “They are incredibly energetic. They are devoted” (E3). Another commented about the Lunchtime #2 event in which the security awareness lead presented: “He's very enthusiastic about it” (E7).

8.1.3 Creativity and Adaptability

Because the security awareness team has a minimal budget, they recognize the need to be creative in their approaches. During regular team brainstorming sessions, there is an emphasis on creativity and a willingness to try new approaches. The team lead encourages the team to not be “afraid to try something new, not afraid to put yourself out there” (S1). A team member admired his creativity and openness to new ideas:

“He wants to try new things. He rarely says no to an idea. He always says, 'There is no box. We’re not thinking outside of the box. There is no box.’ He always jokes about that, but I don’t think we’d have the same success” (S2).

Creativity was viewed as closely linked to adaptability to the work environment and employee needs. When asked whether he had experienced examples of people who were not successful at security awareness, the team lead remarked that his predecessor was not “creative and flexible...Being set too much in your ways and not being willing to try new and different is not helpful” (S1). Instead, he believed that effective security awareness professionals should be “receptive to suggestions from the outside...We solicit names of speakers, of topics, of any way we can make things better” (S1).
An example of the security awareness team creatively adapting to employee behaviors was taking shape during case study data collection as part of the agency’s “Click with Care Campaign.” The team wanted to ensure that all members of the workforce viewed important security information about phishing emails:

“We try to adapt and overcome. So, we were told, ‘Oh, I didn’t see the email about phishing awareness because my emails are so backed up’...

OK, maybe we’ll go old-school then. One of our ideas that we’re actually in the middle of coming up with, we have a little phishing handout. And it just has some tips of what to look out for. And we want to put it on half a piece of cardstock and go around at like 4:00 when everyone’s gone and put it on everyone’s desk with a little lifesaver with the information of who to contact when you believe [you have received a phishing email]” (S3).

The handout provided to employees is shown in Figure 2.

![Phishing Awareness Handout](image)

**Figure 2.** Phishing awareness handout. Front (left) and back (right) of handout. Original handout has been modified to anonymize the agency.
8.1.4 Interpersonal Skills

The security awareness team lead feels that, in order for security to resonate on an individual level, a personal touch is required, requiring strong interpersonal skills to build relationships via positive interactions, preferably face-to-face if possible: “You need to make sure you put yourself out there” (S1). These skills may be in contrast to those of other security professionals within the organization: “a lot of the security people aren't used to interacting with people, and they're used to being behind the scenes” (M1).

An example demonstrating the interpersonal skills of the team was observed during the Lunchtime #1 event. A team member was manning a cybersecurity trivia-based table. She was friendly and smiling while encouraging people to play as they walked by. She praised game participants for getting answers correct. If they answered incorrectly, she was still encouraging and explained the answers in an easy-to-understand way.

The team members are also viewed by their colleagues as approachable. An IT specialist felt “the team is wonderful...They're friendly, they're open to suggestions, they are open to questions if you have concerns” (E9). Another employee expressed:

“a lot of what this is is a relationship. And if you have a good relationship with your security team, your group, then you feel that you can approach them if you have a question. Even if the question is a very basic question, they never treat it that way” (E3).

8.1.5 Communication Skills and Context Awareness

Security awareness was viewed as requiring strong communication skills. As the public face of the team, the security awareness lead serves as master of ceremonies at all
the security officer forums and security day events and often speaks about security topics. He viewed his effectiveness as being grounded in his “ability to get those points across to everyone in an area where they’re going to understand” (S1). He recognized the importance of tailoring the message to the audience and their level of understanding: “I can sit up there and speak to the technical aspects of things and bore everybody except for the few techno-geeks in the back. Or I can try to make things more generalized” (S1). As an example of message tailoring, during an agency “Take your child to work day,” the team lead described how he had to fill in for a speaker at the last minute and talk about cybersecurity:

“There’s this auditorium full of kids and their parents... I just thought if I was a kid, what would I be interested in? And the fact that I knew about things like World of Warcraft and the different sims out there like MineCraft. and I knew some dad jokes when it comes to starting it all off” (S1).

An awareness of the context of the organization and work roles was also seen as contributing to successful tailoring of the message. This helps with explaining the reasons behind security practices, i.e. why they are important to both the individual and the mission. The team lead often has to communicate the benefit and reasons behind security training requirements, commenting that his predecessor “didn’t really get people to understand why they’re taking the training. That’s one thing that we try to do is push that. This is why you should pay attention. These are the things that are really happening” (S1). For example, at the observed security officer forum, the lead talked about cybersecurity role-based training, including the federal directives that require it,
who it applies to, why it’s important, and how and when role holders can complete the training requirements. As another example, during the security days, at the conclusion of each talk, S1 asked at least one question of each speaker that attempted to tie in the topic to Agency A’s mission so that attendees could make the connection.

Employees expressed positive perceptions of the team’s communication abilities. When asked about her thoughts on the content of the security awareness information she receives at work, a research librarian said, “I think it's simple, to the point, so you don't have to read in detail to...try to understand” (E1). Another staff member said it was beneficial

“having the information presented in a manner to where it’s not intimidating, which is something that I feel that our group does, to where they take it seriously, but it is also presented in a way that you can embrace it and take away information” (E3).

Marketing is another form of communication. The security awareness team believes they have to excel at being able to market their events and campaigns in order to engage as many people as possible. S2 and S3 put a significant amount of effort into advertising the events beforehand. They post flyers throughout the agency workspaces, station posters on easels in high-traffic areas (such as the main lobby and by elevators), and advertise via electronic signage (video displays) throughout the buildings. Special effort is put into promoting security days, which are the biggest events held during the year, as described by a team member:

“Especially for our [security day] we have a promo team leading up to it.

In October we actually took it another step...We worked with DHS. We
became one of their National Cybersecurity Awareness Month partners.

And so each week of the month of October they had a topic, a spotlight topic...Once a week we would have a promo table...And then we would have little bags of cookies because we did 8 cookies equal a bite, so we called them ‘cookie bytes.’ And we would pass them out in preparation for the event” (S3).

The marketing of events does not end after the event. In an effort to gain leadership buy-in and motivate future attendance of events, the security awareness team writes post-event reports that summarize each event’s theme, content, and attendance numbers. The reports are emailed to senior leadership in the Office of the CIO and to all event attendees who had signed in for training credit.

8.1.6 Discipline Diversity

The security awareness team consists of three individuals with different educational and work backgrounds coming together to focus on security awareness. As previously mentioned, the team lead has a deeply technical background, having worked in IT and cybersecurity for over three decades. However, neither contractor had cybersecurity experience prior to supporting Agency A. S2’s formal degree was in criminology, but she was passionate about working in the training field before obtaining her current position three years prior: “the cybersecurity aspect, the awareness aspect of it wasn’t something I was seeking, but it was a wonderful benefit and bonus that came along with it” (S2). S3 also unexpectedly fell into a cybersecurity role when she joined the security awareness team two years prior. With a business degree and having primarily worked in customer service,
“I had no background in cybersecurity or anything… But I’ve always been interested in event coordinating... they thought with my skills and my background and being around people and personalities...that it would be a good fit. And it actually turned out to be one” (S3).

Each team member was seen by other team members as contributing his or her own strengths in a cooperative, synergistic fashion: “We just work really well with each other and can bounce ideas and everything” (S3). For example, S1 has the security and technical knowledge, but admits:

“I am not a subject matter expert in the marketing and the others that [S2 and S3] do, the organizational skills. I need them to do that. They’re also brilliant when it comes to the ideas and how we’re going to make things happen. I wouldn’t be able to do that on my own” (S1).

8.2 Engaging and Empowering the Workforce

The team utilizes their cybersecurity advocate skills to transform the security awareness program. This transformation entails a shift from an extrinsic motivation of security being an organizational compliance requirement to intrinsic motivation where security becomes something one wants to do because of its inherent value. The shift involves changing the work place security culture by first facilitating recognition (engaging) but then also instilling a sense of personal responsibility and self-efficacy (empowering): “it’s getting that mindset to change from ‘Yep, security’s important’ but not implementing it to ‘Security’s important. So let’s make sure we’re doing it’” (S1).

The team lead likened this goal to the development of dental hygiene habits:
“knowing that you have to brush your teeth, to actually brushing your teeth and then not even thinking about brushing your teeth every day. That’s what I’m trying to push for in our program, where security awareness is now second nature” (S1).

Engagement is about the personalization of the security message and bringing awareness of security issues and the relevance of those to individuals. At the observed security officer forum, S1 told the audience, “We don’t want to make you paranoid. We just want to make you aware” (S1). The CISO discussed the prior view of security training as being education-based versus the current awareness-based approach:

“I would say that our view of education was you had a web presentation or a classroom presentation, and then you did multiple choice to make sure you heard and were able to respond to that very specific feedback. Now that we have more generalized presentations on more and varied content, people are now making the connection to security on their own, to how they do things” (M1).

The team lead recognizes the importance of involving the workforce as active participants and contributors to the security of the organization, believing that “Human beings are the most important cybersecurity tools” (S1). Empowerment involves providing actionable steps, increasing feelings of self-efficacy, and encouraging individuals to be more reflective about their security behaviors as part of their day-to-day lives both at work and home. This involves a shift of the locus of concern from just the security of the organization to also include the security of the person. The CISO believes that, because of the security awareness program, people at Agency A “have become more
aware of the choices that they're making” (M1). The team lead views effective security awareness as going beyond compliance: “I’m not going to force anybody to change but give them the opportunity to see that they can” (S1). An employee commented on the synergy between bringing awareness and encouraging action:

“The more we know about it [security] and the more we know people that we can reach out to that can help us if we have a question about it, I think that can make you feel more empowered and more comfortable in doing it the right way and protecting yourself as well” (E3).

This section describes ways in which the security awareness team attempts to engage and empower the agency workforce.

8.2.1 Topicality

One way in which the security awareness team attempts to convince the workforce of the relevance of security to their lives is by ensuring that concepts highlighted in events, campaigns, and other communications are topical. Security awareness focus areas and event themes might be related to the season of the year, items in the news, or recent organizational security needs or threats to the agency. For example, an event held shortly before the Super Bowl was entitled “Cyber Kick-off.” A September event’s theme was “Prepare to Fall Back into Your Cyber Routine.” Security officer forum themes may be related to current security hot topics within the federal government or in response to other areas of interest communicated by ISSOs. For example, with cloud computing becoming more prevalent and a need for ISSOs to understand related federal government policies, one forum’s theme was “Get Your Head in the Cloud.” Another theme, “Wake Up and
Smell the Cyber,” featured talks on several tools and processes useful in ISSOs’ daily work.

When deciding on speaker topics for security officer forums and security days, the team often considers recent security or technology issues at Agency A. In past security day events, there have been primers on different emerging technologies that may be useful in more efficiently executing Agency A’s mission, for example blockchain and drones. The team lead provided another example:

“we just had an inspection where we found a bunch of people that were leaving their PIVs [Personal Identity Verification smart cards] in their readers when they weren’t at their desks. So we’re going to be talking at the [security officer] forum about that because when you take a look at some of the largest hacks especially in government has been when system administrators have done things with their system administrator account they shouldn’t, like clicking on email or a link…So we try to be timely and situational with everything we’re doing” (S1).

To ensure events are relevant and of interest, the team also involves the workforce as active participants in deciding which topics to address at security awareness events. As the CISO stated, “We're learning from our participants, which I think is very important because they're the ones who have to be secure” (M1). The lead described how his team has increased attendance at the security officer forums:

“in the past, the training person dictated what she thought the ISSOs [information system security officers] needed to learn. The first thing we did when we took over, we brought a bunch of them together and asked,
'What do you want? What would make these more efficient and effective?’
And again, we saw the numbers just jump up. We changed the venue so it was totally different. We started bringing in people they wanted to hear, subjects they wanted to hear that meant most to them. It’s been very successful as far as that’s concerned” (S1).

When asked how they come up with topics to include during security awareness events, a team member explained:

“At the end of all of our events we send out a survey... And then at the end we always ask, ‘What are you interested in hearing about at the next event?’ And so we save all that. We use senior leadership if they say, ‘We really need you to talk about this.’ Or ‘This has been an issue. Can you mention that?’ And then just talking to people who come to the events. Sometimes they’re like, ‘Oh, I really like this person. Bring them back.’ Or ‘I really was wondering about this.’ And so we’ll just jot it down and keep a running tally” (S2).

Since the security awareness team is viewed as approachable by agency employees, some feel comfortable suggesting topics to disseminate to the workforce. For example, an attorney said:

“I have taken an active role in informing some of their staff about external threats like the IRS scam and the social security scam. Because if it hits the paper, I just press send and send it to people who work in the program. And they go like, ‘Oh yeah, this is really timely information. Thanks for letting me know that’” (E5).
8.2.2 Work-Home Connection

One of the major objectives of the security awareness program is to move employees toward intrinsic motivation where they want to do the right thing when it comes to security and feel a sense of ownership, self-efficacy, and responsibility. The team strives to shift the mindset of employees to always make informed security decisions and follow safe cybersecurity practices regardless of where they are so that security becomes a habit.

Towards this objective, at most of the security awareness events, there is a "mix of cybersecurity at work and home" (S1). An team member commented that incorporating the home aspect really gets people’s attention. At work people might feel like someone else is responsible for security, but at home they are responsible. The team lead further sees the work-home lines blurring as people telework more often:

“It’s no longer ‘Here’s my work computer and here’s my home computer.’

Now everything is on their phone and mobile device. They’re using Citrix or logging in using a VPN. That whole thing together of what people outside of work and at work coming together. And I feel that’s the best and most where we can increase the knowledge of the user so they can just be aware of what’s going on and what they can do to make their life easier and protect themselves” (S1).

The interviewed employees discussed ways in which security information gained at work helps them in their personal lives. One employee remarked:

“They've incorporated some things that you can use both at work and at home so that you can protect yourself, whether you're using your cellphone to do a search, or buy something online, whatever, so that you
are alerted and educated to how things can happen. And so the variety of
tings and how it can be applicable both personally and at work are really
good” (E3).

An IT specialist also appreciated the work-home emphasis:

“I really like when they send out information too that’s not just helpful for
the agency but where you can apply it to your own home computer as well.
So it may not be anything major, but even the passwords or the best way to
create a password. And that might be a better way that they get attention
of the other people as well, something where they can apply to both home
and at work” (E7).

As a result of security awareness training, “people are starting to think more critically
about what it is they put on their phone, what it is they have in their backyard where a
drone could see it, what they send out in an email” (M1).

As an example of the work-home connection, the holiday-themed Lunchtime #1
event featured a table called “Information Station Holiday Edition: Are your gifts
vulnerable?” This station was led by an agency contractor who spoke to attendees about
security and privacy considerations for Internet of Things gifts (e.g., voice-controlled
assistants, smart security cameras, drones, fitness trackers, and internet-connected toys).
He discussed how the device features and functions can sometimes be provided at the
expense of security and privacy, for example, cameras in drones and other smart home
devices. He also provided a handout (Figure 3) with recommendations for how people
could protect their privacy and ensure that security vulnerabilities do not negatively
impact their interactions with these technologies.
The events do not just focus on cybersecurity topics related to work and home; rather, the team also tries to provide useful information related to other types of security, such as personnel and physical security. The CISO commented on this approach: “we want to secure the person, and we want everyone to think about all aspects in which they could secure themselves” (M1). For example, a “Cyber Hygiene” lunchtime event held during cold and flu season had, in addition to cybersecurity-related stations, representatives from the agency’s gym and health center. A summer “Traveling Cyber Safe” event featured an agency employee from the personnel security office who provided information about foreign travel safety. At the Lunchtime #1 event, three stations addressed physical and financial security topics that might impact agency employees in their personal lives. The local county consumer protection office provided recommendations for safe shopping, for example monitoring credit card activity closely.
and exercising caution against phone scams. The local fire department talked to attendees about fire safety during the holidays. At a popular table, a county police officer educated staff about credit card skimmers using videos and examples of confiscated skimmers.

8.2.3 Varied, Engaging Communication Techniques

In order to engage the workforce, the security awareness team disseminates security information using a variety of communication channels and techniques, such as speaker presentations at security day events, handouts, remote broadcasting, and other novel approaches. Whatever the media, the approach must pique interest. The team lead described, “rather than forcing it down your throat, we’re trying to make it entertaining at the same time” (S1). A team member relayed, “[S1] says, ‘If we can get five eye rolls at an event, we can call it a win.’ Because especially in this industry, everyone’s so business and serious. So, we like to have a little fun” (S3). For a successful program, a manager recognized the need for security awareness efforts to take into consideration employees’ constraints: “we need to keep it making as user-friendly as possible, not having it be a big commitment of people's time. And doing it in such a way that people want to keep coming back to the program” (M1).

8.2.3.1 High-quality Speakers

The security awareness team takes great care in selecting topics of interest to the agency workforce and finding engaging speakers for security days and security officer forums. As mentioned previously, team members periodically attend other organizations’ security awareness training events to identify potential speakers. They also regularly consider recommendations from agency employees and other speakers:
“We tell people ‘Let us know what you want to hear, if there’s a specific speaker.’ Because we actually had two great speakers at our October [security day], and it was because someone suggested it...And we had them, and it was awesome, and they were the best speakers of the event” (S3).

The majority of speakers are from external organizations and represent other government agencies, academic institutions, and industry: “we’re getting in these outside speakers and that’s exciting for people to listen to. They’re just hearing another perspective and another point of view that’s not from our agency” (S2). For example, at the Security Day #1, four external speakers from government and academia discussed topics that included privacy policies, artificial intelligence application to critical infrastructure, supply chain risk management, and assessing cyber risk.

8.2.3.2 Handouts

The team makes regular use of security-related handouts. Handouts come in different formats, including pamphlets, one-pagers, bookmarks, and postcards. At each event, handouts are available at an Office of the CIO table for attendees to take. One team member commented:

“At our events we always have one table that’s just strictly handouts...We’ve noticed people will just walk by, ‘Oh, this is interesting.’ We tried to do a lot of different types of handouts. We have phishing, we have cyber bullying, different things for kids and parents” (S3).
Because high-quality handouts can be labor-intensive and expensive to produce, most are from reputable third-party non-profit and government sources. For example, materials are often sourced from the National Cyber Security Alliance (2019) and the Federal Trade Commission (2019), which distribute pamphlets in bulk, free-of-charge. The security awareness team will generate their own materials when they see a gap in third-party offerings, want to advertise their upcoming events or training opportunities, or need to customize guidance to be agency-specific. For example, Figure 4 shows the front and back of the team’s “Click with Care” campaign handout.

