

REASONS FOR NON-COMPLIANCE WITH MANDATORY
INFORMATION ASSURANCE POLICIES
BY A TRAINED POPULATION

by

D. Cragin Shelton

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Science in Cyber Security

CAPITOL TECHNOLOGY UNIVERSITY

December 2014

UMI Number: 3692148

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 3692148

Published by ProQuest LLC (2015). Copyright in the Dissertation held by the Au

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code



ProQuest LLC.
789 East Eisenhower
Parkway
P.O. Box 1346

© 2014 by D. Cragin Shelton

ALL RIGHTS RESERVED

Approved for Public Release; Distribution Unlimited. Case Number 14-4186.

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

REASONS FOR NON-COMPLIANCE WITH MANDATORY
INFORMATION ASSURANCE POLICIES
BY A TRAINED POPULATION

by

D. Cragin Shelton

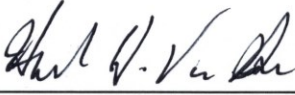
December 2014


Approved:


Howard H. Van Horn, PhD, Chair/Mentor


Salim U. Zafar, DSc, Committee

John W. Bornmann, PhD, Committee

Accepted and Signed:  12-05-2014
Howard H. Van Horn, PhD Date

Accepted and Signed:  12-07-2014
Salim U. Zafar, DSc Date

Accepted and Signed:  12-11-2014
John W. Bornmann, PhD Date

 12/05/2014
Date
Helen G. Barker, DM
Dean, School of Business and Information Sciences
Capitol Technology University

ABSTRACT

Information assurance (IA) is about protecting key attributes of information and the data systems. Treating IA as a system, it is appropriate to consider the three major elements of any system: *people*, *processes*, and *tools*. While IA tools exist in the form of hardware and software, tools alone cannot assure key information attributes. IA procedures and the people that must follow those procedures are also part of the system. There is no argument that people do not follow IA procedures. A review of the literature showed that not only is there no general consensus on why people do not follow IA procedures, no discovered studies simply asked people their reasons. Published studies addressed reasons for non-compliance, but always within a framework of any one of several assumed theories of human performance. The study described here took a first small step by asking a sample from an under-studied population, users of U.S. federal government information systems, why they have failed to comply with two IA procedures related to password management, and how often. The results may lay the groundwork for extending the same methodology across a range of IA procedures, eventually suggesting new approaches to motivating people, modifying procedures, or developing tools to better meet IA goals. In the course of the described study, an unexpected result occurred. The study plan had included comparing the data for workers with and without IA duties. However, almost all of the respondents in the survey declared having IA duties. Consideration of a comment by a pilot study participant brought the realization that IA awareness programs emphasizing universal responsibility for information security may have caused the unexpected responses. The study conclusions address suggestions for refining the question in future studies.

Keywords: information assurance, cyber security, compliance, systems engineering, self-efficacy, password

DEDICATION

I dedicate this work to family members who contributed variously in the form of support, guidance, advice, motivation, time, and patience over many decades of my pursuit of higher education. My father, Colonel Douglas C. Shelton, USAF Retired (deceased), rose to positions of high leadership and great accomplishment in spite of never having earned a single diploma or degree. He instilled in me the value of true educational accomplishment, having learned the hard way the difficulties in overcoming the limitations imposed by not having those documents in hand. My mother, Margaret R. Shelton, stood with Dad in making sure I completed my undergraduate efforts without a youthfully ill-thought-out 'break in service' which would have derailed my academic progress. Today she continues to express pride and support as I report on the work reflected here.

During my last graduate school effort almost thirty years ago my daughters Kathryn and Sam put up with a dad who seemed too busy, too often, for little girls to understand, but without complaint. As adults those same girls inspire me to complete this degree. Kathryn began her own quest for a doctorate in 2005, sadly cut short by her untimely passing. Sam earned her terminal degree in her field of scenic art, an MFA, several years ago, in spite of thinking herself a non-academic type.

Most importantly, I dedicate this work to my wife, Kay, who has stood by me with support, encouragement, and advice through four different graduate schools spread across forty years of marriage. For the past few years she has suffered an "absentee husband" hiding in the study nights and weekends, has advised me on writing quality (her academic forte), taken on extra work in the house, and kept me focused on what is important in life.

ACKNOWLEDGEMENTS

I have so many people to thank for the support, advice, guidance, and encouragement leading to completion of this dissertation. My employer, the MITRE Corporation, has not only supported the financial aspects of my studies, but has given me an intellectually rich and stimulating work environment in which to thrive. Corporate officers, managers, colleagues, and friends across the company have encouraged, advised, and contributed questions for my studies and this research. MITRE has provided supplemental technical instruction, research resources, and staff to make this research possible

The geographically far-flung but close-knit Capitol family has been essential to every step of the journey leading to this dissertation. I thank Dr. Char Sample, DSc in IA Class of 2013, who braved the unknown by joining the very first program cohort in 2010, for convincing me to apply for the program. I thank Dr. Helen Barker and Dr. Jason Pittman, who have advised me, and so many other students, throughout this arduous path, keeping me on track to the goal. I thank all of my course professors, but in particular Dr. Howard Van Horn, who agreed to mentor me and chair the committee overseeing this research. I also thank committee members Dr. Salim Zafar and Dr. John Bornmann, both also MITRE colleagues, who with Dr. Van Horn are making sure I "get it right."

Finally, I thank two family members: Dad for teaching me the value of true research with his advice, "Always know the real rules; look it up yourself to be sure," and Kay for letting me rant, calming me when I needed it, pushing me when I needed it, and just plain putting up with me through this amazing experience.

TABLE OF CONTENTS

| | |
|---|------|
| List of Tables | xv |
| List of Figures | xvii |
| CHAPTER 1: INTRODUCTION | 1 |
| Background of the Problem..... | 2 |
| Statement of the Problem | 5 |
| Purpose of the Study | 6 |
| Significance of the Study | 8 |
| Nature of the Study | 11 |
| Overview of Research Method..... | 11 |
| Overview of Design Appropriateness..... | 13 |
| Research Questions | 13 |
| Theoretical Framework | 14 |
| Systems Engineering Framework..... | 15 |
| Information Assurance Framework..... | 17 |
| Human Performance Framework..... | 18 |
| The Overarching Framework..... | 18 |
| Definition of Terms | 19 |
| Assumptions | 23 |
| Scope and Limitations | 24 |
| Scope and Scale | 25 |
| Limitations..... | 26 |
| Delimitations | 28 |
| Summary | 30 |
| CHAPTER 2: REVIEW OF THE LITERATURE | 31 |

| | |
|---|----|
| Title Searches, Articles, Research Documents, and Journals | 32 |
| Historical Overview | 33 |
| Current Findings..... | 36 |
| Theoretical Frameworks for Worker Compliance with Procedures..... | 36 |
| Methodologies for Gathering and Analyzing Quantitative Data..... | 39 |
| Methodologies for Gathering and Analyzing Qualitative Data..... | 54 |
| Compliance with Security Guidelines | 57 |
| Conclusion..... | 61 |
| Summary | 64 |
| CHAPTER 3: METHOD | 67 |
| Research Method and Design Appropriateness | 67 |
| Research Questions | 69 |
| Password Policies | 71 |
| E-Mail Policies | 71 |
| Data Protection Policies..... | 72 |
| Ethical Computer Use Policies..... | 72 |
| Variables..... | 73 |
| Population..... | 74 |
| Sampling Frame | 75 |
| Geographic Location..... | 76 |
| Data Collection..... | 76 |
| Confidentiality, Anonymity, and Participant Trust..... | 78 |
| Instrumentation..... | 80 |
| Validity and Reliability | 82 |
| Survey Reliability | 82 |

| | |
|--------------------------------|-----|
| Content Validity | 83 |
| Internal Validity..... | 83 |
| External Validity..... | 86 |
| Experiment Procedure..... | 87 |
| Participant Solicitation | 88 |
| Population Sampling | 89 |
| Data Analysis | 93 |
| Response Analysis..... | 94 |
| Quantitative Analysis | 94 |
| Qualitative Analysis | 100 |
| Summary | 102 |
| CHAPTER 4: RESULTS..... | 104 |
| Pilot Study..... | 105 |
| Content Validation..... | 105 |
| Survey Validation..... | 105 |
| Data Collection..... | 107 |
| Participant Solicitation | 107 |
| Participation Timing..... | 108 |
| Findings..... | 109 |
| Data Plan Modification..... | 109 |
| Sample Size | 110 |
| Response Rate..... | 110 |
| Quantitative Results | 111 |
| Password Composition | 112 |
| Password Storage..... | 114 |

| | |
|--|-----|
| Correlation of Responses..... | 116 |
| Qualitative Results | 117 |
| Password Composition | 120 |
| Password Storage..... | 124 |
| Summary | 129 |
| CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS | 132 |
| Limitations | 132 |
| Findings and Interpretations..... | 133 |
| Answers to the Research Questions..... | 133 |
| Password Composition | 134 |
| Password Storage..... | 135 |
| Conclusions Related to the Frameworks..... | 136 |
| System Engineering Framework | 136 |
| Information Assurance Framework..... | 137 |
| Human Performance Framework..... | 140 |
| The Overarching Framework..... | 140 |
| Recommendations | 141 |
| Recommendations for Future Research | 141 |
| Use of Collected Data..... | 141 |
| Follow On Quantitative Studies | 142 |
| Comparing IA and Non-IA Workers | 143 |
| Ask the Counterpoint Questions..... | 144 |
| Improving the Qualitative Data | 144 |
| Response Rate in Data Collection | 145 |
| Summary | 146 |

| | |
|---|-----|
| REFERENCES | 147 |
| APPENDIX A: IA TRAINING CONTENT..... | 168 |
| APPENDIX B: SURVEY INSTRUMENT | 189 |
| Introduction and Instructions | 190 |
| Survey Preview | 192 |
| Informed Consent Agreement..... | 193 |
| Confirmation of Eligibility to Participate..... | 193 |
| IA Job Duties..... | 194 |
| Questions Supporting the Research Questions..... | 194 |
| Password Policies | 195 |
| E-Mail Policies | 196 |
| Data Protection Policies..... | 197 |
| Ethical Computer Use Policies | 198 |
| Conclusion and Thanks | 200 |
| Pilot Survey Questions | 201 |
| APPENDIX C: SURVEY PARTICIPANT SOLICITATION | 202 |
| Content Validity Review..... | 202 |
| Pilot Participant Solicitation..... | 203 |
| Research Survey Request for Volunteers..... | 205 |
| First Reminder, September 28, 2014..... | 206 |
| Second reminder October 6, 2014 | 207 |
| Third reminder, October 13, 2014 | 207 |
| Fourth reminder, October 19, 2014 | 208 |
| Fifth Reminder, October 26, 2014..... | 208 |
| Final Notice, Closing the Survey, October 31, 2014..... | 209 |

| | |
|---|-----|
| APPENDIX D: LITERATURE SEARCH | 210 |
| APPENDIX E: MEASURES OF TRAINING EFFECTIVENESS IN PRIOR STUDIES | 211 |
| APPENDIX F: POPULATIONS, IA FOCUS AREAS, & RELATED TRAINING IN PRIOR STUDIES | 213 |
| APPENDIX G: LITERATURE SUMMARY FROM ABRAHAM (2012)..... | 217 |
| APPENDIX H: METHODOLOGY MAP | 219 |
| APPENDIX I. ACRONYMS..... | 221 |

List of Tables

| | |
|---|-----|
| Table 1. Sample Sizes at Two Levels of Confidence and Margins of Error, $p=0.5$ | 90 |
| Table 2. Demonstration of Lack of Effect of Adjusting for Population | 91 |
| Table 3. Response Rate for Individual Questions (Example)..... | 94 |
| Table 4. Compliance Frequency Responses (Example) | 97 |
| Table 5. Compliance Frequency Responses by Percentage (Example)..... | 97 |
| Table 6. Mean Amount of Time Users Do Not Comply..... | 100 |
| Table 7. Planned Steps in Qualitative Analysis Process..... | 101 |
| Table 8. Themes of Non-Compliance Reasons, a priori..... | 102 |
| Table 9. Affinity Group Membership Levels | 108 |
| Table 10. Number of Submitted Surveys by Week | 108 |
| Table 11. Response Rate for Each Data Collection Question for Entire Survey..... | 111 |
| Table 12. Compliance Frequency Responses for Password Composition..... | 113 |
| Table 13. Compliance Frequency Responses by Percentage for Password Composition | 113 |
| Table 14. Compliance Frequency Responses for Password Storage | 114 |
| Table 15. Compliance Frequency Responses by Percentage for Password Storage..... | 114 |
| Table 16. Mean Amount of Time Users Have Not Complied with Password Guidance | 115 |
| Table 17. Themes for Possible Reasons for Non-Compliance | 119 |
| Table 18. Behavioral Theories in Information Security Studies (Abraham, 2012)..... | 120 |
| Table 19. Distribution of Themes in Reasons for Using Personal Information in Passwords... | 120 |
| Table 20. Distribution of System Components in Reasons for Using Personal Information in Passwords | 121 |
| Table 21. Distribution of IA Elements in Reasons for Using Personal Information in Passwords | 122 |

| | |
|---|-----|
| Table 22. Distribution of Performance Theories in Reasons for Using Personal Information in Passwords | 123 |
| Table 23. Distribution of Framework Categories in Reasons for Using Personal Information to Form Passwords..... | 124 |
| Table 24. Distribution of Themes in Reasons for Writing Down Passwords..... | 124 |
| Table 25. Distribution of System Components in Reasons for Writing Down Passwords..... | 125 |
| Table 26. Distribution of IA Elements in Reasons for Writing Down Passwords | 127 |
| Table 27. Distribution of Performance Theories in Reasons for Writing Down Passwords | 128 |
| Table 28. Distribution of Framework Categories in Reasons for Writing Down Passwords | 128 |
| Table D1. Literature Search Categorization | 210 |
| Table E1. Measures of Training Effectiveness | 211 |
| Table F1. Prior Research Study Populations, Focus, & Training..... | 213 |
| Table G1. Summary of Behavioral Theories in Information Security Studies..... | 217 |

List of Figures

| | |
|--|-----|
| Figure 1. Compliance frequency distribution (example) highlighting the frequency distribution across the entire sample with proportionate contributions of each sub-group (with and without IA duties) visible. | 98 |
| Figure 2. Compliance frequency distribution (example) highlighting the comparison of distribution curves of the two subgroups, with and without IA duties. | 98 |
| Figure 3. Compliance frequency distribution (example) illustrating the proportion of IA and non-IA subgroups at each declared frequency level. | 99 |
| Figure 4. Th3 P@\$\$WOrd_Ch@ll3ng3 summary page from the Cyber Awareness Challenge 2.0 training (DISA 2013). | 112 |
| Figure 5. Compliance frequency distribution for password composition showing the approximate proportion of time personal information was used to develop passwords. | 113 |
| Figure 6. Compliance frequency distribution for password storage showing the approximate proportion of time passwords were written down, | 115 |
| Figure 7. Comparison by proportion of the sample of the frequency of failing to comply with password formation and password storage guidelines. | 116 |
| Figure 8. Th3 P@\$\$WOrd_Ch@ll3ng3 practice screen providing two examples of password complexity guidelines (DISA, 2013). | 126 |
| Figure 9. Th3 P@\$\$WOrd_Ch@ll3ng3 summary screen showing the mandatory password complexity policy used in the intelligence community (DISA, 2013). | 127 |
| Figure A1. Contents of Cyber Awareness Challenge by major topic. | 168 |
| Figure A2. Guidelines for using computer ethically. | 169 |
| Figure A3. Tips for peer-to-peer (P2P) and unauthorized software. | 169 |
| Figure A4. Social engineering tips. | 170 |
| Figure A5. Password tips. | 170 |
| Figure A6. Password tips, 2. | 171 |
| Figure A7. Ethical e-mail user agreement. | 171 |