8.2.3.3 Novel Communication Approaches

The team sees the necessity of employing novel security awareness approaches to overcome complacency and garner attention. One team member said:

"You definitely need to be creative. That’s a big thing because you want to just put a different spin on it because people just see stuff all the time:"
‘Have a good password. Lock your computer.’ But I think to be creative and think outside the box for different reasons or different tactics to make people think” (S3).

Several examples of non-traditional security awareness approaches are provided in this section.

Most lunchtime events included some kind of gamification. At the Lunchtime #1 event, a team member manned a game table that included holiday-themed trivia about non-security topics (e.g., how many candy canes are sold each year?) and questions about security relating to cell phones, common security attacks, passwords, and safe use of Universal Serial Bus (USB) devices. For example, attendees were asked to define man-in-the-middle attacks. If an attendee did not know the answer, the team member would read the definition and then provide a short, illustrative story using a metaphor of two people sending a letter back and forth and how a letter could be intercepted and modified. Prizes were a bag of “bitcoins” (wrapped chocolate coins).

Another example of a novel approach was observed when the team executed a campaign to encourage employees to complete their annual security training early rather than waiting until close to the deadline. In addition to displaying posters with reminders about the training, the team wanted a memorable, humorous way to promote the training, so they distributed “Now and Later” candies on people’s desks with postcards that said, “Take your training now and not later.”

The Lunchtime #3 event was a humorous parody of a late-night television show. The security awareness lead served as the host and opened the event up with a comedic
monologue with IT and cyber-related jokes. Various guests joined him on the “stage” to discuss security and IT topics.

The Lunchtime #2 event also demonstrated the security awareness team’s willingness to try novel approaches. The event, entitled “To Send or Not to Send” was held in a different format than prior lunchtime events and involved adaptations of popular Shakespeare plays to address cybersecurity concerns. The impetus for the theme stemmed from recent security issues observed within the agency:

“we were told a lot of people were having issues with their PII [personally identifiable information] and sending out their W-2s [to their personal email accounts] and not knowing what to send. We were brainstorming, and someone said, ‘Oh, to send or not to send’...They’re not paying attention to emails, they’re not paying attention to posters. Maybe we’ll do a little show about it and put our own cybersecurity spin on it” (S3).

Instead of the information table configuration, the exhibit area was set up with rows of chairs to accommodate an audience. Attendees were given a “playbill” containing the performance script and associated cybersecurity tips (see excerpts in Figure 5) and were offered a bag of popcorn. During the performance, the team lead donned a Shakespearean-era style hat and proceeded to read through three “acts” based off plays but re-written by the security awareness team to incorporate cybersecurity themes. The first act, “To Send or Not to Send,” addressed sending email safely. The second act, based on “Romeo and Juliet,” featured Juliet as a phisher trying to entice Romeo to click on a phishing link. The third act, “Training of the Shrew,” discussed the importance of annual security awareness and role-based training.
Although the team is not afraid to try new approaches, “not everything works” (S2).

The team members described a station-based lunchtime event in which they designed a “cyber passport” for attendees:

“Everyone going to the [event] could go and get a signature from each table [on the passport]. So, basically stop by each table, get a signature for each participant, and put it in the box to win a gift card. And we thought it would be great, but it was just hard logistic-wise also because with the [lunchtime events] people kind of come in different ways...And then a lot of people are kind of like ‘Oh I don’t know. I want to do this.’

And when they found out it was a gift card to the cafeteria, they’re like ‘Oh, I don’t want that.’ ...We noticed only like 5 people were doing that, not many people were filling them out and putting them in the box. So that idea kind of fizzled” (S3).
Failure, however, does not deter the team from continuing to try new ideas.

8.2.3.4 Remote Broadcasting and Recordings

The majority of Agency A employees, including the security awareness team, are located at agency headquarters. However, Agency A has several remote, regional sites. Each site has local IT administration staff but no on-site cybersecurity personnel. Rather, sites’ security functions fall to headquarters to manage. Providing security awareness for these remote locations poses a challenge:

“*How do we get the people in our regional offices engaged? Everything is headquarters-centric, actually here at the headquarters, because that’s where we primarily are. But how do we also get that word out to our regional offices again without having a travel budget to travel out there?*”

*(S1).*

To address this challenge, the team arranges for security days and security officer forums to be made available via webcasting for staff at remote sites or headquarters-based employees who cannot attend the events in person. Slides and videos are also posted on an internal SharePoint site afterwards for those who could not watch the event live.

8.2.4 Practical Recommendations

The security awareness team felt that bringing awareness of security threats is important but does not necessarily lead to behavior change. Rather, in addition, they recognized that people need to be provided practical, actionable steps they can take to counter the threats and protect themselves and their organization. As expressed by the security awareness lead, “*cybersecurity awareness is not always ‘The bad guys are*
coming to get you’ but here are some better tools to use” (S1). He believes that people can take small steps that have a large, long-term impact: “You need to just be aware of the little things you can do to protect yourself from the little things that are going to happen that are going to end up being a big pain” (S1).

The team makes an effort to ensure security awareness topics include recommendations that are achievable given employees’ skillsets, described in terms they understand, and are accompanied by points of contact if more information is needed. Recommendations are often offered by event speakers and in handouts. For example, at the Lunchtime #2 “To Send or Not to Send” event, after each act, the team lead described the security issue in plain language and offered concrete steps attendees could take (Figure 5). The accompanying “playbill” handout also included links to agency web pages for more information. At the observed technical security officer forum, the lead talked about PIV card security vulnerabilities and provided concrete recommendations for mitigating those. An agency contractor also demonstrated a recent security exploit and suggested mitigation actions.

Presenting security threats without practical advice may leave employees feeling unsatisfied and powerless. During an interview, one employee discussed an event speaker who attempted to scare the audience without offering practical mitigation advice:

“We had one fellow who was tremendously entertaining and informative, but he completely unplugs his entire home system, computer system and everything else, every time he leaves the house. And I'm thinking, ‘Oh my God. Should I be doing this?’ And what should you do?” (E6).
8.3 Gauging Success

The team understands that security awareness training compliance, while required for a government agency, does not necessarily translate into effectiveness. How, then, can an organization measure the true impact to workforce attitude and behavior change? The development of meaningful measures of effectiveness can be non-trivial but is still a goal for the team lead, who views compliance and effectiveness metrics as being complementary: “I’m coming up with different ways of measuring how we’re making that impact as well as making sure we’re hitting all the right checkboxes for compliance. So, it’s kind of a balancing act” (S1). Currently, the security awareness team measures impact of the program based on a combination of compliance metrics, event attendance, event survey results, verbal feedback, and user-generated incidents and reporting.

8.3.1 Compliance Metrics

Compliance metrics reveal how many employees fulfilled their federally mandated annual IT security awareness training or role-based training requirements. These metrics are reported to leadership within the agency, but also to DHS, which has a role in overseeing federal civil agencies’ compliance with information security policies (DHS, 2019).

Compliance, although sometimes deceiving, can be one indicator of progress as expressed by the team lead: “Seeing our training numbers, meeting our goals for the training numbers, even though that’s just compliance, it’s still showing that people realize that they have to take this, start making that awareness” (S1). The CISO reflected on how security compliance metrics can show improvement over time:
“as we look at our OIG [Office of the Inspector General] reports, as we’re looking at our reporting to DHS, we’re seeing continuous improvements.

Not as large as we have in the past, but that’s okay. We’re making incremental improvements, and that’s the important thing” (M1).

Not meeting compliance goals can be disappointing. The team lead described a recent issue that resulted in compliance numbers appearing to be lower than desired:

“Our annual computer security awareness training, the annual stuff, we just missed our goal last year because we uncovered another problem. People are on the list who no longer worked here, so it was an off-boarding issue, a reporting issue when it came to contractors. And we just missed our goal for a point and half, and that really upset me” (S1).

8.3.2 Event Attendance

Event attendance is used as an indicator of the reach of the security awareness program: “I think we’re starting to make a difference. I can see that by the numbers of people who come to our events and look forward to it” (S1). Attendance at more structured events, such as the security days and security officer forums, is tallied based on sign-in sheets for those wanting to earn cybersecurity role-based training credit plus a count of employees joining in remotely. At the lunchtime events, a team member performs a head count of those entering into the area and also maintains a sign-in sheet for those wanting training credit.

Although saying little about the impact, attendance may be the only immediate measure available to the team: “right now, we can only gauge if it’s successful by how many people attended. That also is affected by the time year” (S2). Since taking over the
program, the security awareness team has seen an increase in attendance. Referring to
security days, the lead compared the 200-300+ attendees in recent years with prior
attendance: “We’ve also seen some after action reports from some of the other
cybersecurity events that took place...They were excited to get 50 people” (S1). The
CISO also monitors attendance trends:

“we use our learning management system to register folks for the class.

But they can show up and sign in. We’re seeing increases in both. So, a lot
more people are preregistering and showing up. And a lot more people
are just showing up” (M1).

He attributes some of the attendance increase to the location of the events: “We have
them in public areas of the building, so they're difficult to ignore but easy to skip if you
don't want to” (M1). In addition to event attendance, the team looks at how many people
view posted content after the event: “We have also noticed now that we've put the content
of these presentations online, people are going back to watch them again” (M1).

Event attendance is not just assessed by the numbers of attendees. Audience
involvement is another indicator of success: “When we're doing a [security day], seeing
the reaction from people in the crowd and seeing the engagement. People are asking
questions after a speaker” (S1). The types of staff who attend the events also shows
progression of the program. In recent years, the team has noticed a more diverse
audience. The team lead observed:

“I can say that just looking into the crowd, I noticed it going from
primarily our information officers to now starting to see people from
different mission offices showing up especially to our big [security day]
events where we have 300 people either watching off the computer or in the auditorium downstairs” (S1).

A team member had a similar observation: “A lot of times people will come to our events and not even be on the cyber side of our agency. It's great to see those people stopping by” (S3). The team also informally keeps track of senior leadership participation so they can gauge management support and direct market events to them in the future.

8.3.3 Employee Feedback

Employee feedback is another way in which the security awareness team feels they can begin to gauge the effectiveness of their program. Feedback is primarily received via post-event surveys and personal interactions. My interviews with agency employees also revealed perceptions of the security awareness program and are summarized in this section. While the feedback I collected was predominately positive, likely due to the bias of what I had access to, negative feedback was obtained via post-event surveys and also gauged by outward engagement of employees. For example, as mentioned earlier, the “cyber passport” idea at a lunchtime event was not positively received. Team members observed that people expressed that they did not wish to participate and few completed passports were entered in the drawing for a prize.

8.3.3.1 Post-Event Surveys

After every security day and security officer forum, the team invites attendees to complete an online post-event survey. Although survey results may be biased due to self-selection of respondents, the surveys provide a useful mechanism for the team to obtain feedback on the event as well as suggestions for topics at future events. As part of case study data collection, the team provided survey results for the previous two security
officer forums in 2018 and three security days in 2018 and the first half of 2019. Survey response rates were typically low: roughly 12% and 30% of attendees took the survey for the two security officer forums and approximately 21%, 15%, and 9% completed the survey for the three security days in May 2018, October 2018, and May 2019 respectively.

Security officer forum surveys asked respondents to rate the quality of the topics and presentations, the organization and communication of the event, and experience with the webinar application if viewing the event remotely. Respondents were also asked what topics they would like to see at future events, and what additional feedback they have. Overall, survey respondents viewed the security forums positively. Out of 43 total respondents in two surveys, 93% rated the overall quality of the topics/presentations and the organization/event communication as above average or excellent (scale = Very Poor, Below Average, Average, Above Average, Excellent). In the additional feedback survey field, 21 respondents suggested topics to include in future forums. The field also allowed respondents to voice open-ended thoughts about the forums, such as:

- “I’ve attended every forum for years at [Agency A], and they keep getting better each time. Excellent, pertinent topics, and great speakers.”
- “Interesting and informative, even for non ISSO people.”
- “Final presentation was not geared for the needs of the ISSO audience. Seemed more like a sys admin [system administrator] talk.”

Security day surveys included all the questions from above and also asked respondents to rate their overall experience at the security day. Like the security forums,
most respondents had positive views of the security days. Out of 109 total respondents in three surveys, 95% rated the overall quality of the topics/presentations as above average, or excellent, and 88% rated organization and communication as above average or excellent. When asked to rate their overall experience at the security day, roughly 93% said above average or excellent. In the additional feedback survey field, 47 respondents suggested topics to include in future forums. Examples of other comments include:

- “The topics were very relevant to our everyday lives using the internet.”
- “All the speakers are experts in their field and did a good job.”
- “I would like to see more concrete guidance provided to folks.”

The survey for Security Day #1 in 2019 additionally asked the 21 respondents why they attended the event. Employees were provided with five options (plus a fill-in-the-blank Other option) and asked to “check all that apply.” Figure 6 shows the results for this question. Reason for attendance provides insight into whether attendees were there to earn role-based training credit or for some other reason. Two-thirds indicated that they did indeed want to earn training credit, while over 85% said that the advertised talks looked interesting. Interestingly, just over half attended because they thought the information would be helpful in their jobs.
8.3.3.2 Personal Feedback

The security awareness team also often receives feedback directly from employees (face-to-face or via email), most of it positive. The team lead commented, "I do get unsolicited feedback saying, 'It's a great program you put on. Your [security day] event. This is really different.' When we're having our [lunchtime event], 'We're not used to seeing this'" (S1). When staff members found out that S3 is involved in planning the security awareness events, they talked to her about how they enjoyed past events: "We were still hearing things about speakers we had a couple years ago, and people saying, 'Oh can we get them back, can we get someone similar.' ... The fact that we still hear feedback months and years later is very rewarding" (S3). Even managers in the team’s chain of command have received feedback:

"I'm getting a lot more positive feedback from the agency, from the user community, than I had in the past. And before, when we thought not getting negative feedback was good, getting positive feedback is even
better... And people are now coming to us and saying, ‘I like what you've
done at your last [lunchtime event]. I'm glad I can now go to the security
officer forum. I'm glad that you're having these things because I've
brought my partner, my child, my parents, so that they could hear the
importance of security’” (M1).

8.3.3.3 Employee Interview Feedback

Interviews with agency employees also shed light on the impact of the security
awareness program. Although not quantifiably measured, employee responses provided
anecdotal evidence that security awareness training is shifting security attitudes. One
employee now sees that he has an important role in security: “we have to pay attention...
I have a lot [of responsibility]...bottom line is if something happens, we all look bad. And
we have to look after each other” (E4). Another commented on how the training caused
her to reflect on her own behaviors: “some of the training from the [security day] events
opens your eyes to things and makes you step back and think about things a little bit
more and see if there's anything here that we could do differently” (E8).

During the interviews, employees were asked how security awareness information
they receive at work helps them make security decisions in their day-to-day jobs. As an
example of empowered action, five out of nine participants discussed the personal impact
of security awareness efforts related to phishing and appropriate email behaviors (e.g.,
not clicking phishing links, not sending sensitive information outside the agency). From
an awareness perspective, one employee commented, “I didn't have that awareness
before... I am much more educated now than I used to be...I know now that emails can
be hacked into. That by itself is a big deal” (E4). Others demonstrated that their
awareness also translates into action. They now feel empowered to report potential phishing emails. A research librarian said, “Sometimes you have a doubt [about an email] saying, ‘I don't know. Is this suspicious or is it legitimate?’ So I don't click on an attachment, and I just re-forward it to the computer security people” (E1). An attorney remarked on how agency security awareness training has led to increased vigilance:

“You can get messages from the agency, and I go like, ‘Is this real?’ And I send it to the cybersecurity team to say, ‘Am I supposed to be answering this?’ So, basically as a result of my training here, I am very, very suspicious of everything” (E5).

Several employees with cyber roles commented on the value of information presented at the security officer forums. An IT specialist mentioned that one talk “made me think more about my system... [It] was something that I could apply to my own systems going forward” (E7). Another learned new information that helped with a particular task:

“We have processes and templates we have to go by. And in one instance I was tasked to develop a business impact assessment for a particular system, and I didn't know that the template had changed. So, going through the forum...I was informed that the template has been updated to a newer version. So, it's things like that we get from the ISSO forums” (E9).

Employees were also asked how the security awareness information they receive at work has helped them make security decisions at home. Being able to identify phishing email was mentioned repeatedly: “I think I'm very cautious about what I open up and
send at home” (E6). Employees also discussed security tips they’ve received at work about other topics such as social media, cell phones, applications, and phone scams, which they in turn pass on to their families. An IT specialist said:

“some of the information, [the security awareness team] will pass out and say, ‘You can send this and share this with family’...Just little things like that, really paying attention to what my kids are doing online, and I definitely have thought about several of the talks going home. And I have sent information that was approved to my parents saying, ‘You need to read this’” (E7).

A lunchtime event presented security information related to mobile apps, prompting one employee to educate her daughter:

“I went home and just ran through my daughter's phone, said, ‘Let me see everything that's on your phone. Let me see everything that you access’...And I'll say to her, ‘Well, certain things you have to look at the link...Although you may not know where it's going to direct you, but just be cautious about which link.’ So, I now was showing her the difference” (E9).

8.3.4 User-Generated Incidents and Reporting

Trends in user-generated security incidents were seen as another gauge that employees are becoming more security-aware: “Are they going up? Are they coming down? Are we seeing more people going to the training and does that mean we’re seeing fewer events?” (SI). For example, indicators of employee behavior change might include decreases in the number of incidents of badges being left unattended in computers or
fewer incidents of employees emailing unencrypted personally identifiable information (PII).

Agency phishing exercise click rates are an example of metrics involving user incidents and reporting. Click rates involve the number of employees that click on the phishing email link, and repeat clickers are those that click on phishes in two or more consecutive exercises. A manager reflected, “I think we've already seen a lot of success in phishing, where the click rate was driven down, ...repeat offenders [were fewer]” (M2). When click rates dipped low, the team lead wondered if this was because the phishes were too easy or if the security culture was improving. To test this, the team increased the difficulty of phishes sent during quarterly exercises. The subsequent click rates remained low, implying that employees were indeed informed about phishing and making good security decisions.

User reporting of security issues is also viewed as a success indicator. When asked about what measures of effectiveness are most meaningful, the CISO commented:

“Once upon a time, I would have said fewer incidents. Now, I'm saying more better-reported incidents. So, people are recognizing that they've done something, recognizing that there’s a problem. And they’re even calling us to tell us that: ‘I got this message and I recognized it. I didn't respond to it, but I wanted you to know that it was there, so you could study it and block it’” (M1).

8.3.5 Evidence of Leadership Support

The security awareness team has witnessed increased support from senior leaders in their chain of command (CISO, Deputy CISO, CIO, Deputy CIO). Prior to the current
team running the security awareness program, the leadership viewed it as “just kind of this small little program. I don’t think it had that much spotlight on it” (S3). However, that has changed in recent years: “now I’ve got the CIO and the deputy CIO and the CISO and the deputy CISO sitting in the crowd and watching the whole thing rather than just showing up to give their opening remarks and then leaving” (S1). At least two of these leaders were seen attending all the observed security awareness events. Another manager commented, “We have the attention of our CIO, and he wants to get the word out. And I know that when he has meetings with his counterparts, he’s letting them know” (M2). The two interviewed managers were pleased with the progress the security awareness team has made. The CISO said, “I think we’re in a fairly good place” (M1). The security awareness lead’s immediate supervisor complimented, “I think we’re doing a fantastic job with the resources we have” (M2).

As the program has grown, leadership’s trust in the security awareness team has increased for a variety of reasons, including more awareness of the program and its scope:

“we make sure to loop them [leadership] in and everyone be on the same page. But I think because our events have gotten bigger, more people are being more aware, and we’re getting great speakers, and we’re trying to market it as much as possible, I think they’re noticing it more and more” (S3).

When asked about management’s view of the program, a team member said:

“Since I’ve started, they’ve always seemed to be very supportive, and they seem to view what we’re doing in a positive way…they’re very hands-
off...But I think that’s a good thing because I think that they trust that,
from what they see, it looks like it’s running smoothly...They hear good
things so I think they kind of just leave it be” (S2).

The security awareness lead also engages with senior leadership outside his chain of
command: “I also do the senior executive training, and I’m trying to make them more
aware of what we’re doing and why we’re doing it. And so far, I’ve gotten a lot of
positive feedback” (S1). He believes, “if we can get the leadership to look forward to
what we’re doing and show some interest rather than just being another line on a report,
I think that’s very good. I think we’re making some progress” (S1).

8.4 Continuously Improving

The team recognizes the need to improve the program to meet evolving security
requirements and threats to the agency. Throughout his interview, the lead repeatedly
took personal responsibility for making the program better and addressing perceived
shortfalls. For example, when asked what he finds most challenging or frustrating about
his role, he said, “I’m impatient about it and passionate about it. ...I’ve found it
frustrating sometimes that I can’t get a broader audience. That’s on me” (S1). He later
remarked, “I think that we’re starting to make an impact. Not as quickly or as large as I
would like. That’s why we keep pushing” (S1). The team shared their ideas to expand the
program and pursue more meaningful measures of effectiveness, including taking a more
holistic approach and trying to reach a broader audience. However, much of those plans
are dependent on obtaining additional resources.
8.4.1 Holistic Approach

Recognizing that there is more to telling the agency’s cybersecurity story than compliance numbers, the team lead spoke about wanting to take a more holistic approach to measuring the effectiveness of the security awareness program but currently not being able to do so because of limited resources. He expressed the desire to examine agency cybersecurity security data (e.g., security logs, incident reporting, real-world phishing emails) and physical security data (e.g., badge incidents) to explore potential relationships to security awareness training and identify areas where new or different training might be beneficial:

“you could take personnel security stuff, the security awareness training, the user-generated events, and now let’s take a look at our automated systems. Let’s take a look at our DLP [data loss prevention software]. Let’s take a look at our logs. Let’s merge that data together to see if we see a real pattern of what’s really taken care of... to be able to take a look at security from a holistic standpoint” (S1).

A better understanding of the agency’s security posture can also inform customization of annual online security awareness training, which is a future plan of the team: “we’re probably going to try to find what exactly the agency is deficient at. And that’s where the holistic approach comes in. And that’s where we’re going to focus our training” (S1). The lead would like to adapt the training each year instead of the current model in which the training may remain stagnant over the course of several years: “And then this way every year people take it, it’s different and it’s not just click, click, click, click, and done...If it’s different all the time, people may pay attention to it” (S1).
Phishing was discussed as an exemplar of how a holistic approach might work. Data from phishing exercises and real-life phishing incidents observed by the agency security operations center can help inform security awareness approaches. For example, the team would like to investigate whether employees in certain job functions are more prone to clicking on phish during exercises. The team lead commented on other ways phishing data could be utilized:

“We’re trying to – this is where the resources come in handy – be able to tie in together the people who take their training to the people who get caught with phishing exercises, the people who are really getting caught with phishing exercises with people who are losing their badges to people who send out information they shouldn’t to see what’s the correlation here. Are these people just too busy? Are they not paying attention? Is there a training problem?” (S1).

It is also important to observe real-life phishing attacks to look for trends and contribute to the design of more realistic phishing emails to be sent out during exercises. The lead said:

“what does the phishing look like that’s coming? Is it people just casting a net, or is there some sort of spear phishing going on? Are they going for the whales?... So, take those things that are actually happening and seeing how your agency is doing against those real-world events, compare it to what you’re seeing in the training. For example, is our phishing close enough to what’s really hitting us so people will be able to tell the
difference? Are they getting the training that they need? Is the application of that training effective?” (S1).

8.4.2 Developing New Incentives

Currently, the agency offers few tangible, positive incentives to the workforce for demonstrating good security behaviors. However, the security awareness team has been brainstorming ideas on how to reward and recognize “cyber champions” in the future (not to be confused with the idea champions cited in Diffusion of Innovations Theory). Although they are still determining criteria, cyber champions are envisioned by team members to be employees who show cybersecurity initiative above and beyond their normal duties. For example, this would include people who report a significant cyber event, provide the security awareness team with an event speaker suggestion, help coworkers with a cybersecurity task, or outwardly promote good cybersecurity practices.

One idea is to hand out poker chips with the team’s logo that could be redeemed for items at the agency gift shop. The team also has considered having the agency CIO present cyber champions with a certificate of appreciation and agency challenge coin (a coin bearing the agency insignia which is given as a sign of achievement or thanks) at the security day events or spotlighting champions in the agency’s newsletter. However, due to a lack of budget and staff, the team has not been able to progress in their proposed incentives initiative.

8.4.3 Broader Reach

Although the team had seen an increase in event attendance by those not in cybersecurity roles, there still remains a large portion of the agency population who choose not to attend security awareness events. When talking about security day event
attendance, the team lead had observed some employees from different mission offices coming, but said, “I want more” (S1). A manager noted:

“Our events are somewhat well-attended, but we know that we get pretty much the same people, a lot of repeat customers, with a few sprinklings of new ones. But we also know that there's a whole set of people that never attend. So, we got to try to figure out a way to reach those people” (M2).

During the employee interviews, two agency staff members also expressed that broader reach is needed. One commented, “You need to get much more of the agency as a whole” (E2). An ISSO said:

“They need to push the support staff, like administrators [to attend security awareness training]. They invite them, but, as an agency, I think more push should come from management to make them attend…They [support staff] are our first line of defense. So I think they need to be properly trained” (E8).

In addition to increasing marketing of events, the security awareness team must look to new ways to increase awareness. Due to employee time constraints and reluctance to step away from work to attend security awareness events, ideas for future improvement center on the team going directly to staff. A manager of an information security organization wondered

“if there is a way to give staff like a 15-minute, ‘Oh, here's what you need to know today about security at [Agency A].’... I don't know what the vehicle would be or anything like that. But something that is much more timely, and I want to say, in your face a little bit about security” (E2).
A manager suggested that the team should consider occasionally attending group staff meetings to briefly talk about security:

“\textit{I don't know if you had a true all-hands for the agency or at the different divisions when they have their all-hands, but those are the kind of things that we're going to start looking at trying to get out in front of}” (M2).

Because of thin resources, M2 also discussed the possibility of having cybersecurity “ambassadors” within each agency mission organization. These would be mission employees who serve as an extension of the security awareness team by keeping up with and passing on security tips and reminders to their coworkers.

8.4.4 Alignment with Other Agencies

The security awareness team strives for strategic growth by trying to align their program with what other agencies and industry security awareness teams are doing. As discussed in section 8.1.1, the team often attends conferences and other agencies’ security awareness events to be exposed to new approaches and hear about lessons learned. They are constantly looking for better ways to gauge effectiveness of the program and align themselves with successful programs:

“\textit{I’d also love to learn are we doing it right, are we doing it wrong, is there a better way we could be doing things? How do we measure ourselves against other agencies when it comes to all this so we can make improvements and I can go back to my management and show them here’s how we stack up against other agencies, not just from a compliance standpoint}” (S1)
The team also incorporates other agencies’ security guidelines into their training. For example, NIST scientists are common speakers at security officer forums and security days. The team also aligns its October security awareness activities with the DHS-sponsored National Cybersecurity Awareness Month.

8.5 Chapter Summary

This chapter details a case of cybersecurity advocacy in action. I describe the progression of the security awareness team from being largely focused on compliance with federal mandates to one focused on advocacy and audience empowerment. As the primary security advocate on the team, the security awareness team lead exhibits both technical and non-technical skills and has a passion for the work and for helping the agency workforce in both their professional and personal lives. The team engages and empowers agency staff by incorporating topics relevant to current agency and societal concerns with a focus of providing information that benefits employees both at work and at home. Communication channels are varied and strive to be engaging with an emphasis on creativity and quality speakers. The team moves beyond simple awareness of security issues and also provide actionable steps employees can take to secure themselves. Various measures of effectiveness, such as surveys, employee feedback, and user-generated incidents, are utilized to gauge security awareness program success. Despite resource constraints, the team strives to continuously improve by introducing a more holistic approach to security awareness, developing new incentives for good security practices, and reaching a broader range of agency employees.

The purpose of the case study was to observe cybersecurity in action over a period of time to augment the self-reported snapshots from the interview study. Chapter 9
synthesizes my research to identify areas in which the case study confirms, contradicts, or extends the definitional boundary of cybersecurity advocates discovered in the interview study.
9 Study Synthesis

The case study was conducted for the purpose of carefully examining the advocacy practices identified in action. This synthesis chapter maps insights uncovered in the two studies in order to reflect on complementariness and explore areas of difference.

9.1 Security Awareness Case as an Instantiation of Cybersecurity Advocacy

The case study is a contributor to the validity of findings from the interview study as an instantiation of the security advocate roles first observed in the interview study. It serves as proof that the generalized properties of advocates and what they say they do (interviews) is demonstrated in real life (case study).

The interview sample was diverse and included advocates working with a variety of audiences, for example, the general public, those in specific sectors, and different work roles. Some advocates had national spheres of influence, while others were concentrated within their own organizations. They served as educators, non-profit directors, security consultants, security engineers, researchers, executives, and security awareness professionals. The interview participants also came from diverse educational and professional backgrounds, with around half having non-technical degrees. Overall, the interview study was a snapshot of perceptions of those working in the advocate role. This effort ultimately illuminated the work practices of cybersecurity advocates and uncovered advocate characteristics within an unbounded variety of contexts.

In contrast, the case study was bounded, context-specific, and longitudinal over the course of a year. It sought to supplement the interview study by investigating one type of security advocate (security awareness professionals) advocating to an audience within a specific sector (U.S. federal government) and one organization (Agency A). The
security awareness team was small, with the team lead serving as the primary advocate and team members serving in support roles. Ultimately, the case study team had the same goal for their audience as the advocates from the interview study: greater awareness of security issues and the adoption of security best practices.

Although more limited in scope, the case study allowed for a richer understanding of the advocate role in context. In addition to gathering self-report data, I was able to observe an entire team and the details of their day-to-day work practices for an extended period of time. The timeframe allowed for obtaining a sense of seasonality of the program and an observation of the evolution of the team’s approaches over the course of a year. Interviews with the organization’s employees revealed perceptions of how the team’s efforts had impacted their own security attitudes and behaviors. The boundedness of the case study also provided a deeper sense of the organization and its leadership. Conversely, in the interview study, each participant was considered in isolation and provided self-reported, higher-level comments and overviews of tasks. This high-level look did not afford an opportunity to observe daily routines, delve into specific organizational characteristics, or talk to advocates’ audience members to gauge effectiveness.

9.2 Advocate Skills & Characteristics

As part of the interview and case studies, participants discussed the qualities and skills of those successful in advocate roles. In the case study, I also had the opportunity to observe qualities of the security awareness team members during their routine work and gained insight into others’ perceptions of them via agency employee interviews. Both
studies revealed similarities in perceptions of characteristics and necessary skills for successful advocates.

9.2.1 Technical Knowledge and Discipline Diversity

Up-to-date technical knowledge of cybersecurity was, not surprisingly, a frequently-mentioned skill in the interview study. This observation was confirmed in the case study. As the primary cybersecurity advocate in the security awareness team, the team lead had strong technical credentials bolstered by decades of hands-on experience. His other security-related job duties and position within a security-focused organization allowed him to keep a finger on the pulse of the technology and the security issues facing the organization. Even though the two supporting contractors did not have a formal background in computing, the entire team maintained relevancy via constant monitoring of security news, establishing professional networks, and aligning with best practices from other agencies.

The interview study also suggested that, although technical knowledge was deemed to be important for gaining technical credibility, it was not viewed as a requirement for every member of an advocate’s team. Technical knowledge was often perceived as something that could be obtained later in one’s career and not contingent on formal educational background. I found that advocates come from varied professional backgrounds, bringing skills developed in diverse fields to their cybersecurity work, and often working in multi-disciplinary teams. Agency A’s security awareness team is an example of such a multi-disciplinary group, with only the team lead having a technical background. The skills brought to bear by the other two team members (e.g.,
interpersonal, marketing, organization) contributed to the progression of the program and demonstrated the benefit of having diverse teams for advocacy efforts.

9.2.2 Non-technical Competencies

Non-technical skills were also deemed necessary for advocates in the interview study. Attempting to understand human nature and practicing interpersonal skills, such as respect for others, listening skills, and flexibility, were seen as instrumental to relationship building. These competencies ultimately allowed advocates to establish trust and gain credibility with their audience. Although fewer unique interpersonal skills were enumerated in the case study (likely due to the small number of advocates interviewed), I observed many of these skills in actual practice during my own interactions with and observations of the team at work. For example, the team regularly took under consideration the feedback and suggestions of employees when planning security awareness events, which alluded to the listening skills identified in the interview study. In addition, during events, team members were friendly and approachable, with the team lead regularly networking with attendees. Ultimately, the team tried to “meet people where they were” in terms of the audience’s background, knowledge, and emotional response to cybersecurity.

Communication skills were frequently mentioned by participants in the interview study as a necessary skill for effective advocacy. Interestingly, none of the case study security awareness team members explicitly mentioned communication skills or the word “communicate” or its derivatives during their individual interviews. However, the lead did provide several examples that implicitly indicated that communication skills were vital in security awareness. For instance, he did not have formal training in
communications but said, “I wish that I had some sort of training on being a teacher” (S1). He also mentioned the importance of marketing security awareness efforts to leadership and the workforce, his ability to describe technical topics in more general terms, and how he was asked to fill in at “Take Your Child to Work Day” because of his prior speaking experience. All of these references are examples of communication skills.

Lastly, in both studies, context awareness was seen as instrumental in discerning which advocacy approaches to use, determining what topics to cover, and tailoring security risk communications to the audience. The majority of advocates from the interview study targeted organizational audiences holding a variety of roles, such as senior leaders, technical staff, developers, or employees. As such, they had to be cognizant of organizational attributes, constraints, motivators, and challenges when formulating an advocacy plan of action. For instance, interviewees spoke about being aware of and then appealing to organizational values (such as profit) when communicating to senior executives. An advocate who worked with software developers discussed framing the benefits of secure development in terms of developer-centric incentives such as the avoidance of unplanned work and productivity boosts if code is developed securely from the start. The term “translation” was repeatedly used to describe the combination of communication skills and context awareness advocates employed to tailor messages to less-technical audiences. For example, an attorney-turned-security-advocate drew on his law background to translate security concepts into terms that would resonate with other attorneys.

The security awareness professionals in the case study were also obviously organizationally-focused. Like those interview study participants who advocated within
their own organizations, the team was intimately familiar with the organizational context of their agency. The team lead was particularly knowledgeable given his many years of service at the agency. The case study provides clear examples of how being context aware contributed to the evolution of the program. For example, the team incorporated employee preferences and needs related to security awareness events by actively seeking out feedback with post-event surveys and focus groups. They also ensured events were topical to security issues relevant to the organization and its use of new technology, for example cloud storage and secure email exchange with agency stakeholders.

Instead of targeting a particular group within the agency, the team’s sphere of influence encompasses all roles within the organization. This presents a unique challenge in constructing meaningful security risk communications and guidance that resonate with employees having diverse technical/security skillsets and job duties. Some efforts, such as the security officer forum, were geared toward those with security and IT roles in the organization, so could be more technical in nature. However, other security awareness efforts, such as the “Click with Care” campaign, were targeted at the entire workforce, regardless of technical knowledge. As such, the message was tailored to be understandable to everyone, using simple terminology and providing links to extra resources for those who needed it. Lunchtime events were similarly designed to appeal to multiple roles in the organization with the different tables allowing people to pick and choose those topics most relevant to them. Security days were also targeted at the entire organization. Therefore, selected topics had to appeal to multiple interests. Based on feedback survey responses, security day attendees appreciated the diversity of topics. For example, after one event, an employee commented, “You have always provided a wide
variety of speakers and topics. Please keep it up.” However, when trying to appeal to disparate groups, the team could not please everyone all the time and sometimes missed the mark. This was evidenced by feedback survey responses in which some employees wanted to see more technical topics, for example, “data-at-rest/data-in-transit encryption; SSL/TLS encryption,” while others wanted more simplified “cookbook instructions on how to protect one’s home networks and digital devices.”