| | |
|---|-----|
| Figure A8. Tips about phishing: a type of social engineering. Phishing attempts use suspicious e-mails or pop-ups. | 172 |
| Figure A9. Tips about phishing: a type of social engineering. To protect against phishing. | 172 |
| Figure A10. Tips about internet hoaxes. | 173 |
| Figure A11. Tips about spear phishing. | 173 |
| Figure A12. Tips about whaling. | 174 |
| Figure A13. Guarding against identity theft. Guidelines to protect yourself. | 174 |
| Figure A14. Summary of security advice for e-mail. | 175 |
| Figure A15. Removable media and mobile computing/PEDs. | 175 |
| Figure A16. Tips for removable media use. | 176 |
| Figure A17. To protect removable media. | 176 |
| Figure A18. Situational awareness tips. | 177 |
| Figure A19. Social networking - guarding your online privacy. | 177 |
| Figure A20. Social networking tips - protecting your organization. | 178 |
| Figure A21. Travel tips, when using mobile computing devices in public. | 178 |
| Figure A22. Tips for identifying personal identity information (PII) and personal health information (PHI). | 179 |
| Figure A23. Tips for protecting personal identity information (PII) and personal health information (PHI). | 179 |
| Figure A24. Tips for security of mobile computing and PEDs. | 180 |
| Figure A25. Guidelines for identifying sensitive information. | 180 |
| Figure A26. Protecting sensitive information. | 181 |
| Figure A27. Data classification guidelines for classified information. | 181 |

| | |
|--|-----|
| Figure A28. Protecting sensitive information, continued. | 182 |
| Figure A29. Data classification guidelines - Unclassified. | 182 |
| Figure A30. To protect classified data - summary. | 183 |
| Figure A31. Spillage tips. | 183 |
| Figure A32. Spillage tips - if a spillage occurs. | 184 |
| Figure A33. To protect against the insider threat. | 184 |
| Figure A34. Classified data on the Internet tips. | 185 |
| Figure A35. Telework guidelines. | 185 |
| Figure A36. Beware of cookies. | 186 |
| Figure A37. Malicious code tips. | 186 |
| Figure A38. Mobile code tips. | 187 |
| Figure A39. Home computer security. | 187 |
| Figure A40. Wireless technology tips. | 188 |
| Figure H1. Mixed method procedures diagram for concurrent, embedded design research, in the format recommended by Creswell and Plano Clark (2011). | 219 |

CHAPTER 1: INTRODUCTION

Schneier recognized that "security is a process, not a product" (2000, p. xii). Explaining the importance of incorporating a systems approach into security, Schneier declared, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" (2000, p. xii). The foundation for the research described here rests on treating information assurance (IA) as more than just technology, indeed as a system, as Schneier recommended. As a system, IA has elements that include policies, procedures, hardware, software, and people (Haskins, 2011). To analyze IA failures, and then propose corrective action, it is essential to consider which system elements may have contributed to the failures. It would be illogical to assume a priori that IA failures are always due to the failure of any one element of the IA system.

For instance, Schneier (2000) admitted that it had been wrong to assume that lack of strong data protection was the problem with information security. Schneier acknowledged that the technology of cryptography was not the singular solution to protecting information. Likewise, Adams and Sasse (1999) argued against the assumption that users are always the problem in security. Pfleeger and Caputo (2012) demonstrated that human behavior, including the interaction of attitudes and policies, must be considered in addition to technology when addressing cybersecurity. Various system elements interact together, affecting successes and failures in IA. People, complying with policies, following defined procedures, using the tools of hardware and software to work with information, are at the critical intersection of the interacting elements of an IA system. The study took a step forward in determining reasons for failures of specific IA policies by asking people, as one element in the IA system, reasons for not complying with IA policies (following operating procedures) when working with information.

This introductory chapter includes a discussion of the background of the problem of IA compliance and the nature of the study. The discussion continues with a statement on the purpose of the study and how the study results will assist the IA community in future endeavors. After presenting specific research questions, the chapter presents the theoretical framework in which the work was designed. The chapter continues by describing the overall scope of the study, assumptions used in the design, and limitations recognized in the study. Throughout this research effort there has been an underlying philosophy of taking a systems engineering approach to the problem, described further below. Throughout, the study design keeps in mind the major components of every system: people, processes, and tools (Haskins, 2011).

Background of the Problem

Users do not always comply with security policies; Al-Omari, El-Gayar, and Deokar (2012) saw a need to develop a tool to test whether employees are likely to comply with security procedures. Software developers still see security and usability as conflicting requirements, trading off one for the for the other in software design, and can display a failure to consider usability as a factor for the end-users (Al-Saleh, 2011). In contrast, other researchers such as Susarapu (2012) have taken a more positive position, advocating aligning security and usability from the beginning of development of systems. By examining information assurance as a system, with system elements that include policies and procedures; technology, both hardware and software; and people, to include training, skills, capabilities, attitudes, and motivations (Haskins, 2011), IA proponents can examine all of the system elements for opportunities to improve the IA state of an environment. It is not realistic to assume that all IA policies are reasonable, or all IA procedures are practicable, or all IA technologies are effective, or all IA technologies are easily usable, or that the only weak point in the IA system is the human element, without testing to

confirm each of those assumptions. Yet, there may be a temptation to make just such an assumption treating any one of the elements of the IA system as the sole source of weakness. The described research used the human element as a source of information on IA effectiveness, but may open the door to evidence of a variety of IA system elements that would benefit from re-examination and subsequent improvement.

The need to design security¹ processes to meet actual users' needs and expectations is not a new revelation. Adams and Sasse (1999) pointed out the particular problem of addressing user capabilities in designing password management processes. That same year Whitten and Tygar (1999) reported the difficulty average users had in using the digital signing and encryption program PGP 5 because of the poor design of the user interface. Seven years later, Sheng, Broderick, Koranda, and Hyland (2006) reported very little improvement in the usability of the updated PGP 9. Over a dozen years ago Brostoff and Sasse (2001) argued for the need to incorporate human factors elements into security design, taking a lead from safety critical processes in other systems. Researchers continued to encourage security developers to pay attention to the human factors and environment (Sasse & Flechais, 2005).

Boss, Kirsch, Angermeier, Shingler, and Boss (2009) approached the challenge of user compliance with security policies from the standpoint of a directive oversight process for supervisors. Displaying a similar attitude that external processes must control system users,

¹ As can be seen by inspection of the references, common terms used alternatively in the literature include *computer security*, *information security*, *information assurance*, *cyber security*, and simply *security*. The preferred term used in this paper is *information assurance*; however, the alternate terms have also been used, in context with cited works.

D'Arcy and Hovav (2007) proposed a combination of technical and procedural steps to prevent system misuse. Research continued by examining how user awareness of system enforcement, the threat of negative consequences for non-compliance, might reduce misuse (D'Arcy, Hovav, & Galleta, 2009).

Researchers have examined attempts to align user expectations with security processes (Heckle, Lutters, & Gurzick, 2008). Heckle and Lutters (2011) observed situations in which basic security procedures conflicted with common workflow expectations by system users in work environments. In contrast to security specialists' attitude towards users as being malfeasant (Kraemer & Carayon, 2007), security professionals have begun to recognize users may have good reasons for ignoring the procedures dictated by the security designers (Herley, 2009).