9.2.3 Service Orientation and Pro-social Passion

Evidence of advocates possessing a service orientation was found in abundance throughout my research efforts. Advocates in both studies generally had an inclination to help people navigate the complexities of cybersecurity to “make their life easier and protect themselves” (S1). Interview study participants often saw themselves as having an education role, which was reflected in their teaching and security awareness work. They also viewed the work as selfless. For example, a participant said that what she does is “for the best interest of the organization. It’s not for [my] glory” (P03). In the case study, the security awareness team lead talked about his desire to make a positive impact in whatever job he does.

Service orientation was also accompanied by a sense of passion for the work. One participant said, that it “gives me a great deal of pride to be able to do this kind of work and to be able to help as many people as possible” (P01). Others commented that passion was integral to the job since changing people’s behavior and mindsets is a difficult task: “You have to have the passion there because you’re still having to smash through a lot of barriers” (P10). The Agency A security awareness team lead likewise expressed his passion, believing that his efforts help the organization as a whole. Although his job
responsibilities are split between security awareness and other security tasks, he felt that security awareness is the most important duty he has.

However, with respect to service orientation, there are some differences in perceptions of potential impact between the more diverse set of interview participants and the smaller case of the security awareness team. Several interview participants had large spheres of influence, so viewed their potential impact as greater, for example, to "save lives through security research" (P11). One participant was passionate about securing critical infrastructure because "without critical infrastructure, society cannot operate" (P20). Other participants, although having a smaller audience, viewed themselves as being a contributing member of a larger cybersecurity collective with the ability to have a ripple effect. For example, one advocate talked about her corporate and community advocacy work: "I know that I have done something that could impact millions of people, maybe not immediately, but in some significant amount of time" (P23).

In contrast to advocates with broad-impact potential, the case study team’s sphere of influence was primarily the agency workforce. The team lead exhibited the same pro-social passion as the advocates in the interview study but recognized the smaller scope of his influence. However, the team did view impacts as extending beyond the organization and into employees’ personal lives, including transfer of knowledge to family and friends, which echoes the ripple effect expressed by several in the interview study.

9.2.4 Motivations

The interview study identified several intrinsic and extrinsic motivators for security advocates: personal interest, self-efficacy, sense of duty (service orientation), evidence of impact, comradery, and awards/monetary compensation. Several of these
motivators were less evident from the case study likely due to the small sample size of advocates. For example, comradery was not explicitly discussed as a motivator, although the security awareness team did frequently engage other organizations in their security events and attended external events to learn about the state-of-the-art in security awareness approaches. Awards and monetary recognition were not discussed within the case study at all, perhaps due to limited salaries and merit compensation for government employees and contractors. In addition, working in a federal agency, there may be a public servant mentality in which serving one’s country is deemed more important than high salaries. Lastly, self-efficacy was not outwardly expressed by the security awareness team. Although the security awareness lead did feel like the program was making progress, he admitted that he and his team were relatively new to security awareness, having only taken on that role three years prior: “Every time we go and try something it’s for the first time, at least for me, because I have zero experience doing this” (S1). He also repeatedly articulated his desire and impatience for the team to continue to progress.

The advocates in the case study did, however, share several common motivators. From a personal interest perspective, S1 expressed a passion for and curiosity about technology while S2 mentioned her passion for training. Although S2 and S3 did not have a formal background in cybersecurity, they discovered a growing passion for the field after working on the security awareness team. The team also relied on evidence of impact - including metrics, praise, and observations of employee behaviors - to gauge their current progress and push them towards improving their program and reaching more people within the agency. The most significant similarity was a sense of duty/service.
orientation which was largely shared among advocates in both studies as discussed in the prior section.

It is also valuable to examine motivations related to the avoidance of negative consequences. Interestingly, whereas some interview participants were keenly aware of consequences should security advocacy efforts fail (e.g., loss of life, breach of national security, economic loss, identity theft), the security awareness team members seldom alluded to consequences of their security awareness program not being effective. The team lead did discuss the potential of employees falling victim to phishing attacks or having sensitive information exposed but was not specific about how these events may directly impact the mission of the agency in its protection of national critical infrastructure. However, interviewed managers and several interviewed agency employees recognized that a security breach of the agency could lead to stakeholder’s sensitive information being compromised and critical infrastructure being at risk.

9.3 Organizational Challenges to Cybersecurity Advocacy

The interview study identified several perceived organizational challenges to cybersecurity advocacy and adoption, including weak security culture, economic barriers, cybersecurity workforce issues, and policies (discussed in Chapter 5). Similar challenges were found within Agency A. Table 6 shows a mapping between interview study and related case study challenges. Note that all challenges identified in the case study relate to those found in the interview study. However, one interview study challenge pertaining to the lack of relevance of overarching cybersecurity policies did not map to the case study. This does not mean that the challenge did not exist, just that it was not observed during the course of case study data collection. In addition, since the case study was more
focused on one particular agency, challenges were more limited in scope as compared to interview study challenges. This was likely because many of the interview study advocates had worked with multiple, diverse organizations, and, therefore, had more opportunity to observe challenges and place them into context in different ways. These differences also contributed to the different terminology I initially used to code challenges in the case study as compared to the interview study. For example, in the case study, lack of resources was the only economic challenge mentioned by the team and managers, all of whom worked in the same office. However, in the interview study, economic barriers were described more broadly by advocates observing organizations from different perspectives and included challenges such as difficulty in showing return on investment.

Table 6

*Interview study challenges mapped to case study challenges*

<table>
<thead>
<tr>
<th>Interview Study Challenge</th>
<th>Related Case Study Challenge</th>
<th>Synthesis Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak security culture</td>
<td>Lack of workforce buy-in</td>
<td>9.3.1 Cybersecurity Culture and Buy-in</td>
</tr>
<tr>
<td>Economic barriers</td>
<td>Resources</td>
<td>9.3.2 Economic Barriers</td>
</tr>
<tr>
<td>Cybersecurity workforce – Skilled workforce shortfall</td>
<td>Resources</td>
<td>9.3.2 Economic Barriers</td>
</tr>
<tr>
<td>Cybersecurity workforce – Failure to consider the human element</td>
<td>Human error</td>
<td>9.3.3 Human Element</td>
</tr>
<tr>
<td>Policies and regulations – Compliance-driven cybersecurity</td>
<td>Compliance-driving training</td>
<td>9.3.4 Compliance-driven Cybersecurity Awareness</td>
</tr>
<tr>
<td>Policies and regulations – Lack of relevance</td>
<td>N/A</td>
<td>9.3.5 Policy Relevance</td>
</tr>
</tbody>
</table>

This section synthesizes organizational challenges uncovered in the studies as categorized in the last column of Table 6. Commonalities and differences in advocates’ strategies for overcoming these challenges are highlighted in sections 9.4, 9.5, and 9.6,
which discuss techniques, audience empowerment, and measures of effectiveness respectively.

9.3.1 Cybersecurity Culture and Buy-in

The interview study identified weak security culture of an organization as being an impediment to security adoption. A lack of management buy-in can be especially problematic due to potential negative impacts to security resourcing and enforcement if security is seen as a low priority. In the case study, I was able to go beyond the interview study’s general observations of culture and gather multiple perspectives (although limited) of Agency A’s security culture and level of buy-in for security awareness training along. Case study findings also revealed specific examples not afforded in the interview study.

Case study interviews with agency security awareness team, managers, and employees revealed mixed opinions about culture with some thinking the agency has a strong security culture and others doubting the commitment to security. Security is championed by the Office of the CIO and other security-focused groups and is communicated as a priority for the agency as a whole. However, a lack of buy-in for the importance of security was observed among managers and employees in mission elements who may view security as an afterthought and not relevant to their work. This observation was also a common negative perception reported by advocates in the interview study. With respect to agency leadership buy-in, the security awareness team had the ear of their direct line of management within the office of the CIO, but it was unclear as to the influence they had on other agency leaders beyond interactions during role-based training classes. In addition, the workforce may not see the value of security
awareness training, instead only completing the required minimum, while some managers
discourage employees from spending time away from their assigned duties to engage in
security education.

9.3.2 Economic Barriers

Economic barriers mentioned in the interview study included lack of resources
and unclear return on investment. The case study did not uncover findings directly related
to return on investment and how it might be considered by agency leaders. In addition,
even though managers were asked how security awareness resource allocation decisions
were made, answers were vague. Ultimately, the case study did not delve into how
resources for security awareness are allocated at higher levels and if and how the team
may be able to influence those allocations. However, lack of resources (budget for
personnel and program expenses) was cited by both the team and managers. Despite
progress made with the security awareness program over recent years, economic
priorities for security awareness have not changed. The agency has not adapted its long-
term personnel allocations to allow for a full-time security awareness lead, instead
choosing to assign lead duties as part-time (50% of S1’s duties) and investing all the
security awareness operational budget into the two supporting contractors.

Lack of resources is also closely related to the skilled cybersecurity workforce
shortfall challenge discussed in the interview study. The interview study participants
spoke more broadly about the cybersecurity workforce shortfall, while the security
awareness team and its managers were more focused on their own resource issues. Within
Agency A, there was a need for more security awareness personnel to expand the
program, for example by revamping the annual training or for helping to analyze security incident data to inform training and contribute to measures of effectiveness.

9.3.3 Human Element

The interview study included a fair number of participants who are deeply technical and advocate technical solutions and tools that are targeted at security and IT professionals, including security frameworks and checklists of recommended security settings. In these cases, the advocates and their audience have much common ground, for example with respect to technical language, and exhibit high homophily, which is the “degree to which a pair of individuals who communicate are similar” (Rogers, 2003, p. 305). However, when addressing less-technical end users, participants noted that some security professionals experience a disconnect in relating to their audience and fail to consider the human element when designing, recommending, or implementing cybersecurity solutions and processes. They may treat users as the weakest link and do little to move beyond technical solutions to understand the complexity of human behavior change and how people can be part of the solutions. Or they may place unrealistic expectations on employees instead of focusing on putting solutions in place to filter out potential threats as much as possible (e.g., phishing filters) or serve as technical stop-gaps when (not if) employees make poor decisions. This sentiment was demonstrated when several participants spoke about naive expectations that annual security awareness training should result in employees making all the right security decisions. When employees eventually failed, security professionals would view users as stupid and hopeless instead of investigating ways in which users could be better guided and educated.
In contrast to those working purely with security and IT teams, the case study security awareness team was charged specifically to focus on people and their behaviors, not the technology. The team lead noted that the people “are the most important cybersecurity tools” (S1) available to the agency. Therefore, the team took a human-centric approach. For example, they often selected topics that appealed to people’s emotions (e.g., a household safety topic at a lunchtime event) or illuminated human perceptions and limitations (e.g., a security day guest speaker talking about security fatigue). The team was also aware of demands placed on employees, so tried to adapt their security awareness approaches to accommodate those. This adaptability was illustrated when phishing reminder postcards were put on people’s desks after team members realized that employees were not reading reminder emails. Interviewed agency employees also recognized their own cognitive and security skill limitations and susceptibility to distraction and the general busyness of work life. Several expressed their fear that, even though they felt better educated on security than they once were, one day they would slip up and click on a phishing link.

9.3.4 Compliance-driven Cybersecurity Awareness

Interview participants talked broadly about issues with organizations focusing solely on cybersecurity compliance while the case study focused more on compliance related to security awareness training. In the interview study, only four interviewees were currently working or had worked as security awareness professionals. However, others had observations about how security awareness training contributed to or detracted from advocacy efforts. Study participants generally described mandatory security awareness
training as being a rigid, mind-numbing, “check-the-box” activity with questionable impact on employee behavior.

The case study mirrored perceptions of the challenges described more generally in the interviews as the security awareness team is faced with the non-trivial task of finding a balance between federal security awareness training requirements and what works best for the agency and its employees. The team lead echoed interviewee sentiments that traditional, computer-based training can be monotonous, and compliance metrics can be misleading in portraying effectiveness of the program.

9.3.5 Policy Relevance

Advocates in the interview study discussed how broad policies pushed down from high levels of government do not consider the unique context of organizations further down in the hierarchy. In addition, they lamented that high-level policy makers may lack security expertise, which results in flawed policies. Several participants mentioned the difficulty in advocating for change at leadership levels, particularly with respect to the importance of framing security in terms understood and seen as valuable by those in these positions. However, this was an underexplored area.

Policies were not mentioned as challenges in the case study. This is likely because the security awareness team had no influence on overarching cybersecurity policies as compared to several of their interview counterparts, rather were among those tasked to comply with the mandates. The security awareness program appeared to be more driven by security happenings observed within the organization rather than their program feeding into agency-specific security policies. Furthermore, although the agency has a program for security enforcement that is housed in an office separate from the security
awareness team’s CIO office, the team lead said that his team has no direct input into the program. However, they do maintain a relationship with the enforcement program’s personnel and exchange relevant information. In addition, there was some evidence of influence over how security training policies were executed within the agency, for example, how role-based training requirements were changed in recent years to allow for attendance of security awareness events.

9.4 Advocacy Techniques

Many of the cybersecurity advocacy techniques and approaches identified in the interview study were demonstrated in the case study despite the case study being much more limited in context. In this section, I discuss similarities and differences between the studies’ findings regarding communication channels, how advocates make security relevant to the audience, use of rhetorical devices, motivation via external rewards and consequences, and how advocates might influence technical solutions.

9.4.1 Communication Channels

Advocates in the interview study used a variety of communication channels in their jobs that were also employed by the security awareness team in the case study. Among these channels were focused campaigns, classroom and online training, games/contests, and small and large group events. When audience members are not able to attend events in-person, webcasts and recorded videos are utilized. The team also disseminated security information via written materials/handouts, posters, and email.

The case study provided an opportunity to see and experience many of the communication methods described more broadly in the interview study. The security awareness team organized small group events (e.g., lunchtime drop-in events) and large
groups events (security officer forum and security day) featuring engaging internal and external speakers and topics of interest to the workforce. The lunchtime events in particular were an opportunity to employ more entertaining approaches (e.g., the Shakespeare-themed event, game/trivia tables, and the late-night TV themed event). Various campaigns also tried to connect with employees in a more physical way, for example with reminder postcards and candy.

There were differences, however, between communication channels mentioned in the two studies. Most of the lunchtime events catalogued in the case study, but only one of the observed lunchtime events, were held in an informal station format, with attendees dropping in to peruse content at several tables. The format worked well at Agency A to catch employees’ attention as they walked between buildings or to the cafeteria, allowing them to participate as little or as much as they wished. This type of event was not noted in the interview study. Creative approaches were mentioned in both studies, but few examples of what was meant by “creative” were provided in the interview study. Creativity was emphasized among the case study team as a way to attract employees to events and better facilitate recall of security information. Creative approaches may be easier for advocates, such as the case study team, that are more intimately familiar with the culture of the organization and what approaches might resonate with the workforce.

There were also significant differences in written materials based on scope and audience. Since the team’s audience was smaller in scope than many of the advocates in the interview study, they did not have the opportunity (or need) to develop over-arching frameworks or communicate via mass media. Furthermore, the team did not engage in technical report writing, rather focused on post-event reports aimed at marketing events.
and success indicators. The team also produced written materials targeted at agency staff which were largely presented in more manageable chunks (e.g., postcards with tips or one-page handouts) versus longer white papers geared towards technical audiences. Social media was mentioned frequently as a communication medium in the interview study, but was not utilized by the security awareness team, likely because they are internally focused and do not have access to any internal social media platforms.

9.4.2 Making Security Relevant

In order to convince people to adopt security best practices, they must see the relevance and benefit of security to their own lives, whether it be at work or at home. Advocates attempt to establish this relevance first by being keenly aware of the environment of their audience, including what they care about, their constraints and skill levels, and their goals when working online with computers. Both studies identified three major ways in which advocates translate audience context into security promotion: linking security to the business mission (in the organizational context), topicality, and establishing a work-home connection.

A number of advocates in the interview study worked to convince organizations of the business value of implementing security best practices, attempting to sell “security as mission assurance, revenue assurance, reputation assurance” (P02). To affect organizational security culture, persuasion must be effective across all levels of the organization, from front-line staff to senior executives. In the case study, employees working in cybersecurity roles obviously made the connection between security awareness and their jobs and had a better understanding of the importance of security to the organization’s mission. However, several agency employees believed that, despite
marked improvements in recent years, the security awareness team could do better in linking security awareness to the missions of the various non-cyber groups within the agency. This was evidenced by relatively low (but growing) attendance of non-cyber employees during security awareness events and mission leadership questioning the value of their mandatory training. As part of their plan for continuous improvement, the team has considered efforts to engage employees within their own work spaces, e.g., during group meetings, instead of expecting them to come to security awareness events on their own.

Relevance was also viewed as being established by explicitly linking security communications to known or pressing features of people’s daily lives. Both studies revealed that security advocates put great effort into making their security communications topical, whether that be related to hot security topics in the news, pressing issues within an organization, or seasonal activities. In the interview study, several advocates mentioned the importance of staying abreast of the latest security happenings within their audience industry sectors in order to link those to security advice. Others capitalized on current events and time of year, as expressed by a non-profit director:

“*When the iron’s hot, you strike. So, it’s current events, or something happens, that’s an opportunity because their awareness is already heightened to maybe sneak in there a little bit more and educate them a little bit more about that issue. Tax time, we have a tax time tip sheet*”

(*P24*).
The case study provided specific examples of how topicality played a role in their program. Seasonality was exemplified by themes of security awareness events, for example the “Cyber Kickoff” lunchtime event that occurred just prior to the Super Bowl. In addition, the team constantly scanned for security items of interest in the news and also incorporated recent agency security threats, for example people sending unencrypted emails with sensitive information, into their events.

The security awareness program strongly emphasized the work-home connection. This connection was viewed as especially important given employee opportunities to occasionally work from home. The team also felt that good security habits are easier to form when they permeate someone’s entire life and do not just end when they leave the office. Conversely, establishing a work-home connection via security advocacy was only mentioned by three participants in the interview study. This may be because the advocacy work of many of the interview participants was targeted at security activities that might not translate into a home setting, for example, secure software development and IT administration.

9.4.3 Use of Rhetorical Devices

Advocates in both studies felt that cybersecurity advocates must promote security in understandable and appealing ways that attract attention and encourage knowledge retention. Engaging personal experience and demonstrating relatability may sometimes require more creative approaches, which were often manifested by the use of rhetorical devices in both written form and during presentations. Advocates in the interview study mentioned various rhetorical devices they employed which included metaphors, humor, and allusions/pop culture references. These devices were most often discussed in general
terms. The case study, however, provided concrete examples of rhetorical devices being used in practice. A list of rhetorical devices common to both studies, along with examples, is included in Table 7.

Table 7

<table>
<thead>
<tr>
<th>Rhetorical Device</th>
<th>Interview Study Example</th>
<th>Case Study Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alliteration</td>
<td>Talked to audience about three Cs of security awareness: communication, collaboration, culture (P09)</td>
<td>“Click with Care” campaign</td>
</tr>
<tr>
<td>Allusion/pop culture reference</td>
<td>In a talk, used a line from the movie “Terminator” about the Terminator not being able to be stopped to describe threat actors (P06)</td>
<td>“To Send or Not to Send” lunchtime event</td>
</tr>
<tr>
<td>Humor</td>
<td>“Two-raptor authentication” - two-factor authentication (P23)</td>
<td>“Take your training now and not later” reminder postcards with Now-and-later candy attached</td>
</tr>
<tr>
<td>Imagery</td>
<td>Used an image of “fog” to convey people being “paralyzed by abundant options” in technology and security (P04)</td>
<td>Click with Care campaign logo that uses a caution street sign (see Figure 4)</td>
</tr>
<tr>
<td>Lists and principles</td>
<td>Published annual top 10 list of security issues encountered by non-profit members (P15)</td>
<td>“Three clicks of death” featured in the Click with Care campaign</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. clicking on a link you shouldn’t visit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. clicking on an attachment you shouldn’t open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. clicking send on an email you shouldn’t send</td>
</tr>
<tr>
<td>Metaphors and analogies</td>
<td>Security likened to a deadbolt on a door (P23)</td>
<td>“Cyber Hygiene” themed lunchtime event</td>
</tr>
<tr>
<td>Parody</td>
<td>Not mentioned</td>
<td>Late Night Cyberside Chat lunchtime event in a late-night television show format</td>
</tr>
<tr>
<td>Narratives/anecdotes</td>
<td>Shared her own personal identity theft story during a media interview (P07)</td>
<td>At a lunchtime event, a police officer educated staff about credit card skimmers using stories of and examples of skimmers.</td>
</tr>
<tr>
<td>Slogans and taglines</td>
<td>“Food for Thought” cybersecurity food truck event (P26)</td>
<td>Branded events (anonymized in this paper) and themed names for individual events, e.g., “Traveling Cyber Safe” lunchtime event</td>
</tr>
</tbody>
</table>
Due to the more granular data collection of the case study, I also identified rhetorical devices not mentioned in the interview study. The security awareness team makes extensive use of parody, as exemplified by the lunchtime event that included a cyber spin on excerpts from Shakespeare’s plays (Lunchtime #2) and the event that mimicked a late-night television show (Lunchtime #3). The team also sometimes uses puns in event themes. For example, the security officer forum event “Get Your Head Out of the Cloud,” which was focused on providing information on federal cloud data storage initiatives, was a pun of the idiom “get your head out of the clouds.”

9.4.4 Extrinsic Incentivization

In both studies, achieving intrinsic motivation for cybersecurity adoption was seen as an important goal. However, advocates in the interview study believed that extrinsic motivation, especially via positive incentives, might be able to play some role as well. Specific incentives mentioned by interview study participants included contests, raffles, personal thanks, and small tokens or rewards for going above and beyond compliance requirements. Negative incentives for individuals, such as job termination for being a repeat clicker during phishing exercises, were generally viewed as unhelpful. Organizational incentives were viewed as being more complex, relied on making a business case, and were often a mix of positive and negative. For example, advocates believed organizations could be incentivized by estimating how security best practices could ultimately save the organization money with the flip side being how much money or reputation could be lost if a security breach occurred. Some believed that executives of companies that make poor security decisions should be held legally liable.
Conversely, positive incentives were not largely discussed in the case study beyond employees being able to earn role-based training credit by attending security awareness events, indicating a potential area of exploration for the security awareness team. As mentioned in Chapter 8, the team has brainstormed ideas for offering positive incentives, but has not progressed in this due to resource constraints. The team did, however, mention two negative incentives. In addition to having to take extra training if an employee clicked on a phish during phishing exercises, the employee’s supervisor could be notified for repeat clicking. In addition, employees would have their accounts locked out if they didn’t complete their annual cybersecurity training on time.

9.4.5 Influence on Technical Solutions

A number of advocates in the interview study mentioned that part of their advocacy efforts focused on influencing technology. Influence came in several forms, including championing technology automation to remove burden from security staff and end users, promoting usability of security solutions, and influencing vendors to produce products with built-in security. A participant discussed his team’s efforts advocating security automation technology to IT vendors:

“One of our philosophies today in the area of security automation is we want ultimately, want an ecosystem where any organization that buys technology, they can’t buy technology without this stuff coming as part of it. So, influencing the vendors to deliver that kind of stuff better is another way of influencing security” (PO5).

Several usable security champions discussed efforts to influence technologies that alleviate user burden and serve as a backup line of defense for human limitations: “My
goal in usable security is how can we eliminate the user from the security problems. How can we fix the underlying system so that the user’s poor practices don’t matter?” (P16).

However, the case study security awareness team did not appear to have this same influence on technical solutions. This is likely because their efforts were more internally focused and scoped to human-centric security awareness efforts (as discussed in section 9.3.3). There also was no mention of how their observations of employee struggles with security were communicated to technical staff in order to affect change.

9.5 Audience Empowerment

Audience empowerment was a prominent concept perceived as important in both studies. Empowerment was viewed as helping to overcome organizational challenges, such as weak security culture/buy-in and failure to consider the human element, as well as individual’s negative perceptions of security as described in Chapter 5. Interview study results revealed that effective advocates are seen as those who view their audience as capable partners rather than unaware actors or antagonists. Ultimately, advocates aim to move people away from viewing security as a “have to do” towards it being a “want to do,” as expressed by an interview study participant:

“People are interested in protecting themselves. But how do I tap into that...so people can actually intrinsically choose to do it and not out of compliance. I really want to see what programs would look like if you could generate, if you could tap into that source” (P21).

The case study security awareness team had a similar goal and saw this shift in motivation as integral in evolving beyond a compliance mentality in which security
awareness training is seen as a mandatory burden. I observed the team’s attempts at changing workforce attitudes via techniques discussed in Chapter 8, for example, by trying to make security awareness events more entertaining and establishing connections between security and people’s work and personal lives. The team also engaged the workforce in becoming partners in security awareness by incorporating employee suggestions into events.

It is also interesting to note the perceived role of fear motivation in audience empowerment. Interview study participants agreed that advocates must be honest about risk and that fear can be motivational. However, too much fear may result in paralysis, which is contrary to empowerment. Although fear was talked about extensively in the interview study, it was not explicitly discussed by the case study team in terms of it being a motivator. However, the team lead and his managers did speak to some degree about security threats to the workforce and how those were addressed during events. In addition, several employees also reflected on how some talks at events scared them into examining their own behaviors, for example, relating to social media usage. However, one employee discussed the possibility of people being overwhelmed by fear-based security awareness communications if those are sent out too frequently: “We can't always send out announcements scaring people because there'll come a point where they'll just be numb to it and won't even respond” (E5).

Advocates felt that they must then strike the right balance when communicating security threats. The interview study suggested that part of the job of a security advocate is encouraging self-reflective security behavior and a sense of agency to make informed decisions, i.e. audience empowerment. To this end, advocates follow up awareness of
security threats with the proper knowledge and tools, for example in the form of actionable, practical recommendations. Advocates also must engender within their audience a feeling of hope that protection from security threats is possible and doable even for with fewer technical skills.

These findings were confirmed in the case study. Security awareness events often included speakers who talked about threats and provided recommendations. Lunchtime events, campaigns, and handouts provided concrete guidance and suggested tools in terms non-technical workforce members could understand. In addition, as evidenced by employee interviews, the security awareness team was viewed as an approachable, credible resource should questions arise.

9.6 Measures of Effectiveness

Advocates in both studies reflected that it is difficult, but necessary, to measure the effectiveness of security advocacy efforts beyond simple compliance metrics. An interview participant remarked:

“Even though [institutions are] training more faculty and staff on information security issues because of compliance requirements, it’s hard to always be sure that your message is being heard. It’s hard to measure when someone didn’t fall for a phishing message or with something that didn’t happen” (P15).

Evidence of success not only serves as a motivator for advocates, but also helps to inform future advocacy approaches and convince organizational leaders of the value of security advocacy efforts and the need to allocate adequate resources towards those.
Interview study participants revealed how they conceptualize whether they are doing a good job, for example, trends in incident data, attendance/views, and personal feedback. In the case study, I was able to go deeper into understanding this conceptualization, discovering that attempts at finding meaningful measures of effectiveness were often best-effort, imprecise endeavors. Measures were collected formally (e.g., via post-event surveys) and informally (e.g., face-to-face feedback) and involved both quantitative data (e.g., phishing click rates, attendance numbers, and number of user-generated incidents) and qualitative data (e.g., employee comments, manager feedback). The team and its managers also held hope that better measures could eventually be found, for example, by learning from what other agencies are doing or jumpstarting a more holistic approach involving the agency’s security operations groups.

9.7 Chapter Summary

The interview study began to form a picture of the work of cybersecurity advocates through self-reports. To validate interview findings, the in-depth case study provided a clearer understanding of what advocates do in real life. This chapter described areas of alignment and divergency between the two studies.

In the case study, I observed many of the advocate characteristics and technical and non-technical skills identified in the interview study. Although professional motivations were explored more deeply in the interviews due to the larger sample of advocates, I found that the security awareness team was also motivated by passion for the technology and training, evidence of impact, and a sense of duty/service orientation. Both studies shed light on perceived impediments to advocate work, including organizational
culture and buy-in, economics, human nature, and a compliance mentality. However, policy issues identified in the interview study were not observed in the case study.

Advocacy techniques categorized in the interview study at an aggregate level were observed specifically in the case study. Both studies found that advocates use a variety of communication channels and aim to make security relevant to their audience. The case study demonstrated participants’ view of the importance of tailoring approaches to context via examples of tactics that worked well in that particular organization. For example, there was an emphasis on the work-home connection and frequent use of parody to engage the workforce.

Finally, audience empowerment was prominent in both studies as advocates try to increase their audience’s intrinsic motivation to adopt security best practices. Measuring the effectiveness of those techniques was universally viewed as difficult but pursued using any available means, such as audience feedback, compliance metrics, attendance/views, and trends in user security incidents.

The synthesized findings feed into the final discussions and conclusions in the next two chapters. Chapter 10 discusses possible applications of my findings. Chapter 11 summarizes the overall contributions of my research to both the research body of knowledge and the security practitioner community.
10 Implications

Although there have been research studies exploring techniques to encourage security best practices and technology adoption, there is much to learn from successful practitioners who are engaged in this activity on a regular basis. These findings can be used to influence the creation of cybersecurity professional development frameworks, advance risk communication within the cybersecurity domain, and contribute to resources for others working in a cybersecurity advocate role. This chapter focuses on the practicalities of what can be done with my research findings. Although some references to related work are included in this section, a more detailed discussion of how my research integrates with the research body of knowledge is provided in Chapter 11.

10.1 Defining the Emerging Cybersecurity Advocate Role

The interview study and case study begin to uncover the uniqueness of the cybersecurity advocate role versus traditional IT or cybersecurity professionals, such as analysts, administrators, and system architects. In some meaningful ways, the practice of securing a system appears to be different than advocating for securing a system. Yet, there is no professional preparation for the latter. An analogous situation was the foundation of human factors/usability engineering as a profession distinct from other disciplines such as testing or business analysis. This was rooted in a discovery that human errors in systems were fundamentally different than system errors. As a result, this observation necessitated different approaches. Similarly, there appears to be a new and rapidly growing need for security professionals with a special set of advocacy skills and techniques. In this section, I describe how my research findings can be used to encourage the development of advocates having the skills necessary to be successful.
10.1.1 Defining an Advocate Career Track

Advocates in the interview study tended to be advanced in their careers, having built on prior real-world experience in both security and non-security fields. Many became advocates by chance, with no pre-mediated intention. Phrases used to describe their progression to advocate included “fell into it” (P24), “accident” (P08), and “a perfect storm of good stuff that fell together” (P14). Two members of the case study security awareness team also had no initial plans to work in the cybersecurity field but found that their skillsets could be useful in developing a training program. While recognizing that career paths are often influenced by happenstance, one may wonder if more people might aspire to become a cybersecurity advocate if there was a defined career track for this role. A formalization of the role could aid in both recognition of the possibility of such a career and in the preparation to become an advocate.

Currently, there is no such formal career track. Most of the emphasis within today’s security professional development curricula is on gaining technical knowledge (McGettrick et al., 2014; NSA, 2020; Newhouse et al., 2017). A quick review of cybersecurity work roles in these guidelines reveals that none contain a set of skills that resemble the work of a cybersecurity advocate. This gap suggests the development of a more formalized definition of the advocate role may be needed. This need requires enumeration of advocate knowledge, skills, and abilities, all of which have been uncovered in my research. My recommendations are in-line with a recent, promising proposal from the SANS Institute to establish a formal NICE framework work role for a “security awareness and communication officer” who “builds, maintains and measures
the organization’s security awareness and communications program with the goal of securing the workforce’s behaviors and ultimately creating a secure culture” (SANS, 2019b). As a security awareness community organizer and leader in security awareness education, SANS recognized that no current work role adequately describes a security awareness professional. The proposed work role includes a variety of non-technical skills similar to those identified in my research, including communication, partnering, and behavior modeling.

In addition to a formal work role, there is a need for the development of continuing education efforts to aid in the progression to cybersecurity advocate from both security and non-security fields. For those coming from fields outside of IT, efforts may focus more on how to apply non-technical skills in the cybersecurity context as well as provide resources for mastering technical concepts.

10.1.2 Bolstering Non-Technical Competencies

Cybersecurity is often viewed from a technical perspective, with technology and tech thinking seen as the solutions to security problems. While technical knowledge is important, those trained only in computing disciplines may not have all the skills to be an effective advocate. Even though there is general agreement within the security community that people contribute to security problems, advocates in my studies felt that security professionals often do not specifically address people considerations because they may not be equipped to do so. Rather, there is an over-reliance on employing technology to solve socially-grounded problems. Cybersecurity advocacy requires a fundamentally different approach that is not techno-centric and considers security problems through a social science lens.
The interviews suggested that having a well-rounded approach by being able to address social and organizational factors may be more imperative than the technical solutions alone. All 28 interview participants and the case study security awareness team members mentioned non-technical skills and abilities when asked to describe qualities of those successful in security advocacy. Competencies most often mentioned were interpersonal skills, context awareness, and communication skills.

Some had formal training in the social sciences or humanities or a field in which non-technical skills were interwoven within the curricula as essential for success in that field. As an example, lawyers do not just know legal matters, but also how to adequately communicate and sell their position; therefore, it is not surprising that several lawyers-turned-advocates were represented in the interview study. Others mentioned the importance of mentorship and how they learned hard lessons on-the-job that made them realize the importance of non-technical skills. For example, a former security executive described how he took a less-than-successful hardline approach the first time he presented a report to his company’s CEO. Afterwards, he was mentored about alternative approaches:

“My boss pulled me…and he said, ‘Let’s work through how you do these future briefings in a way that they’ll understand. They’ll hear you, and they’ll understand.’ So, it became less about smacking them in the face and more about showing how it affected the company, using examples, and kind of softening the language. And again, knowing the audience” (P02).
These observations highlight the importance of context-specific mentoring and continuing education in addition to integrating non-technical skills into formal computing education.

The studies also revealed that cybersecurity advocates demonstrate an innate understanding of human behavior and persuasion. Although the security advocates seemed to consider the human element (even if subconsciously), they suggested that other security practitioners may not share this basic interpersonal orientation. These practitioners often contribute to negative perceptions of security by not taking the human element under consideration when describing, designing, administering, and enforcing security mechanisms. The advocates revealed a desire to move away from the common security practitioner perception that “employees are the weakest link” (P21) to instead regard users and security professionals as capable partners. To be effective, my study results suggest that advocates should be more socially-oriented, skilled in persuasion and communications, and more context-aware than their non-advocate colleagues.