The described study proceeded by asking people reasons for not complying with specific IA policies. The resulting data could have indicated problems with the people themselves, such as lack of or poor training (Abraham, 2012), indifferent attitude or lack of motivation (Johnston & Warkentin, 2010a, 2010b; Kim, 2010; Herath & Rao, 2009a, 2009b; Workman, Bommer, & Straub, 2008, 2009), or differing priorities than IA principles (Heckle & Lutters, 2011). The resulting data could have indicated problems with the overarching policies, such as unresolved conflicting policies (Heckle & Lutters, 2011). The resulting data could have indicated problems with the procedures, such as actions prescribed that cannot be carried out in the work environment (Adams & Sasse, 1999; Heckle & Lutters, 2011; Koppel, Wetterneck, Telles, & Karsh, 2008). The resulting data could have indicated problems with the hardware and software, such as designs that are effectively unusable (Whitten & Tygar, 1999; Sheng et al., 2006). Although cited references above date to 1999 and 2000, the review in Chapter 2 has demonstrated that a gap still exists in the literature on understanding reasons for IA system

failures. The described research results have narrowed some of that gap. Further, the literature review has demonstrated that each of the cited studies, as well as other discovered research, began by focusing on only a specific element of the full IA system. Researchers apparently implicitly assumed that understanding a single IA system element could lead to improvements in overall IA conditions. The research provides data to help prioritize future research into the most impactful IA elements.

Users of computer systems do not consistently comply with prescribed information assurance policies (Al-Omari et al., 2012) or with generally advised IA practices (Aytes & Connolly, 2004). As demonstrated in Chapter 2, existing research literature does not provide sufficient information on why users do not comply with IA policies. Without an adequate understanding of why users do not follow IA guidance, practitioners cannot propose meaningful changes in policies, procedures, technology, or user development intended to improve IA. Results from the described research provide the IA community with a validated set of users' stated reasons for non-compliance.

Statement of the Problem

A general problem is that users of computer systems do not consistently comply with prescribed information assurance policies (Al-Omari et al., 2012; Workman et al., 2008, 2009). As Blythe, Koppel, and Smith (2013) expressed the problem, "Good users do bad things" (p. 80). Al-Omari et al. saw a need to develop a tool to test whether employees are likely to comply with security procedures. To be effective, such a tool must be based on an understanding of why users do not comply with IA policies. Al-Omari et al. focused attention on user training as a reason for non-compliance. However, as observed above, such a training-centric view may be too restrictive to fully understand the breadth of reasons users have for not complying with IA

policies. The need for understanding why users do not always comply leads to a more specific problem: existing research literature does not provide comprehensive information on why users do not comply with IA policies.

In an extensive review of the literature, no studies have been identified in which researchers simply asked participants reasons for not following IA policies. As detailed in Chapter 2, reports in the literature of IA compliance by users either addressed actions but not reasons (i.e. Jones & Heinrichs, 2012) or tested theories about reasons for not complying focused on only a single element of the IA system (i.e. Herath & Rao, 2009a, 2009b). The described research adds to the collection of validated information on reasons users do not comply with IA policies. The study followed a mixed methods research design to obtain and organize information on users' stated reasons for not complying with IA policies.

The study used anonymous survey questions to determine quantitatively what proportion of the study population has not followed specific IA policies and to what extent. See Chapter 3 for details on the source training program of the selected IA policies. The survey also asked participants to state reasons for non-compliance, resulting in qualitative data as narrative responses. Using qualitative research data analysis methods (Bornmann, 2014a, 2014b; Creswell, 2012; Creswell & Plano Clark, 2011; Ryan & Bernard, 2003) allowed organization and categorization of the study participants' stated reasons. The general target population for the described study was working adults in a broadly defined employment sector who have all completed mandatory IA training prior to participation in the study.

Purpose of the Study

The general goal of the described study was to develop data on stated reasons users do not follow IA policies on the job. More specifically, the purpose of the described study was to

determine reasons IA-trained U.S. federal government workers state for not complying with specific IA policies, using a mixed methods research methodology with an online anonymous survey data collection instrument. The study gathered the required data by asking a volunteer sample from the target population to report anonymously on recent (within two years) activity with regard to specific IA policies. Data collection and analysis involved both quantitative and qualitative methodologies, using a mixed methods study design (Creswell & Plano Clark, 2011). Mixed method research was appropriate for the described study, because the quantitative portion confirmed participants' level of non-compliance, and the qualitative portion allowed collection and categorization of reasons for non-compliance. As originally planned the independent variable for quantitative analysis was whether participants have any IA job duties. The dependent variables for the quantitative analysis was whether the participants have complied with each IA policy and, if not, with what general frequency. For the qualitative data, the variable information was the narrative statement of reasons for non-compliance.

The target research population was adult workers who have completed mandatory IA training on the job, similar in that respect to research by Caputo, Pflieger, Freeman, and Johnson (2014); Eminağaoğlu, Uçar, and Eren (2009); and Heckle and Lutters (2011). However, for the described study, the target population was workers in or supporting U. S. Federal government work with associated IA training, a population not previously identified in discovered literature. The selected target population, encompassing federal civil service, uniformed service, and supporting contractors, has mandatory annual IA training. Further, the same IA training program, the *Cyber Awareness Challenge v2.0* (Defense Information Systems Agency [DISA], 2013), developed and maintained by the Department of Defense, is used across the government. Thus, the target population was not be restricted to specific government departments or agencies.

Significance of the Study

The described study is significant because the resulting data may set the stage for follow-on research to quantify the impact of reasons for not complying with IA policies. As explained in more detail in Chapter 3, the described study followed a concurrent mixed methods research design, gathering quantitative and qualitative data in a single stage. In addition, the resulting qualitative analysis may set the stage for a follow-on quantitative study, thus making the described study the first stage of a larger exploratory sequential mixed methods design (Creswell & Plano Clark, 2011).

While not planned for study as part of the described research, a follow-on study may be able to use the categorized and normalized reasons for non-compliance in a survey to quantify the occurrence of each of the main categories of reasons across a population. Even without such a follow-on quantization of reason usage, the normalized set of reasons from the described study may guide efforts to improve IA by changes to policies, procedures, technology, training, or motivation elements. Should the suggested follow-on study take place, the resulting quantified results may help improve the prioritization of the decisions on how to improve IA performance. The described study has not broken new ground with the planned methodology but adds to the literature for defined user populations studied. The described study has also expanded existing knowledge in the literature by simply asking participants reasons for actions, instead of embedding assumed reasons in the experimental design.

The fundamental methodology for the described research is not unique. Previous research has included self-reporting of compliance with IA policies (Jones & Heinrichs, 2012; Kruck & Teer, 2010; Lomo-David & Shannon, 2009; Mensch & Wilkie, 2011; Mylonas, Kastania, & Gritzalis, 2013; Stanton, Stam, Mastrangelo, & Jolton, 2005; Teer, Kruck, & Kruck,

2007). Use of pre-existing IA training content as the basis for compliance studies is also not unique (Caputo et al., 2014; Dodge, Carver, & Ferguson, 2007; Eminağaoğlu et al., 2009; Heckle & Lutters, 2011; Kruck & Teer, 2010). One unique aspect of the described study is asking participants reasons for non-compliance, instead of assuming a possible set of reasons. Koppel et al. (2008) used interviews to ask for reasons for non-compliance with prescribed medical practices, discovering several common staff workarounds to standard bar code medication system procedures with as a practical reaction to the actual hospital working environment. However, no study discovered in an extensive literature review reported asking similarly about IA procedures.