To address the nuances of advocates’ work, education efforts might encourage the development of an organizational change agent skill set, as described by Markus and Benjamin (1996). Like advocates, change agents work to facilitate change, build a solid information exchange relationship, and attempt to ensure long-term adoption. These researchers proposed a preparatory course that includes units on approaches, personality characteristics, how to cope with challenges, ethical considerations, and awareness of environmental conditions. Building on this foundation, Table 8 outlines a proposed educational program that modernizes and tailors the Markus and Benjamin curriculum to the specific needs of cybersecurity advocates identified in my research.
<table>
<thead>
<tr>
<th>Concept</th>
<th>Topics</th>
</tr>
</thead>
</table>
| Cybersecurity advocacy          | • The role of a cybersecurity advocate – goals, characteristics, professional credibility, change agentry  
                                  | • Differences in advocacy based on audience type  
                                  | • Routine difficulties encountered in advocacy work  |
| Cybersecurity basics            | • Information assurance triad – confidentiality, integrity, availability  
                                  | • Overview of security technologies, mechanisms, and terms  
                                  | • Recent trends in threats, vulnerabilities, and mitigation strategies  
                                  | • Overview of security professional roles  
                                  | • Staying current – evaluating trustworthiness of security information, building professional networks, awareness of security resources and communities  |
| Non-technical skills            | • Interpersonal skills - establishing trust, building relationships, conflict management, group dynamics, active listening  
                                  | • Communication skills – risk communication, marketing basics, communicating value to different audiences (e.g., management, IT staff, end users)  
                                  | • Understanding context – awareness of audience environment, goals, and constraints  |
| Human-centered cybersecurity basics | • Human behavior basics – cognitive limitations, cognitive biases, decision-making, risk evaluation, behavior change  
                                  | • Usable security concepts – user-centered design, usability tenets, overview of usable security research  |
| Organizational context         | • Economics of cybersecurity – return on investment, cost of cyber intrusion, resource allocation  
                                  | • Cybersecurity governance – understanding cybersecurity policies and regulations that govern organizations  
                                  | • Coping with challenges – common organizational challenges and how to deal with them constructively (e.g., gaining leadership and workforce buy-in)  
                                  | • Prioritizing efforts – determining immediate and long-term security needs of the organization  |
| Advocacy techniques            | • Security advocacy tactics and how they can be used in different situations  
                                  | • Making effective use of different communication channels  |
10.1.3 Attracting a Cybersecurity Advocate Workforce

Establishing an education and career path is a first step in defining the cybersecurity advocate role. However, once the role is better defined, recruitment and retention strategies are needed to move qualified individuals into the role and keep them once they are there. My research findings related to motivations of advocates aid in an examination of how these strategies may align with those traditionally used for other security professional roles. There appears to be a need for a more nuanced approach to build the advocate workforce by advertising cybersecurity as a profession that has the potential to fuel these motivations via an advocacy role, encouraging discipline diversity within the field, and sustaining motivation for current advocates by documenting impact and providing energizing feedback.

10.1.3.1 Recruitment

Given that a cybersecurity career is often marketed through a purely technical lens, current recruitment efforts may inadvertently dissuade those who seek a career in which they can regularly engage with people, employ a variety of communication techniques, and make a positive, societal impact. Likewise, individuals in non-security fields may not understand how their skills might be valuable, especially in advocacy roles. While interpersonal and communication skills are generally noted as useful professional skills, my studies also identified service orientation as an attribute not typically emphasized in security professions, but essential for those performing advocacy roles. Therefore, to enhance the future cybersecurity advocacy workforce pipeline, there may be benefit in cybersecurity education and recruitment programs expanding the scope
of security professions by incorporating and advertising the non-technical skills and service orientation identified in our interviews as relevant attributes of security advocates.

When marketing cybersecurity positions with advocacy duties, in addition to touting the work as interesting and challenging, there should be emphasis on the important service to individuals and society. For example, when recruiting advocates for jobs in the public sector, salaries can seldom compete with those in private industry, so appealing to motivators like a sense of civic duty and national pride may be especially helpful in attracting qualified individuals (Dawson & Thomson, 2018). Service orientation of the work may also appeal to currently underrepresented populations in the cybersecurity workforce who may perceive cybersecurity as having limited social benefit (Shumba et al, 2013) or women who desire a career with a socially motivated purpose (Blum, 2001).

Individuals coming from other disciplines could also be encouraged to become security advocates. One of the most surprising observations of the interview study was the participant diversity with regard to discipline and training, especially since I did not purposefully sample along education or career dimensions. Discipline diversity was further exemplified in the case study, as two of the three security awareness team members came from non-technical backgrounds. Among the advocates in both studies, diversity appeared to be quite beneficial with advocacy teams.

Additionally, although security applies to all industries and sectors, contexts vary widely. Advocates working within a particular professional setting may have more intimate knowledge of that environment than an external advocate might. It is then logical to increase the reach and effectiveness of security advocacy by encouraging the
Development of cybersecurity advocates who are trusted insiders within diverse fields, for example, law, finance, education, and health.

Therefore, the opportunity to work collaboratively with talented, diverse people from multiple disciplines should be highlighted in recruitment efforts. This emphasis may counter a lack of awareness of the breadth of opportunities available in security careers (Gonzalez, 2015) and belief that only those with deep technical skills can be successful (D’Hondt, 2016; Gonzalez, 2015). The interdisciplinary framing might help attract individuals from other fields who possess important non-technical skills and unique perspectives and encourage a greater sense of self-efficacy. Additionally, an emphasis on the value of diversity may encourage participation of women and minorities who otherwise may be deterred by the stereotype of a white male, hacker-dominated workforce (Bagchi-Sen et al., 2010; D’Hondt, 2016).

10.1.3.2 Retention

Due to the dynamic nature of cybersecurity risks and technologies, organizational challenges, and human nature, my study results suggest that the work of advocates can sometimes be daunting and thankless, requiring perseverance and resilience. In addition, individuals qualified for cybersecurity advocate positions possess a valuable blend of skills, so may be in danger of being recruited away by others. Therefore, special emphasis should be placed on their retention. To aid in retention, foster motivation, and encourage progression of current professionals into advocate roles, the following recommendations for employers (based on study findings regarding motivations) are proposed.
Organizational leaders should recognize those who are doing advocacy work within the organization, even if in the background. They should offer sincere praise and feedback about advocate successes (even if minor), tout their mix of technical and non-technical skill, support innovative approaches, and provide opportunities for advocates to assume more responsibility for security promotion activities. Leaders should also clearly communicate to the workforce that advocates are supported by the organization as important contributors in protecting people, systems, and information. Outward displays of support lend authority and credibility to security advocates and is an assertion that advocates’ advice should be heeded. This may be especially important given that advocates often do not have enforcement power and may be viewed by others as just providing voluntary guidance.

Advocates should be provided ample opportunity to receive direct feedback from their audience about their efforts via mechanisms to measure effectiveness and value of advocacy approaches. They should be permitted professional development and continuous learning opportunities that can aid them in their jobs. This learning should address the interdisciplinary nature of cybersecurity and include organizational, social, and technical aspects of cybersecurity. To stay relevant and obtain ideas for their own advocacy efforts, advocates should also be encouraged to participate in collaborative and information sharing opportunities with others working in related areas. Establishing personal connections through these communities of practice (Lave & Wenger, 1991) may result in advocates continued learning as well as feeling better supported and equipped to do their jobs.
10.2 Communicating Cybersecurity Risk and Guidance

Cybersecurity advocates ultimately serve as security risk communicators and change agents for security adoption. My studies revealed a number of general and specific tactics advocates employ in their communication and promotion of security best practices and their efforts to influence their audience’s security behaviors. These tactics can serve as a valuable resource for others performing this role, whether it be through continuing educational programs as described in Chapter 10 or via outreach efforts to the security community.

Perhaps unconsciously, security advocates seemed to understand the importance of the human element in cybersecurity adoption. They regularly employed techniques to combat common behavioral heuristics and biases that could negatively affect security decisions, as suggested by Pfleeger and Caputo (2012). For example, they addressed cognitive load by breaking recommendations down into manageable, prioritized chunks. Storytelling, sharing personal experiences, and referencing recent events helped with availability, which is an evaluation of the likelihood of an event based on recall of similar events happening. Advocates also encouraged audience self-efficacy, which they often referred to as empowerment. Empowerment is supported not only by raising awareness of security issues, but also by providing tools and actionable guidance.

My research also explores the effectiveness of rhetorical devices like narratives, analogies, and metaphors, within security contexts. For example, even though only four interview participants explicitly said that they employ metaphors and analogies when communicating with their target audiences, we observed that many advocates, including the security awareness lead in the case study, naturally used a variety of these to describe security concepts to me during our interviews. This was the case even though I was
known to have security experience, suggesting that their use goes beyond being purely instructive.

There may also be value in applying security advocacy techniques to the design of security interfaces and training resources. To overcome negative perceptions of security, these resources should aim to empower users to take appropriate security actions and create a positive affect towards security. Security resources should create an appropriate level of concern without overwhelming or paralyzing by conveying severity and likelihood in clear, understandable terms. Resources must be usable, tailored to the audience, and encourage empowerment by providing concrete, achievable steps in simple language. Additional references to threat information that includes real stories of security incidents can lend greater credibility to risk claims. Training materials should consider the incorporation of storytelling and other creative rhetorical methods, for example, as demonstrated in story-based phishing training proposed by Lastdrager et al. (2017).

10.3 Advancing Security Awareness Programs

My research confirmed that security awareness, at least from the perception of advocates, is subject to a negative stereotype of being boring and driven by compliance rather than effectiveness. Furthermore, as found in prior industry reports (SANS, 2018; Woelk, 2015) and confirmed in the case study, security awareness professionals may be at a disadvantage because they often perform their security awareness duties on a part-time basis, have to work with limited resources, and may lack formal training or resources on how to develop successful security awareness programs.

The security awareness professionals I interviewed and observed were attempting to overcome the negative stereotype as well as the misguided compliance mentality held
by some organizations: “I see a lot of organizations are now trying to smash through that and take it to the next level” (P09). In order to “take it to the next level,” interview study participants discussed designing more engaging training that encourages intrinsic motivation to perform security best practices while finding meaningful measures of effectiveness beyond compliance numbers. Even those not directly engaged in security awareness efforts discussed their own tried-and-true techniques that could often be applied within the security awareness context. Study of the agency security awareness program revealed specific examples of how a security awareness program can evolve beyond the compliance-driven stereotype by translating the intent of the policy into organization-relevant approaches aimed at changing attitudes and behaviors of individuals. For example, the team has plans to customize annual security awareness training to address agency-specific issues and ensure the training is slightly different from year to year to prevent the material from becoming stale. To lessen the burden of security training given employees’ busy schedules, the team permits multiple paths towards completion of role-based training requirement, e.g., by attending internal security awareness events or external conferences in lieu of multi-day classroom training. The team also attempts to distribute security information using a variety of engaging formats to accommodate differences in employee preferences, such as informal drop-in events, more structured security days, and physical materials.

As discussed previously, cybersecurity advocates often rely on others in their professional communities to keep abreast of the latest trends and happenings. To that end, the lessons learned, security advocacy tactics, and measures of effectiveness identified in my research can serve as an initial resource to guide the work of security awareness
professionals and other security advocates conducting similar work. Even though the case study focused on a specific agency and the government sector, many of the case study findings mirrored those described in the more diverse interview study, so may be transferrable to a variety of contexts.
11 Contributions and Future Work

As promoters and educators of security best practices, cybersecurity advocates serve in a unique role in the ecology of security professionals. However, up to this point, little has been done to encourage development of additional advocate career pathways or attract individuals with the interests and skills to be effective in this role. To address this gap, I first conducted an interview study of security advocates from diverse backgrounds and sectors. This broader, exploratory study began to illuminate the skillsets and practices of those performing this role. A follow-up in-depth case study of a security advocacy team at a government agency confirmed and expanded the interview study findings in a real-world setting.

In this chapter, I summarize my contributions to both the research and practitioner communities. I also propose a plan for future research to address the limitations inherent in my studies and conclude with a summary of overall implications of my work.

11.1 Contributions to the Research Body of Knowledge

This section reintegrates my findings into the literature cited in Chapter 2 by describing how my work confirms, contradicts, extends, and advances previous research.

11.1.1 Security Professionals

My research extends previous research about those who work in the cybersecurity field by defining a new security professional work role. I found that cybersecurity advocates do indeed share some work practices, challenges, and characteristics of traditional security professionals identified in prior research projects (Botta et al., 2007; Haber & Kandogan, 2007; Paul, 2014; Goodall, Lutters, & Komlodi, 2009). For example,
they experience many of the same challenges encountered by those in other security roles, including staying up-to-date on the latest technologies and having to communicate with stakeholders having different security risk perceptions, knowledge, and security culture. While security professionals in general must have critical thinking and technical skills as identified in Botta et al. (2007), advocates more often work at social and organizational boundaries. They must be skilled in a variety of non-technical duties, including: raising awareness and empowering people to take action; facilitating adoption of security best practices and influencing behaviors; contextualizing security risk messages; incentivizing security best practice behaviors; and building relationships with their audience. These tasks require skills and competencies including, but beyond, mere technical acumen, such as interpersonal and communication skills and context awareness.

My findings also confirm many of the same motivations as IT and cybersecurity professionals identified in the prior literature (Lounsbury et al., 2007; Chai & Kim, 2012; Bashir et al., 2017; Dawson & Thomson, 2018), such as sense of duty/service, self-efficacy, working with others, and interest. I also found an emphasis on intrinsic motivations (e.g., personal interest and sense of duty) inherent in the work of cybersecurity advocacy and its immediate goal of enacting positive behavior change. However, even extrinsic motivators (e.g., praise and compensation) were contributors to intrinsic motivation. For example, most participant advocates were not ego-driven, so praise was viewed in the context of reinforcing self-efficacy and sense of duty. Despite these similarities, there were also subtle differences. For example, advocates appear to be more driven by a powerful service motivation, thrive on evidence of real impact, and often have larger spheres of influence.
11.1.2 Technology Adoption and Change Agentry

My research confirms many of the observations of technology adoption factors described in Diffusion of Innovation (DOI) theory (Rogers, 2003). My work applies DOI to cybersecurity context, which has been sparsely represented within DOI literature. Through the eyes of advocates, I identified many of the same technology adoption factors such as client (audience) motivation to change, complexity of the technology, and technology compatibility with organizational and social constructs. By identifying organizational challenges pertaining to a lack of buy-in and not seeing clear return on investment, I saw evidence of adoption challenges with preventive technologies (like cybersecurity tech) since it can be difficult for adopters to observe rewards and consequences.

Perhaps most significantly, my findings confirm that cybersecurity advocates are quite similar to the change agents prominently featured in DOI. To the best of my knowledge, this is the first research to document change agentry within the cybersecurity domain. Advocates play the same roles as change agents, for example, creating a need for and intent to change in their clients, establishing information exchange, and encouraging client independence (represented as empowerment in my studies). Advocates also have similar success factors as change agents, including their ability to build credibility and relationships and having strong communication skills. Recognizing this similarity, I used Markus and Benjamin’s (2007) proposed educational program for information systems change agents as a basis for tailoring a program for the cybersecurity advocate role.

Although quite similar, advocates in the cybersecurity field may have some nuanced differences to change agents described in other IT/IS literature. Prior literature
(Allen, 1995; Markus & Benjamin, 1996; Winston, 1999) focused on organizational change through political advocacy whereas security advocates appeared to be more focused on changing individual practice. This facilitation of behavioral changes at an individual level was seen as an incremental approach to changing organizational culture.

11.1.3 Advancing Risk Communication

My results confirm that cybersecurity advocates, as risk communicators, exercise many of the same risk communication and advocacy best practices observed in other fields such as health (Covello, 1997), environmental hazards (Sandman, 2013), and home security (Dolata et al, 2016). For example, they expressed common goals, such as building trust, creating awareness strategies, and motivating people to act. To build trust and credibility, they employed a variety of non-technical, “soft” skills. In communicating their message, security advocates similarly used engaging techniques, served as a bridge between security experts and nonexperts, encouraged audience empowerment, and tailored their message to the audience based on the context.

Similarities suggest there may be much to learn from risk communication in non-security fields, especially those with longer histories and hard-fought successes. In particular, there may be value in a more in-depth investigation into how lessons learned in public health advocacy might be applied to cybersecurity given that this connection was raised repeatedly in the interview study and used as a security awareness event theme in the case study.

Moving beyond these similarities, the findings suggest some unique properties of security risk which may advance the overall risk communication discipline as well as security-specific communications. Specifically, my research identified how advocacy in
the security domain may be more urgent and challenging than in other domains and may require additional tactics. This discovery confirms prior literature regarding people’s perceptions of security and security challenges commonly encountered by security professionals. It also is in-line with challenges to cybersecurity policy offered by de Bruijn and Janssen (2017), which included: the intangible nature of security; socio-technical complexity and dependence; ambiguous impact; and the contested nature of security defense, which includes disagreement on necessary security measures and unclear enemies.

Foremost, the security field is incredibly dynamic, having to adjust to constantly changing technologies and defend against determined adversaries who can exact significant damage with relatively little cost or sophistication. Security applies to everyone and every organization within an interconnected, technology-dependent society. However, as also noted in prior studies, most are not equipped to deal with security measures since security consists of abstract concepts not well understood by the typical person (Stanton et al., 2015; Wash, 2010). In addition, people are often dependent on security interfaces with poor usability (Garfinkel & Lipford, 2014) and are subject to mandated security processes that do not take under consideration human limitations or most people’s general lack of experience with the complexities of security.

Motivation to enact security measures may likewise be problematic because people suffer from security fatigue (Stanton et al., 2015; Furnell & Thomson, 2009), are distracted by other priorities (West et al., 2008), and the consequences of poor behavior are not always immediate or easily observed (Huang et al., 2007). In addition, perceived benefits of following security best practices may be less tangible at the individual level,
especially if someone has not been personally impacted negatively in the past. Whereas in related risk communication domains, like health, where benefits are usually more individualistic, cybersecurity may be considered a common good that “nobody owns but everybody is involved in and can be affected” (de Bruijn & Janssen 2017). As a public good, it can then be hard to assign responsibility for taking action. People also may not be cognizant of how their poor security practices may have potential impact on others. For example, if I practice poor security habits on my network, it may impact others if my network is exploited and becomes a jumping off point to get into other networks.

Interestingly, although the advocates in my studies often talked about collective consequences and responsibility in terms of the common good, their approaches often reflected attempts at individualizing security behaviors by emphasizing personal relevance and responsibility. Therefore, addressing possible differences in approaches to risk communication between individualistic domains (like health) and common good domains (like cybersecurity) through future research efforts may be warranted.

Finally, the economics of security are hard to measure as discussed by advocates in both of my studies as well as previous work (Moore & Anderson, 2011; Gordon et al., 2018; Moore, Dynes, & Change, 2015; Herley, 2009). This results in an unclear return on investment with people having a hard time conceptualizing what is worth their time and effort unless something actually goes wrong.

To better explore these similarities and differences, there is future research potential in performing in-depth comparisons of security advocacy practices to those in other relevant risk communication domains.
11.1.4 Persuasion Techniques

As discussed in Related Literature section 2.7, most prior research on persuasive methods in the security context has taken the perspective of the target end users and not those who do the influencing. My research addressed this gap while confirming, extending, and challenging previous findings related to persuasive techniques in cybersecurity.