Another unique aspect of the described study was the addition of a new category of defined population to the literature: workers in and supporting U.S. federal government departments and agencies. Populations described in previous research on IA compliance included university students (Abraham, 2012; Aytes & Connolly, 2004; Dodge et al., 2007; Jenkins, Durcikova, & Burns, 2012; Johnston & Warkentin, 2010a, 2010b; Jones & Heinrichs, 2012; Kruck & Teer, 2008, 2010; Lomo-David & Shannon, 2009; Shaw, Chen, Harris, & Huang, 2009; Teer et al., 2007), healthcare workers (Heckle & Lutters, 2011; Koppel et al., 2008; LaRosa et al., 2007; Warkentin, Johnston, & Shropshire, 2011), workers in the general business environment (Bulgurcu, Cavusoglu, & Benbasat, 2009, 2010; Caputo et al., 2014; Eminağaoğlu et al., 2009; Herath & Rao, 2009a, 2009b; Kim, 2010; Puhakainen & Siponen, 2010; Rhee, Ryu, & Kim, 2012; Shropshire, 2008; Stanton et al., 2005), and the general undifferentiated public (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010; Mylonas et al., 2013; Sim, Liginlal, & Khansa, 2012). The size of the target population may also be unique. The Defense Information Systems Agency (DISA) originally developed the training used in the described study, the *Cyber*

Awareness Challenge (DISA, 2013) for use across the U.S. Department of Defense (DoD). The same training is now used across many federal departments and agencies, in addition to the DoD. The DoD alone includes over 3.2 million military and civilians (DoD, n.d.) plus about 700,000 contractors (Garamone, 2013). Since DISA (2013) made the Cyber Awareness Challenge training available for other non-DoD departments and agencies, the complete target population likely extends many thousands beyond the DoD's approximately 4 million, by including other federal departments' and agencies' staffs. Given the amount and range of sensitive information, from personal healthcare to classified national security, in federal information systems, a better understanding of the IA practices of the target population may lead to practical improvements in protecting that information.

Prior studies described in the literature have asked participants to report on following IA rules or guidelines (Jones & Heinrichs, 2012; Kruck & Teer, 2008, 2010; Lomo-David & Shannon, 2009; Mensch & Wilkie, 2011; Mylonas et al., 2013; Stanton et al., 2005; Teer et al., 2007). Other reported studies have used observation to determine IA policy compliance, with either the researchers as the observers (Yang, Ng, Kankanhalli, & Yip, 2012), or with third parties as the observers (Puhakainen & Siponen, 2010; Rhee et al., 2012; Shropshire, 2008; Stanton et al., 2005). While some of the discovered studies addressed reasons for not complying with IA policies, the reasons were asked with closed-end questions allowing only selection from a set of specific responses, such as in Abraham (2012) and Al-Omari et al. (2012).

Results from the described study may benefit several groups: senior managers in government and non-government enterprises; IA professionals, including IA system developers, IA operations specialists, IA trainers and IA training developers; and the volunteer participants in the study. With the organized set of reasons that users give for not complying with IA policies,

senior leaders in enterprises who are responsible for the high-view policies on use and processing of information may recognize opportunities to update such policies to align the policies more properly with users' environment and motivations. Those same senior leaders may also infer from the responses reason to shift prioritization of resources to meet IA goals among budgets for technology development and fielding, budgets for operations and enforcement, or budgets for IA training and awareness programs. IA professionals may recognize opportunities to improve the nature of design and implementation of IA technologies or of IA awareness and training programs. Such potential benefits would be broader, for instance, than the focus of Al-Omari et al. (2012) on IA awareness only. With the nature of the survey questions derived directly from formal IA awareness training, the study participants may benefit from the survey effectively being refresher training in fundamental IA policies.

Nature of the Study

The described study was an application of mixed methods research, combining quantitative and qualitative procedures in a single study (Creswell & Plano Clark, 2011). Quantitative data was collected and analyzed with regard to the proportion of participants reporting actions within the past two years that did not comply with IA policies. Qualitative data were collected in the form of narrative statements by the participants on reasons for non-compliance with IA policies. The study included an analysis of the qualitative data, categorizing the participants' reasons into generalized reasons for non-compliance.

Overview of Research Method

The described research asked participants two questions concerning several selected IA situations: What have the participants done, and why? By asking the same questions on behavior of a sample of a population, instead of just one or a few individuals, the collected data were

amenable to quantitative analysis with the quantitative results generalizable across the population. The analysis of the collected data used descriptive statistics (Zafar, 2012) to make statements about the proportion of the population that has taken certain actions and about the frequency of those actions.

The quantitative strand of the described study applied statistical methods to the participants' reported level and frequency of compliance with selected IA policies. Descriptive statistics (Zafar, 2012) applied to the data provided answers to the research questions of what proportion of the population has complied with IA policies and of how often have users not complied with IA policies. By asking participants about IA duties on the job, the descriptive statistics also provided information on possible different levels of IA compliance between the two sub-groups.

Salkind (2012) stated that the general purpose of qualitative research is to examine human behavior in context. The study questions were used to consider human behavior in the context of the IA environment in the workplace. Previous studies, discussed in detail in Chapter 2, have examined what people did with regard to IA practices. A subset of the cited studies also examined reasons for the actions. However, no discovered studies in IA, and only limited numbers of related studies in other fields, examined reasons for action without bounding the possible reasons. The described study involved a data collection methodology for qualitative data of open-ended questions (Fink, 2009), followed by thematic analysis of the data (Bornmann, 2014a, 2014b; Ryan & Bernard, 2003). The researcher expected that results of the described data collection and analysis methods would be meaningful data on workers' stated reasons for non-compliant IA actions across a broader spectrum than prior research has provided.

Overview of Design Appropriateness

As stated above, the purpose of the described study is to determine reasons trained users state for not complying with specific IA policies. In order to learn why participants have not followed IA policies, it is first necessary to confirm that the participants have not followed the policies. The collection of research data on the participants' actions, as a precursor to collecting data on the reasons for actions, provides an opportunity to conduct quantitative analysis on levels of activity in the sample and thus to infer activity in the target population. With the actions of the participants established in the quantitative part of the data collection, the use of open-ended narrative data collection in a qualitative research methodology supported the study purpose. The use of statistical analysis (Creswell, 2012; Salkind, 2012; Zafar, 2012) in the quantitative analysis provided potentially useful information about the population. Building on the narrative data using qualitative research analysis methods (Bornmann, 2014a, 2014b; Creswell & Plano Clark, 2011; Creswell, 2012; Ryan & Bernard, 2003), not only provided further insight into participants' reasons for actions, but also developed the basis for possible further research. The planned mixed method research design (Creswell & Plano Clark, 2011) was appropriate to meet the goal of determining the participants' stated reasons for non-compliance with IA policies.

Research Questions

The general question the described study addressed is *why have trained users not complied with IA policies, and what proportion of a trained user populations has not complied with IA policies?* This compound question breaks down into several closely related questions:

- R1. Why have users not complied with prescribed IA policies?
- R2. What proportion of the population has failed to comply with prescribed IA policies?
- R3. How often have users failed to comply with prescribed IA policies?

As stated, these three research questions required further refinement in order to develop a meaningful research design. All three questions include the phrase *prescribed IA policies*. Because there are so many IA policies addressing a broad range of specific and general actions and guidelines, this phrase is not precise enough to gather data. The research data focused on specific IA policies, derived from the *Cyber Awareness Challenge* training program (DISA, 2013). Using the selected IA policies described in detail in Chapter 3, the described research was based on specific, detailed quantitative survey questions plus associated open-ended qualitative survey questions. Once data was available on the responses to those questions, it as possible to make summary conclusions in answer to the three general research questions, as stated above. See the Research Questions section in Chapter 3 of this dissertation for discussion of the selection and use of the policies in the research design. The first research question addressed the purpose of the study, asking *why*. The second and third research questions asked how often the user population violated policies. There are two dimensions to the *how often* question: How many users violate policies, and how often does any one user violate a policy? See Chapter 3 for detailed discussion on how the research design addressed both of these questions for each of the specific policies.

Theoretical Framework

Three frameworks from different disciplines were involved in the process of selecting, defining, and designing the described research: systems engineering (SE), information assurance (IA), and human performance. The overarching framework that influenced the design of the described research was the fundamental approach of systems engineering. When using a systems engineering approach to solve a problem or produce a result, the SE framework prescribes analyzing the context as a defined, bounded system, composed of three major elements of

people, tools, and processes (Haskins, 2011). Within the field of information assurance, IA frameworks described in the literature range from the simple three component confidentiality-integrity-availability (CIA) model for information security (Committee on National Security Systems, 2010) to the ten domain Common Body of Knowledge (CBK[®]) of (ISC)²[®] as Tipton (2010) described, and beyond. Recognizing the impact of the *people* component of any system intended to produce information assurance results led to considerations of human performance engineering frameworks that deal with aspects of capability and motivation. Discussion follows providing more detail on how each of the three framework types relate to the described research.

Systems Engineering Framework

Systems engineering is based on the concept of a system as the basis for design, action, or problem solving. Three formal definitions of *system* (see Definition of Terms) all have in common the concept that a system is composed of interacting elements (ISO/IEC/IEEE, 2008; Haskins, 2011). In IA, as in any system, the interacting elements can include tools (hardware, software, other physical devices), people, and processes (Haskins, 2011). A breakdown in the assurance of any information may result from a failure of any of the interacting system elements. It may not be reasonable to assume that an individual not acting in accordance with any specific IA policy is attributable to only one element of the system without examining the reasons for the non-compliant action. For instance, when a user does not follow a specific IA policy, there are many possible reasons. The reason might be related to any of the following conditions:

- lack of training,
- poor training,
- lack of belief in ability to comply (self-efficacy),
- inability to complete the prescribed procedures at the time and place of action,

- lack of regard for the consequences (positive or negative, i.e. reward or punishment),
- lack of belief in the need for policy,
- lack of belief in the legitimacy of the policy,
- failure of required hardware,
- failure of required software,
- conflicting policies,
- conflicting procedures,
- conflicting goals (e.g. job task accomplishment vs. IA).

The described study treated the provision of information assurance as a system within a systems engineering framework. Following standard SE practices (Haskins, 2011; MITRE, 2012), analysis of any system requires specifying the inputs and outputs to the system and identifying the system elements. For the generalized IA system, the system elements considered in the described research include people, policies, procedures, hardware, and software.

The system element *people* further breaks down to address human factors in design and use of the IA system. With regard to addressing human factors, Haskins (2011) identified human systems integration as an essential enabler of SE. Thus, applying SE to an IA system requires considering aspects of motivation, training, and innate capabilities of the people in the IA system, involving both technical and management processes.

For the purposes of the study discussion, *policies* and *procedures* are related but separate system elements. Using the first definition in Merriam-Webster (Policy, n.d.), a policy is a high-level guidance, while a procedure is a more detailed operational instruction. (See the Definitions section, below, for specific meanings of each word.) As an example, stating general guidelines

for handling classified data (DISA, 2013, see Figure A27. *Data classification guidelines for classified information.*) is a policy. One procedure supporting the stated policy is the password complexity requirement specifying number of characters and character types and re-use limitations (DISA, 2013, see Figure A6. *Password tips, 2.*). The described study does not use an alternate definition of *policy* found within the technical realm of IA usage, such as a *firewall policy* meaning the detailed configuration rules for a firewall allow/deny rule set.

Information Assurance Framework

As stated above, there is no single, universal IA framework. Frameworks extant in the IA community range from the simple CIA model of information security defined by CNSS (2010), to (ISC)²'s CBK[®] (Tipton, 2010), DHS's Essential Body of Knowledge (EBK; Shoemaker & Conklin, 2012), to the framework for critical infrastructure cybersecurity from the National Institute of Standards and Technology (NIST, 2014). The described study adopted Parker's (1998, 2002) essential IA attributes as the most useful and usable IA framework in the context of the research. The Parkerian Hexad of IA attributes consists of confidentiality, integrity, availability, possession (or control), authenticity, and usability (Kabay, 2008). The choice of the Parkerian Hexad for the study's reference IA framework derived from the integration of the framework attributes with the key system elements, discussed further below. Parker's six attributes focus directly on the information and principles of how to treat the information. The six attributes comprise almost as simple a framework as the basic CIA triad, and thus may be more widely applied in practice than more complete, but more complex, frameworks such as the CBK or EBK.

Human Performance Framework

Research literature on human behavior of compliance with IA, safety, and medical practice policies referred to a variety of behavioral models. Al-Omari et al. (2012) considered several models, including Rational Choice Theory (RCT), Protection-Motivation Theory (PMT), General Deterrence Theory (GDT), and the Technology Acceptance Model (TAM; Davis, Bagozzi, & Warshaw, 1989), settling on TAM as a useful basis to propose a parallel Security Acceptance Model (SAM). Other researchers who considered TAM in evaluating rule behavior included Aytes and Connolly (2004) and Herath and Rao (2009a, 2009b). Abraham (2012) identified 11 theories of human behavior derived from seven disciplines that 17 studies in information security have used to consider security behavior. In a review of the literature on security behavior, Lebek, Uffen, Breitner, Neumann, and Hohler (2013) identified 54 different theories on behavior.

The Overarching Framework

The general purpose of the described study, described above, is to learn the reasons that users give for not complying with specific IA policies. More specifically, the purpose of the described study is to determine reasons IA-trained U.S. federal government workers state for not complying with specific IA policies, using a mixed methods research methodology with an online anonymous survey data collection instrument. Using the qualitative analysis methodology of thematic analysis (Ryan & Bernard, 2003) across the collected data of reasons provided a logical organization of the reasons given by participants. The resultant categorization may allow both enterprise managers and IA professionals to focus resources on improvements in the IA system most likely to result in benefit to the overall IA posture of the enterprise. Efforts to improve the IA posture could work in any of the system elements of the IA system. Combining

concepts from an IA framework (Parker, 1998, 2002) and the range of human performance theories (Abraham, 2012) into the structure of system elements (Haskins, 2011) results in a potentially useful set of themes, or categories, to expect in the collected data. The resulting systems engineering framework, informed by both information assurance and human performance theory, provided the a priori set of themes for use in the thematic analysis. For the actual analysis, the process included identification of emergent themes to add to the categories developed from the frameworks and prior research. The researcher also recognizes that every theme identified a priori from the framework may not appear in the completed analysis of the collected data. See the data analysis section of Chapter 3 for more details.

Definition of Terms

The following terms are used throughout this study.

Computer security: “Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated” (CNSS, 2010, p. 15)².

Cybersecurity: “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (Bush, 2008)” (DoD, 2014, p. 55).

² While CNSS published definitions in CNSS Instruction No. 4009 specifically for the National Security community of the U. S. federal government, the U. S. National Institute of Standards & Technology (NIST) included, with source citation, the same definitions for use across all levels of government and the commercial sector (Kissel, 2013).

Human factors: "The systematic application of relevant information about human abilities, characteristics, behavior, motivation, and performance. It includes principles and applications in the areas of human related engineering, anthropometrics, ergonomics, job performance skills and aids, and human performance evaluation" (Haskins, 2011, p. 363).

Human systems integration: "The interdisciplinary technical and management processes for integrating human considerations within and across all system elements; an essential enabler to SE practice" (Haskins, 2011, p. 363).

-ilities: "The developmental, operational, and support requirements a program must address (e.g., availability, maintainability, vulnerability, reliability, supportability, etc.)" (Haskins, 2011, p. 363).

Information assurance: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (CNSS, 2010, p. 35).

Information security: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (CNSS, 2010, p. 37).