The interview and case studies validated prior findings, for example: the value of small group interactions (Albrechtsen & Hovden, 2010); the necessity of framing security communications (Shropshire et al., 2010; Siponen, 2000); some principles of Protection Motivation Theory such as the importance of clearly communicating risk in order to give people a sense of severity, likelihood, and consequences (Maddux & Rogers, 1983); and the value of encouraging security self-efficacy and empowerment (Rhee et al., 2009).

Additionally, my research findings extend the literature by cataloging rhetorical devices not previously mentioned in persuasive security studies, including alliteration, allusion, humor, and slogans. It also provides evidence towards the successful use of previously identified rhetorical devices such as narratives/storytelling (Redmiles et al., 2016; Lastdrager et al., 2017) and metaphorical mental models like physical security and health (Camp, 2009; Zhang-Kennedy et al., 2014). However, in line with the mixed findings in past studies about the efficacy of metaphors (Brase et al., 2017), two of the interview participants cautioned against incorrect use of these for fear that they may oversimplify security concepts and create misunderstandings leading to risky behaviors. However, the case study security awareness team regularly made use of metaphors. Future work is needed to look more deeply into the use of metaphors and the level of
detail and relevancy they must provide in order to positively affect security learning and behavior.

My research revealed mixed opinions concerning the use and efficacy of positive versus negative incentives, including fear appeals (Johnson & Warkentin, 201), with the majority of advocates favoring positive feedback and rewards. Findings also demonstrated how advocates attempt to use both intrinsic and extrinsic motivators to influence security (Herath & Rao, 2009), such as appeals to personal protection, revealing consequences of poor security decisions, and mandatory training requirements. However, the effectiveness of those motivators could be not be confirmed because of the limited number of advocate clients I directly engaged with (nine employees at Agency A) and the lack of actual measurement of any quantifiable effect. Overall, my research suggests that the choice of incentives should likely be context-driven and tailored towards what will be compatible with the organizational culture and individual values. For example, negative penalties in Agency A may be viewed as more acceptable because of the sensitive nature of the work, the potential serious consequences of a security breach to the agency and critical infrastructure stakeholders, and the public servant culture. The use of fear appeals appears to be context-sensitive art as it should be tailored to the audience’s culture and tolerance level for that type of communication.

Finally, my findings partially demonstrated suggestions for addressing economic decisions for security advice as recommended in Herley (2009). Herley recommends prioritized advice, respecting users’ time and effort (part of empowerment), and ensuring advice is relevant to actual harms faced by users, which are similar to that which was identified in my research. In addition, several participants mentioned not propagating
older advice that may not be relevant to a particular situation or audience. However, my findings did not address the identification of victimization rates to guide the design of advice.

11.2 Contributions to Cybersecurity Practice

Beyond filling gaps and extending prior research, the investigation into the work practices of cybersecurity advocates has several contributions that can be applied directly to professional practice. My research informs efforts to build the cybersecurity advocate workforce and aid cybersecurity advocates in their jobs. Most notably, this is the first known attempt at examining the cybersecurity advocacy role and its evolving definitional boundaries through descriptive reporting of advocate skills, characteristics, work motivations, and real-world security advocacy techniques in a variety of contexts. The analysis suggests that there may be value in establishing cybersecurity advocacy as a new work role within the security field. Formalization of this work role could aid in the progression to advocate for both existing security professionals and those coming from other disciplines. To that end, my findings provide a foundation for the development of a security advocacy framework and educational program that includes the recommended attributes, skills, and practices of those who might be successful in the role.

Based on findings that cybersecurity advocates have diverse educational and career backgrounds, are oriented towards contributing to the common good, and must master non-technical skills (e.g., interpersonal, communication) to be successful, I also see an opportunity for my research to influence the marketing of cybersecurity advocacy as a people-oriented service profession that encourages multi-disciplinary perspectives. This new framing may aid in increasing the currently under-staffed security workforce by
encouraging discipline diversity and attracting to the advocacy role a new demographic of individuals who may not otherwise consider cybersecurity as a career choice.

The identified advocacy practices can also serve as a resource consisting of risk communication lessons learned and examples of successful approaches which can be used by others performing the advocate role. Finally, the findings can inform how successful advocacy techniques can be incorporated into tools and interfaces that promote beneficial security behavior. For example, metaphors or storytelling techniques successfully used by the participants might be incorporated into computer-based security awareness training.

11.3 Limitations

My research to date represents an initial investigation of the cybersecurity advocate role, with its key characteristics and professional development pathways, that can be confirmed and expanded in future work. Findings in both the interview and case studies may be transferable to other advocates in a variety of contexts. However, there are limitations in the design choices of the two studies that can be addressed by future efforts.

The interview study, although including a fairly diverse advocate population in terms of background and employment sector, reflected security advocacy only within the United States. Advocacy in other countries may look quite different based on cultural differences, such as Hofstede’s Dimensions of Culture (2011), which includes elements of collectivism/individualism and uncertainty avoidance. In addition, the broader, exploratory nature of the study did not allow for deeper investigation of emerging variables of interest identified in the studies. For example, advocates’ use and opinions of
metaphors and incentives were mixed, so it would be interesting to further explore in what contexts different variations of these might be most appropriate and effective.

The case study, although valuable for exploring advocacy in practice, was limited in scope as it focused on a small security awareness team working in the government sector. Therefore, I cannot generalize findings to other employment sectors and types of advocates. For example, there may be distinct differences in for-profit contexts or among advocates who primarily target software developers.

Originally, I had intended to obtain the audience perspective on the effectiveness of security advocacy efforts during the case study investigation. However, due to a mutual agency-researcher desire to maintain anonymity of employee interviewees and resource constraints that prevented the security awareness team from assisting with large-scale recruitment of participants, I was only able to talk with nine agency employees. About half of those worked in a cybersecurity role, most personally knew members of the security awareness team (and had been identified by the team), and all had attended security awareness events on a regular basis. Therefore, their responses were biased by their experience. Ultimately, although the employee interviews did provide interesting insights, this limited sample was not enough to make general inferences across the entire agency workforce. In addition, I gained little understanding of those who chose not to participate in security awareness events or those who attended but did not like the events beyond second-hand conjecture of interviewed agency staff.

On a related note, although study participants felt that cybersecurity advocacy was valuable, there is has been little work done to provide quantifiable proof of that value. Since my research is largely based on advocate perceptions, my results do not definitively
show that advocates’ efforts positively change people’s security behaviors, or, if they do, how effective different advocate techniques actually are.

11.4 Future Work

Additional research can help to overcome limitations in my research. Overall generalizability could be attempted by formalizing findings to a model to be validated with a broadly-distributed, quantitative survey of those in advocacy roles in other countries/cultures. The survey could contain questions based on the skillsets, motivations, techniques, communication channels, and challenges identified in the interview and case studies.

An option to further validate findings of advocacy in practice is the replication of the case study fieldwork in multiple organizations. Because case studies are labor intensive, this approach is unlikely to achieve a large enough sample to generalize; however, the fidelity of transferable findings could be increased. There are several possible design choices for these multi-case studies, each with a slightly different goal. Organizations might be sampled in multiple sectors to obtain a broader view or within the same sector identify advocacy practices that might be effective in a particular context. Another potential is sampling multiple advocate teams performing the same type of advocacy (e.g., security awareness) to begin to uncover and understand possible specialties within the overall advocacy umbrella. All of these approaches could contribute to building educational and practical resources that would be valuable to advocates, whether it be advocates in general, those targeting a specific sector, or a particular type of advocate. Resources could compile advocates’ lessons learned, commonly used measures of effectiveness, and a context-informed catalog of successful advocacy tactics.
Greater insight into audience perspectives of advocates and their work could be gained via the afore-mentioned case studies. Because they are bounded, case studies would allow a known audience to be surveyed and permit audience reactions to be matched to specific techniques employed by an advocacy team. Audience members could be surveyed more broadly with a largely quantitative instrument; however, in-depth interviews with a smaller subset could be first conducted to inform tailoring of the survey.

Although not the focus of my research, future work can also be done to begin to address the uncertainty about the effectiveness of various advocacy techniques as compared to others since the study participants did not operationalize and quantify the impact of their work. Self-report surveys of target audiences within a bounded context (as described above) may shed some light on technique effectiveness as demonstrated by Kruger and Kearney (2006) who developed a questionnaire to test the knowledge, attitude and behavior of respondents with respect to security awareness. However, as discussed in Wolf, Haworth, and Pietron, these kinds of self-report attempts incorrectly “assume that knowledge of security awareness equates to the correct behavior by the end-user” (2011). These researchers suggested measuring actual user behaviors before and after an intervention. In their study, they deployed four different interventions related to password security and measured effectiveness by evaluating password strength. Therefore, to gain more clarity on technique effectiveness, various quantifiable user incidents and behaviors (e.g., phishing click rates, user-reported incidents, other security incidents) could be measured prior to and after different advocacy techniques are employed to look for changes in the positive direction. To minimize confounding
variables, these experiments could be done within a bounded setting using a between
groups design, with each group receiving a different intervention. Results from the
interview and case studies could be used to guide the types of techniques evaluated (those
indicated as effective by the study participants) in an effort to validate participants’
perceptions.

11.5 Researcher Positionality

In section 3.4, I described my own past professional experience performing
cybersecurity advocacy work, how that impacted my approach, and biases I had to guard
against. I now revisit my positionality to reflect upon how my research findings might
have challenged or confirmed my initial assumptions and how being a security
professional could have impacted data collection and analysis.

Before beginning the research, I assumed that advocates would require non-
technical competencies to navigate social and organizational issues, which was
confirmed in the studies. Having worked in organizations that deeply valued technical
expertise and hired security professionals based not just on their experience but also their
technical degrees, I also thought that having technical knowledge would be viewed as
more important, although not exclusive to, non-technical competencies. However, I was
surprised by the diversity of educational and career backgrounds represented by study
participants, especially among those who had no security experience prior to being hired
for a security advocacy position. I also expected to find typical motivations for the work
(e.g., personal interest and aptitude, evidence of impact). However, although I myself
possess a service orientation to the job, because cybersecurity jobs are routinely touted as
high-paying, in-demand, and stable, I did not expect that the vast majority of advocates I
would encounter also had a strong service motivation. Finally, having had personal experience with mostly computer-based security awareness training, I originally did not anticipate the diversity of security awareness approaches found in my studies.

Although my past experience in the security field aided me in gaining credibility and building rapport with participants, it also posed a challenge at times in collecting and analyzing data. For example, during interviews, there were a few instances in which I should have probed further, but did not, because my personal interpretations seemed to fill in the blanks regardless of whether the participant might have had the same interpretations. Therefore, I missed the opportunity to tease apart certain participant statements in more detail. I had to guard against these same leaps during analysis, being careful not to purposefully select data to support my pre-conceptions, but rather to allow the data to speak for itself. However, reviewing data and interpretations with a second researcher who was not as versed in the cybersecurity field helped to balance out these potential pitfalls.

I was also tempted to evaluate the effectiveness and novelty of advocacy techniques. However, I realized that it was not my goal as a qualitative researcher in these particular studies to evaluate (and I was likely not qualified or equipped to do so); rather I wanted to capture the essence of the security advocate role and the everyday routine of these professionals through the eyes of advocates themselves and those immediately exposed to their work.

Overall, my past professional experience aided my identification of a research problem and questions and helped with understanding the terminology, context, and
culture of these security advocate participants. However, I had to guard against my own personal biases when collecting and interpreting data.

11.6 Conclusion

As the first purposeful effort to learn about cybersecurity advocate work practices, my research begins to uncover the definitional boundaries of these professionals, including their skills, characteristics, motivations, challenges, and tactics. I found that advocates employ technical and non-technical skills and a variety of techniques to overcome negative perceptions of security and other security adoption barriers both at the organizational and individual levels.

To support advocates in their work, my research suggests the need for an expansion of current, predominantly technocentric cybersecurity career tracks. This expansion necessitates the consideration of nontechnical competencies and discipline diversity in professional development, recruitment, and retention efforts for cybersecurity advocates. My work also offers an opportunity for a repositioning of cybersecurity work (in particular, advocacy) as not solely the primarily technical endeavor of its cryptographic roots, but as a people-oriented, service profession. This recharacterization brings with it workforce development implications that could possibly have a transformative impact on the discipline. Given the growing dire conditions due to a workforce shortage and increasingly common and severe attacks, it may be time for a radical rethink about what cybersecurity means and how advocacy roles may contribute in the coming decade.
Appendix A: Interview Study Protocol

1. Can you tell me about what you do in your job? (RQ1, RQ2)

2. How did you come to do this type of work? (RQ1)

3. What motivates you to do this work? (RQ1)

4. Do you think your role as a security advocate is important? Why or why not? (RQ1)

5. Do you think your role is valued by others? Why or why not? (RQ3)

6. What do you think are qualities of a successful security advocate? (RQ1)

7. Have you had experiences with or know of security advocates who you don’t think were particularly effective? What was it about them or what did they do or did not do that contributed to their ineffectiveness? (RQ1)

8. Through what means do you advocate for security, e.g., conferences, invited talks, blogs, social media, articles, client visits, face-to-face meetings, phone, email? (RQ2)

9. Which of those means do you think are the most effective? Why? (RQ2)

10. Do you feel that you’re reaching the right population of people and organizations? (RQ2, RQ3) [Follow up questions if the answer is no:]
    a. What is preventing you from reaching the right people?
    b. What do you wish you could do to reach the right population?

11. How do you keep up with the latest in security? (RQ4)

12. What do you find most rewarding, if anything, about your role as a security advocate? (RQ3)

13. What do you find most challenging or frustrating, if anything, about your role as a security advocate? (RQ3)

14. What do you think are the biggest obstacles organizations face with respect to implementing security measures and technologies? (RQ3)

15. What is your role in helping organizations overcome these obstacles? (RQ2, RQ3)

16. What are other ways these obstacles might be overcome? (RQ2, RQ3)

17. Is there anything else you’d like to add with respect to security advocacy?
Appendix B: Interview Study Demographic Survey

1. Please enter the participant code given to you in an email from the research team: 
   __________

2. What is your job title or position?

3. How many years of experience do you have in the cyber security field?
   ○ Less than 5 years
   ○ 5-10 years
   ○ More than 10 years
   ○ Prefer not to answer

4. Which category best describes your current organization?
   ○ Consumer services
   ○ Education
   ○ Energy
   ○ Financial
   ○ Government – Defense
   ○ Government - Other
   ○ Healthcare
   ○ Retail
   ○ Technology (non-telecommunications)
   ○ Telecommunications
   ○ Other. Please describe:
   ○ Prefer not to answer

5. Which category or categories best describe the organizations you have worked for in the past? Check all that apply.
   □ Consumer services
   □ Education
   □ Energy
   □ Financial
   □ Government – Defense
   □ Government - Other
   □ Healthcare
   □ Retail
   □ Technology (non-telecommunications)
6. Do you represent or work closely with a specific security vendor?
   - No
   - Yes, I represent a security vendor
   - Yes, I work closely with a security vendor
   - Prefer not to answer

7. Who is your target audience with respect to advocating for security practices or technologies? Please do not use specific names of organizations, but do include audience groups/types (for example, technical personnel, management) and sectors or types of organizations (for example, health industry, government).

8. Select the option that best describes your audience.
   - My audience is mainly within my own organization.
   - My audience is mainly external to my organization.
   - My audience is both with and external to my organization.
   - Prefer not to answer
   - Other:

9. How would you describe your preferred approach to security advocacy?
   - I create security technologies or methodologies or coordinate the implementation of these.
   - I facilitate change by increasing people’s/organization’s capacity to create the conditions of informed choice, valid information, and personal responsibility
   - I advocate for the direction of change, try to persuade people about the need for change, and model how to make those changes.
   - Prefer not to answer

10. What is your gender?
    - Female
    - Male
    - Other
    - Prefer not to answer

11. What is your age range?
    - Under 25
    - 25-34
12. What is your highest level of education?
   - High school
   - Associate’s degree
   - Bachelor’s degree
   - Master’s degree
   - PhD
   - J.D.
   - Other - Please describe:
   - Prefer not to answer

13. In what area(s) is your formal education (for example computer science, business, mathematics)?
### Appendix C: Interview Study Codebook

High-level code categories are in **bold**. Sub-codes are bulleted. Descriptions are for high-level codes only. Some sub-codes were further broken into more sub-codes but are not included here.

<table>
<thead>
<tr>
<th>CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audience Type</strong></td>
<td>Advocate’s target populations</td>
</tr>
<tr>
<td><strong>Barriers/Challenges</strong></td>
<td>Challenges to successful security adoption and advocacy; includes people’s negative perceptions of security</td>
</tr>
<tr>
<td>• Bad information</td>
<td></td>
</tr>
<tr>
<td>• Economics</td>
<td></td>
</tr>
<tr>
<td>• Gatekeepers</td>
<td></td>
</tr>
<tr>
<td>• Ineffective security awareness training</td>
<td></td>
</tr>
<tr>
<td>• Lack of accountability</td>
<td></td>
</tr>
<tr>
<td>• Lack of management buy-in</td>
<td></td>
</tr>
<tr>
<td>• Organization culture</td>
<td></td>
</tr>
<tr>
<td>• Organization structure</td>
<td></td>
</tr>
<tr>
<td>• Perceptions of security (audience)</td>
<td></td>
</tr>
<tr>
<td>• Policy, regulations, compliance</td>
<td></td>
</tr>
<tr>
<td>• Poor usability</td>
<td></td>
</tr>
<tr>
<td>• Security field issues</td>
<td></td>
</tr>
<tr>
<td>• Technology</td>
<td></td>
</tr>
<tr>
<td><strong>Career Information</strong></td>
<td>Participants’ educational backgrounds, career progressions, and roles/identities</td>
</tr>
<tr>
<td>• Career history</td>
<td></td>
</tr>
<tr>
<td>• Formal education</td>
<td></td>
</tr>
<tr>
<td>• Roles and identity</td>
<td></td>
</tr>
<tr>
<td><strong>Communication/Translation Skills</strong></td>
<td>Ability to communicate and translate security topics to language that is meaningful for the recipient</td>
</tr>
<tr>
<td><strong>Context Awareness</strong></td>
<td>Being cognizant of the social, organizational, environmental context in which security is situated</td>
</tr>
<tr>
<td><strong>Credibility/Reputation</strong></td>
<td>How advocates establish credibility with their audience</td>
</tr>
<tr>
<td>• Individual</td>
<td></td>
</tr>
<tr>
<td>• Organization</td>
<td></td>
</tr>
<tr>
<td><strong>Education &amp; Awareness</strong></td>
<td>Examples of advocates serving as security educators</td>
</tr>
<tr>
<td>CODE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interpersonal Skills</td>
<td>Soft skills (other than communication skills) of advocates</td>
</tr>
<tr>
<td>• Empathy</td>
<td></td>
</tr>
<tr>
<td>• Flexibility/innovation</td>
<td></td>
</tr>
<tr>
<td>• Honesty</td>
<td></td>
</tr>
<tr>
<td>• Hope/optimism</td>
<td></td>
</tr>
<tr>
<td>• Humility</td>
<td></td>
</tr>
<tr>
<td>• Leadership</td>
<td></td>
</tr>
<tr>
<td>• Listening skills</td>
<td></td>
</tr>
<tr>
<td>• Putting self out there</td>
<td></td>
</tr>
<tr>
<td>• Teaming/collaboration</td>
<td></td>
</tr>
<tr>
<td>• Understanding people</td>
<td></td>
</tr>
<tr>
<td>Motivators</td>
<td>Advocates’ work motivations</td>
</tr>
<tr>
<td>• Awards/monetary recognition</td>
<td></td>
</tr>
<tr>
<td>• Comradery</td>
<td></td>
</tr>
<tr>
<td>• Evidence of impact</td>
<td></td>
</tr>
<tr>
<td>• Passion/enthusiasm</td>
<td></td>
</tr>
<tr>
<td>• Personal interest</td>
<td></td>
</tr>
<tr>
<td>• Self-efficacy</td>
<td></td>
</tr>
<tr>
<td>• Service/importance of the work</td>
<td></td>
</tr>
<tr>
<td>Research-Practitioner Gap</td>
<td>Mentions of lack of communication between the research and practitioner communities and lack of application of research results in practice</td>
</tr>
<tr>
<td>Risk/Threat</td>
<td>Security risks and threats</td>
</tr>
<tr>
<td>• Actual risk/threat</td>
<td></td>
</tr>
<tr>
<td>• Discernment</td>
<td></td>
</tr>
<tr>
<td>Staying Relevant</td>
<td>How advocates stay up-to-date on the latest security happenings</td>
</tr>
<tr>
<td>Tech not everything</td>
<td>How technical knowledge and technology are only one piece of security solutions and advocacy success</td>
</tr>
<tr>
<td>Technical Skills</td>
<td>Technical knowledge of advocates</td>
</tr>
<tr>
<td>CODE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Techniques/Solutions</td>
<td>Advocacy techniques and ways in which advocates accomplish their work</td>
</tr>
<tr>
<td>• Communication Channels</td>
<td></td>
</tr>
<tr>
<td>• Consensus-building/partnerships</td>
<td></td>
</tr>
<tr>
<td>• Data</td>
<td></td>
</tr>
<tr>
<td>• Empowerment</td>
<td></td>
</tr>
<tr>
<td>• Home-work connection</td>
<td></td>
</tr>
<tr>
<td>• Incentives and punishments</td>
<td></td>
</tr>
<tr>
<td>• Management buy-in</td>
<td></td>
</tr>
<tr>
<td>• Multi-disciplinary, holistic approach</td>
<td></td>
</tr>
<tr>
<td>• Policy</td>
<td></td>
</tr>
<tr>
<td>• Practical recommendations/frameworks</td>
<td></td>
</tr>
<tr>
<td>• Promoting usability</td>
<td></td>
</tr>
<tr>
<td>• Rhetorical devices</td>
<td></td>
</tr>
<tr>
<td>• Selling/marketing security</td>
<td></td>
</tr>
<tr>
<td>• Technology and automation</td>
<td></td>
</tr>
<tr>
<td>• Testing</td>
<td></td>
</tr>
<tr>
<td>• Topicality</td>
<td></td>
</tr>
<tr>
<td>• Use of opinion leaders, champions</td>
<td></td>
</tr>
<tr>
<td>• Vendor influence</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D: Case Study Security Awareness Team Demographic Survey

1. How many years have you worked at your current agency?
   - □ Less than 5 years
   - □ 5-10 years
   - □ More than 10 years

2. Which category or categories best describe organizations you have worked for in the past? Check all that apply.
   - □ Consumer services
   - □ Education
   - □ Energy
   - □ Financial
   - □ Government – Defense
   - □ Government – Non-defense
   - □ Healthcare
   - □ Non-profit
   - □ Retail
   - □ Technology (non-telecommunications)
   - □ Telecommunications
   - □ Other – Please describe: ___________________________
   - □ Does not apply – I have always worked in my current organization

3. How many years of experience do you have in the cybersecurity field?
   - □ Less than 5 years
   - □ 5-10 years
   - □ More than 10 years

4. How many years of experience do you have working in security awareness?
   - □ Less than 5 years
   - □ 5-10 years
   - □ More than 10 years

5. What is your highest level of education?
   - □ High school
   - □ Associate’s degree
☐ Bachelor’s degree
☐ Master’s degree
☐ Doctoral degree
☐ Other - Please describe: __________________

6. If you have a degree beyond high school, in what area(s) was your formal education?

7. What is your gender?
   ☐ Male
   ☐ Female
   ☐ Other
   ☐ Prefer not to answer

8. What is your age range?
   ☐ Under 25
   ☐ 25-34
   ☐ 35-44
   ☐ 45-54
   ☐ 55 and over
Appendix E: Case Study Security Awareness Team Interview Protocol

1. Can you tell me about what you do in your job? (RQ1, RQ2)
   • What is your job title or position?

2. How did you come to do this type of work? What has been your career progression? (RQ1)

3. What kind of training, if any, has helped you do your job? (RQ4)

4. What motivates you to do this work? (RQ1)

5. How do you think your team and what you all do are viewed or supported by management/leaders within your organization? (RQ3)
   • What are your thoughts about the amount of resources your team is provided?

6. How do you think your team and what you all do are viewed by other groups of employees in your organization? (RQ3)

7. What do you think are qualities of a successful security awareness professional? (RQ1)

8. Have you had experiences with or know of security awareness professionals who you don’t think were particularly effective? What was it about them or what did they did/did not do that contributed to their ineffectiveness? (RQ1)

9. How do you keep up with the latest in security? (RQ4)

10. What do you find most rewarding, if anything, about your role as a security awareness professional? (RQ3)

11. What do you find most challenging or frustrating, if anything, about your role as a security awareness professional? (RQ3)

12. What do you think are the biggest obstacles the people within your organization face when it comes to security? (RQ3)

13. What do you think are the biggest security-related obstacles from an organizational perspective? (RQ3)

[Key individual interview – skip next two questions and proceed to Key Individual Interview Questions]
Your team leader has provided me with a list of the type of things your team does to provide security awareness and education, for example *<insert based on prior key individual response>*.

14. With which of these efforts are you or have you been personally involved? (RQ2)
   - Which do you think are the most effective? Why? (RQ5)
   - What approaches have you observed that are less effective? (RQ5)

15. Is there anything else you’d like to add related to anything we’ve talked about?

*End of interview for those who are not key individuals.>*

**Key Individual Interview Questions**

Now, I’m going to transition to the second part of our interview and ask you some questions about your team and what you all do.

16. Can you tell me about your team?
   - How many people?
   - Are the team members full time in their security awareness role or part-time?
     - *if some are part-time:* What other jobs do these part-time members have within the organization?
   - Where in the organizational structure is the team located? Distributed or centralized?
   - Who is your audience? For what kinds of people within your organization do you provide security education and awareness?
   - About how long has your organization had a security awareness team? How has it evolved over time, if at all?

17. What other people in the organization outside of your team perform security awareness and training functions, if any?

18. What kinds of security and privacy topics does your team address? (RQ2)

19. Can you describe some of your team’s security awareness efforts? (RQ2)
   - Through what means do you conduct these efforts? *if not sure how to answer: for example, via in-person training, online blogs, email*

20. With which of these efforts are you or have you been personally involved? (RQ2)
   - Which do you think are the most effective? Why? (RQ5)
   - What approaches have you observed that are less effective? (RQ5)

21. How does your team decide what type of information to disseminate? (RQ2)

22. From what information sources do you draw when developing your security awareness program? (RQ4)
• Which material is produced by or based on materials from a third-party?
• Which is developed in-house?

23. How does your team incentivize people within your organization to practice good security behaviors? (RQ5)

24. What does success look like for your team? (RQ5)

25. How does your team measure success either formally or informally, if at all? (RQ5)

26. How do you communicate your team’s impact to managers and decision-makers within your organization? (RQ5)

27. Is there anything else you’d like to add related to anything we’ve talked about?
Appendix F: Case Study Manager Interview Protocol

1. What is your role at work?

2. How long have you been working in this organization?
   • How long have you been in your current role?

3. What do you think is your organization’s view of security and privacy?
   • How is that view communicated to the organization, if at all?

4. What is expected of you as a manager with respect to security and privacy?

5. What are your responsibilities with respect the security awareness program within your organization?

6. What are your overall thoughts about the security awareness team and what they do?

7. How has the security information provided by the team impacted your own security behaviors or knowledge, if at all?

8. What do you think success looks like for the security awareness team?

9. What indicators or metrics do you consider when determining if the team is being successful?

10. How do you make decisions about the team’s priorities?
    • How do you make decisions about what and how many resources to allocate to the program?

11. What kinds of things would you like the team to do that they are currently not doing now?
    • What, if anything, is holding them back from doing these things?

12. What do you think are the biggest obstacles within your organization when it comes to security?

13. Is there anything else you’d like to add about anything we’ve discussed?
Appendix G: Case Study Employee Interview Protocol

**Work Role**
1. What is your role at work?

2. How long have you been working in this organization?
   - How long have you been in your current role?

**Security Behaviors**
3. What do you think is your organization’s view of security?
   - How is that view communicated, if at all?

4. What is expected of you as an employee with respect to security and privacy behaviors?

5. What are the biggest obstacles, if any, when it comes to your own security behaviors?

**Security Information Received at Work**
For the next few questions, I’m going to ask you about your thoughts about the security information you receive at work.

6. What kind of tips, education, or information about security and privacy do you receive while at work?
   - Through what means do you receive this information? [if unsure how to answer: for example, emails, online or in-person training, newsletters, websites]
   - Which information do you voluntarily seek out and which is “pushed” to you?

7. What are your thoughts about the content of the security information you receive at work?
   - In what ways is it valuable, if at all?
   - How much do you trust the information?

8. What are your thoughts about the ways in which the information is disseminated or communicated?
   - In what way do you most prefer to receive this information and why?
   - In what way do you least prefer to receive this information and why?

9. Can you describe any experiences you might have had in which information you received here at work helped you make a security or privacy-related decision while at work?
10. Can you describe any experiences you might have had in which information you received here at work helped you make a security or privacy-related decision while outside of work?

11. What kinds of security-related information would you like to get at work but you currently don’t receive at work?

12. Has any of the security information you’ve received outside of work conflicted with information you received at work?
   - How do you decide which source to trust?

**Perceptions of Security Awareness Team**

I’m now going to be shifting to a few questions about your thoughts on your organization’s security awareness team.

13. What do you know about the security awareness team in your organization?
   - What is their function?

14. Can you talk about any in-person, work-related experiences you have had with any members of the team related to security, for example one-on-one conversations about security or in-person training sessions where a member of the team was presenting information about security?
   - How did those go?
   - What were your impressions of the security awareness team member(s) you interacted with?

15. What are your overall thoughts and opinions about the security awareness team?
   - What is it about the team that influences how much you trust them?

16. What suggestions, if any, do you have for the security awareness team and how they should communicate security information?

**Technology Familiarity**

Finally, I’m going to wrap up with a few questions about your familiarity with technology and security. This information helps us as we analyze the interview data.

17. [if person is currently in a non-technical job:] Have you ever had a job related to technology or cybersecurity?

18. How would you describe your level of familiarity with technology?

19. How would you describe your level of familiarity with cybersecurity?

20. Is there anything else you’d like to add about anything we’ve discussed?
Appendix H: Case Study Codebook

High-level code categories are in **bold**. Sub-codes are bulleted. Descriptions are for high-level codes only. Some sub-codes were further broken into more sub-codes but are not included here.

security awareness = security awareness

<table>
<thead>
<tr>
<th>CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alignment</strong></td>
<td>Alignment with what other organizations are doing</td>
</tr>
<tr>
<td><strong>Barriers/Challenges</strong></td>
<td>Challenges to successful security awareness and adoption</td>
</tr>
<tr>
<td>• Compliance mentality</td>
<td></td>
</tr>
<tr>
<td>• Human error</td>
<td></td>
</tr>
<tr>
<td>• Lack of alignment with other internal organizations</td>
<td></td>
</tr>
<tr>
<td>• Lack of buy-in/awareness</td>
<td></td>
</tr>
<tr>
<td>• Lack of resources</td>
<td></td>
</tr>
<tr>
<td>• Logistics</td>
<td></td>
</tr>
<tr>
<td>• Technology</td>
<td></td>
</tr>
<tr>
<td>• Time</td>
<td></td>
</tr>
<tr>
<td><strong>Career Information</strong></td>
<td>Participant educational background, career progression, and roles/identity</td>
</tr>
<tr>
<td><strong>Communication/Translation Skills</strong></td>
<td>Ability to communicate and translate security topics to language that is meaningful for the recipient</td>
</tr>
<tr>
<td><strong>Context Awareness</strong></td>
<td>Being cognizant of the social, organizational, environmental context in which security is situated; includes how workforce feedback is incorporated into the security awareness program</td>
</tr>
<tr>
<td>• Incorporation of feedback</td>
<td></td>
</tr>
<tr>
<td>• Suggestions for improvement</td>
<td></td>
</tr>
<tr>
<td><strong>Credibility/Reputation</strong></td>
<td>How security awareness team establishes credibility with their audience</td>
</tr>
<tr>
<td><strong>Empowerment &amp; personal impact</strong></td>
<td>Mentions of providing people with the knowledge, resources, or awareness they need to be able to take security actions on their own or change their beliefs/self-efficacy</td>
</tr>
<tr>
<td><strong>External Influence</strong></td>
<td>Involvement with and bringing in perspectives from external organizations</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>Objectives of the security awareness team, including continuous improvement</td>
</tr>
<tr>
<td><strong>Measures of Effectiveness</strong></td>
<td>Indications that the security awareness program is making a difference in influencing security behaviors and attitudes</td>
</tr>
<tr>
<td><strong>Motivators</strong></td>
<td>security awareness team members’ work motivations; includes interest, self-efficacy, service/importance of the work, passion for the work</td>
</tr>
<tr>
<td>CODE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Organizational Characteristics</strong></td>
<td>Information about the organization, its structure and culture, where the team sits in the organization</td>
</tr>
<tr>
<td>• Expectations for security (employee)</td>
<td></td>
</tr>
<tr>
<td>• Security culture</td>
<td></td>
</tr>
<tr>
<td>• Structure</td>
<td></td>
</tr>
<tr>
<td><strong>Perceptions (external to the team)</strong></td>
<td>Employee and manager views of the security awareness team and program</td>
</tr>
<tr>
<td><strong>Relationships-Identity</strong></td>
<td>Employee relationship to security awareness team; how they view their identity with respect to team</td>
</tr>
<tr>
<td><strong>Risk/Threat</strong></td>
<td>Security risks and threats covered in the security awareness program</td>
</tr>
<tr>
<td><strong>Soft Skills</strong></td>
<td>Soft skills (other than communication skills) of the security awareness team; includes relationship building, empathy, listening, teaming, understanding people, creativity, etc.</td>
</tr>
<tr>
<td><strong>Staying Relevant</strong></td>
<td>How the security awareness team stays up-to-date on the latest security happenings and security awareness approaches</td>
</tr>
<tr>
<td><strong>Team Characteristics</strong></td>
<td>Information about the security awareness team, e.g., allotted resources, team dynamic, history</td>
</tr>
<tr>
<td><strong>Technical Skills</strong></td>
<td>Technical knowledge of the security awareness team</td>
</tr>
<tr>
<td><strong>Techniques/Solutions</strong></td>
<td>Security awareness techniques and ways in which the security awareness team accomplishes their work; includes communication channels, marketing, techniques</td>
</tr>
<tr>
<td>• Annual training</td>
<td></td>
</tr>
<tr>
<td>• Campaigns</td>
<td></td>
</tr>
<tr>
<td>• Employee preferences</td>
<td></td>
</tr>
<tr>
<td>• Engaging communication/speakers</td>
<td></td>
</tr>
<tr>
<td>• Events</td>
<td></td>
</tr>
<tr>
<td>• Gamification</td>
<td></td>
</tr>
<tr>
<td>• Handouts</td>
<td></td>
</tr>
<tr>
<td>• Incentives</td>
<td></td>
</tr>
<tr>
<td>• Less successful approaches</td>
<td></td>
</tr>
<tr>
<td>• Marketing</td>
<td></td>
</tr>
<tr>
<td>• Miscellaneous</td>
<td></td>
</tr>
<tr>
<td>• Phishing exercises</td>
<td></td>
</tr>
<tr>
<td>• Remote communications, recordings</td>
<td></td>
</tr>
<tr>
<td>• Role-based training</td>
<td></td>
</tr>
<tr>
<td>• Topicality</td>
<td></td>
</tr>
<tr>
<td>• Work-home connection</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong></td>
<td>Topics addressed by the security awareness program</td>
</tr>
<tr>
<td>CODE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wishlist</td>
<td>security awareness team needs/wants for the future; things they would like to be able to do but haven’t yet</td>
</tr>
</tbody>
</table>
Bibliography


295