Policy has two related meanings; in the IA environment, the reader must determine by context that is intended. When the context is a broad statement of intent, the definition is "a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body" (Merriam-Webster, n.d., 2 a). When the context is for a specific, detailed procedure, the definition is "a definite course or method of action selected from among

alternatives and in light of given conditions to guide and determine present and future decisions" (Merriam-Webster, n.d., 2 b).

Procedure: "a series of actions that are done in a certain way or order" (Merriam-Webster, n.d., 2 a).

Self-efficacy: "Self-efficacy consists of the belief of people in their ability to complete the task (Bandura, 1986)" (Abraham, 2012, p. 20).

System (1) – "A set of elements in interaction. (von Bertalanffy 1968)" (Pyster & Olwell, 2013, glossary).

System (2) – "A combination of interacting elements organized to achieve one or more stated purposes. (ISO/IEC/IEEE, 2008, Terms and definitions 4.31).

System (3) – "A combination of interacting elements organized to achieve one or more stated purposes. An integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements. (INCOSE)" (Haskins, 2011, p. 362).

System element – "A member of a set of elements that constitutes a system. A system element is a discrete part of a system that can be implemented to fulfill specified requirements. A system element can be hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination" (ISO/IEC/IEEE, 2008, Terms and definitions 4.32).

Systems engineering (1) – "Interdisciplinary approach governing the total technical and managerial effort required to transform a set of customer needs, expectations, and constraints

into a solution and to support that solution throughout its life” (ISO/IEC/IEEE, 2010, Terms and definitions 3.3005).

Systems engineering (2) – “An interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs” (Haskins, 2011, p. 363).

Systems engineering (3) – “three-part definition of SE: (1) SE is the translation of a need or deficiency into a system architecture through the application of rigorous methods to the iterative process of functional analysis, allocation, implementation, optimization, test, and evaluation; (2) it is the incorporation of all technical parameters to ensure compatibility among physical and functional interfaces, and hardware and software interfaces, in a manner that optimizes system definition and design; (3) it is the integration of performance, manufacturing, reliability, maintainability, supportability, global flexibility, scalability, interoperability, upgradability, and other special capabilities into the overall engineering effort.” (Committee on Pre-Milestone A Systems Engineering, 2009, pp. 124-125).

Systems engineering (4) – “An interdisciplinary approach and means to enable the realization of successful systems. It focuses on holistically and concurrently understanding stakeholder needs; exploring opportunities; documenting requirements; and synthesizing, verifying, validating, and evolving solutions while considering the complete problem, from

system concept exploration through system disposal” (Systems Engineering Body of Knowledge [SEBoK] Authors, 2013, Systems Engineering glossary Discussion section).

Assumptions

The design of the described study is based on an online, web-based survey instrument, to be completed voluntarily and anonymously. As such, there were two fundamental assumptions about the study participants:

Assumption 1. Participants would answer the survey questions honestly.

Assumption 2. Participants would each submit only one completed survey.

Because participants were asked to admit to violations of policy, the assumption of honest answers is particularly important. The research design includes strong protections of confidentiality and anonymity for participants. The care in protecting the participants' anonymity was based on another study assumption:

Assumption 3. Participants would trust the description of anonymity sufficiently to give honest answers to the survey questions.

The provisions of the data collection steps to maximize anonymity of participants leads, however, to the need for another assumption.

In order to maintain anonymity for participants, the sample were self-selecting members of the population, responding to an openly accessible web-based survey. Further, the questions in the survey asked only minimal demographic information. As a result, it was not possible to either control for or confirm any level of stratified sampling in the final participant group. Lack of the ability to control the sample to be appropriately representative of the population raises the question of whether the study suffered from a response bias (Creswell, 2012) or a sampling bias.

Given the reliance on anonymity to invoke assumptions 1 and 3, it is necessary to include another assumption:

Assumption 4: The participating sample membership is representative of the target population.

During the analysis of the collected data, the researcher discovered an unexpected result in the nature of the data from survey respondents. The analysis required a modification of the study analysis plan and the addition of a fifth study assumption. See the discussion in Chapter 4 for a complete explanation and statement of the fifth assumption.

Scope and Limitations

The scope of this study is to examine the information assurance practices of workers who have completed a mandatory, recurring information assurance awareness training program, represented by the *Cyber Awareness Challenge* (DISA, 2013). Workers required to complete the annual federal government IA awareness training are federal civilian employees (civil servants), uniformed service members, and internal contractors in U.S. federal government departments and agencies, as well as employees of companies working under contract to the federal government not performing such work within a department or agency. The intent is to survey staff across the enterprise, not just high-technology workers or those with information assurance responsibilities. Due to the minimal amount of demographic data collected from participants, an artifact of the design for strong anonymity, discussed in Chapter 3, the number of organizations represented in the study sample is not known. Nonetheless, the results should be generalizable across Federal government organizations. Thus, conclusions based on this study may assist many organizations.

Scope and Scale

Using the reference IA awareness training program (DISA, 2013) as the source, the researcher has identified ten specific IA policies suitable for study in the described research. See the detailed discussion in Chapter 3 on the criteria for and identification of the ten policies. Integrating ten policies into the three generalized research questions results in a total of thirty research questions to answer. Such a robust set of research questions may be overly ambitious for a doctoral dissertation, representing an initial effort in independent research. In order to scale the research leading to the final dissertation to a manageable level, the researcher conducted the complete analysis on only a selected subset of the identified policies. The ten policies group into four general categories: two password policies, two e-mail policies, two data protection policies, and four ethical use policies. The researcher proposes conducting the complete analysis on only the two password policies, using data collected with the online survey.

While proposing to use data on only two IA policies for the dissertation research, the researcher also recognized the potential value of applying the same analysis to all ten policies. Carrying out the full analysis on the remaining eight identified IA policies could expand the literature significantly, beyond the initial contribution of the described research. Further, the researcher suggests that a significant factor of the described research is obtaining participation from the target population in data collection surveys of the type described (Creswell, 2012; Fink, 2009). By collecting data on all ten selected IA policies in a single use of the described online survey, the same statistical significance would apply to all the parallel data. With the data on all ten policies derived from the same sample of participants, additional correlation of responses comparing the different policy types may be possible. For instance, future research could examine whether the set of categories for non-compliance for the memory-based password

policies developed in the described study is the same as the set of categories found in the personal-gain ethics related policies. Therefore, the researcher used the data collection process for the described study to cover all ten identified IA policies, while focusing the study on only the two password-related policies. The use of a one-time survey conserved resources and supports future additional research studies.

Limitations

Creswell (2012) pointed out that research studies might have two types of limitations: weaknesses in or potential problems with the study. As is common in many research survey plans, the researcher cannot guarantee a statistically significant sample size from the population, because only volunteers from the target population will participate in the survey. Further, the researcher cannot guarantee that the proportion of survey participants across any declared independent variables, such as demographic information, will reflect the actual distribution across those variables in the target population. A limitation of the described study is the distribution of IA versus non-IA workers in the surveyed sample may not reflect the same distribution as in the target population. The researcher cannot control for any of these aspects, thus the limitations remain. However, by conducting adequate recruiting in advertising for participants across the target population these limitations were not expected to impact the research. Nonetheless, see the section on Data Plan Modification (p. 109) for actual impact.

One significant limitation of the described study is the reliance on participants' honesty in completing the survey. Heckle and Lutters (2011), citing Cranor and Garfinkel (2004), and Sasse, Brostoff, and Weirich (2001), acknowledged the difficulties in using experimental environments to replicate usability issues and the reality that, with security, people say and do different things (Sasse et al., 2001, p. E52). The described study avoided the first problem by

addressing actions on the job instead of in an experimental situation. The described study addressed the second problem in two ways. The survey questions asked *Have you...* instead of *Do you ...* in order to influence the participants to recall specific actions, rather than considering general intentions. In addition, the data collection process maximized the anonymity of participants (see Delimitations, below) and conveyed as clearly as possible to the participants the confidentiality of the responses and the anonymous nature of participation, removing as much as possible fear of repercussions for failure to follow rules, which might induce lying in the survey.

The use of anonymity for participants introduced another limitation for the described study. With no means of conducting follow-up surveys with participants, there was no way to cross-check for validity of the responses. With only minimal demographic data collected, there was no way to use cross-checks or correlation to confirm the validity of the demographic data from participants. Just as one study assumption is that participants would answer the compliance questions truthfully, so the same assumption of honest responses means the study must trust the validity of all responses.

Another limitation in the study was the inability to control the sample selection for any sort of demographic stratification relative to the overall population. Stratified sampling is a common method for controlling sample selection with a goal of ensuring the sample is representative of the population (Fink, 2009; Zafar, 2012). The decision to maximize the data collection conditions for confidentiality and anonymity of the participants, discussed above, resulted in a lack of data on demographic patterns in the sample, with one exception. The survey questions included only one demographic question for data, whether the participant has IA job duties. Analysis of the collected data was limited in that analysis against many commonly studied demographic variables, such as age, sex, level of education, geographic location, etc.,

was not possible. Since the survey participants in the sample were volunteers from among the population, it was impossible to ensure a truly random sample. Thus, the survey participants may represent a *biased sample* rather than an *unbiased sample* (Zafar, 2012). See below for one delimitation intended to improve the likelihood of an unbiased sample with regard to the independent variable.

Delimitations

While the researcher cannot control the limitations, delimitations are factors the researcher can, to an extent, control, thus establishing the scope or parameters of the study (Baron, 2008). For this study, procedures for handling and storing completed surveys and data will ensure maximum practical confidentiality for participants. Siponen, Pahnla, and Mahmood (2010) recognized the possibility of respondents not answering honestly if there is a fear of exposure to the employer. Just as Siponen et al. limited the amount of demographic data collected and used a web survey site not associated with the employer, the described study used similar controls to assure respondents that anonymity and confidentiality were protected. The survey announcement and introduction communicated the assurance of confidentiality, describing specific actions as supporting evidence, to the target population. These assurances may have influenced the participants to be truthful on the surveys, since the participants would not be personally embarrassed by any perceived failures in IA actions.

Salkind (2012) warned of the possibility of interviewer bias when conducting surveys. Since researcher bias may be reflected in the wording and context of survey questions, a delimitation in the described study to minimize such bias was careful wording and context of the questions. Each of the action questions in the form *Within the past two years, have you ...?* used wording as close as possible to the exact wording found in the Cyber Awareness Challenge

(DISA, 2013), illustrated in Appendix A. See the individual survey questions in Appendix B to compare each question with the source training content, cross-referenced to Appendix A. For the open-ended questions asking for reasons, bias was avoided by including no further context or examples in the question than the immediately preceding action question. The intent of the neutral nature of the reasons question was to avoid any framing that examples or suggestions could cause.

One limitation, described above, is the possibility of a biased sample (Zafar, 2012) resulting from the self-selection of volunteer participants. Due to the method of advertising for volunteers, using numerous professional connections, many of the initial recipients of the participant recruiting notice may be individuals working in the IA field. Since IA duties was the one demographic aspect in the study, optimum validity of results depended on the proportion of sample participants with IA duties being equivalent to proportion of the population with IA duties. As a delimiting action, the participant solicitation included the following statement: *It is important that workers from all job categories take part in this survey. Please share this survey announcement as broadly as possible across your organization with colleagues who may be eligible to take part.* There may be concern that this chained advertising of the survey was a form of snowball sampling. However, as discussed by Goodman (2011), the described study is not using a hard-to-reach population, with limited direct sampling. The redistribution of the solicitation announcement was a broadcast process, specifically asking for broad distribution across many job categories. Thus, the conditions of respondent-driven sampling in hard-to-reach populations (Goodman) calling for population adjustment estimators (Heckathorn, 2011) did not apply. See Appendix C for the solicitation announcement.

Summary

This introductory chapter has presented a general problem of user compliance with IA policies (Al-Omari et al., 2012; Workman et al., 2009), leading to the specific problem of a lack of information in the research literature on reasons users state for not complying. Having derived three research questions from the problem statement, the chapter established the purpose of the described study, to determine reasons IA-trained U.S. federal government workers state for not complying with specific IA policies, using a mixed methods research methodology with an online anonymous survey data collection instrument. Focusing the described study on a large but definable target population of trained users of U.S. federal government information, the chapter described a context for the study analysis, incorporating concepts from three frameworks. The chapter described the integration of information assurance, systems engineering, and human performance into a framework structure for analyzing data collected in an anonymous survey from members of the target population.

The next chapter of this dissertation comprises a review of the literature relevant to the research. The reviewed literature included aspects of IA and worker compliance behavior theory, practice, and measurement. The literature review chapter established the basis for the problem statement of a gap in the literature on reasons for non-compliance with IA policies.

The third chapter presents detailed discussion of the research methodology to be followed, appropriateness of the selected methodology for the study purpose, description of the data collection method using an online survey, and the methods for analyzing the collected data. Following the list of cited references are several appendices referred to in Chapters 2 and 3. Appendix A provides the IA guidelines content from the source training material. Appendix B includes the complete content of the data collection survey.

CHAPTER 2: REVIEW OF THE LITERATURE

The research addressed the general topic of computer security practices and the more specific topic of level of compliance with basic security practices found in a specific information assurance awareness training program. The literature review process began with those same two general topic areas, narrowing the search down to more specific search topics as the literature search progressed. The goal was to understand the current level of knowledge of end-user security practices, related to common information security training. Appendix D summarizes the nature and range of the literature search conducted for the study, including documents not cited as references in this dissertation.

The described research used an anonymous survey asking volunteer participants from a specific population to self-report compliance with selected information security practices. The survey asked for participants' compliance reporting on specific security practices addressed in the organization-specific information assurance training *Cyber Awareness Challenge* (DISA, 2013). Given the research context, the review of the literature discovered during the search included examination of the use of surveys and other methods to measure training effectiveness and to measure compliance with established practices. Appendix E, *Measures of Training Effectiveness in Studies*, presents a summary of the nature of research methods, surveys and others, described in the reviewed literature. The article reviews also examined the descriptions of the populations previously studied for rules compliance, particularly in information assurance, the sub-topics within the broad range of information assurance that were addressed in the studies, and the nature of any training identified as relevant to the studied population. Appendix F, *Study Populations, IA Focus Areas, and Related Training of Prior Research*, collects a summary of key aspects from each reviewed study for ease of comparison across the literature.

This chapter addresses the terms used for general searches, the use of selected specific articles for chaining to other prior research cited in the articles, and additional research documents consulted through the *citation chaining* process. Citation chaining is the process of following reference citations backward from a key, relevant document, checking citations used in that document, and forward, checking documents that cite that key document (Cribbin, 2011). The result is a sequence of references on a topic, documenting the steps in the development of scientific knowledge on the topic, like links in a chain. The process is repeated through *citation cycling*, back to foundational sources and forward to the most recent work in a set of interrelated topics addressed in the research effort, resulting in a network of relevant citations. Cribbin called the process *citation chain aggregation* (p. 2150). From that groundwork, the chapter includes a short discussion of the historical background on research in computer security practices training and compliance and the current level of knowledge, which the described research supplements.

Title Searches, Articles, Research Documents, and Journals

The literature for the study was drawn from the following available online databases: *Scopus, Science Direct, IEEE Xplore, ACM Digital Library, ProQuest, EBSCO Host, SAGE Journals, Microsoft Academic Search, and Google Scholar*. Each of these databases was searched sequentially with a series of search terms or phrases: *effectiveness of security training, compliance with security training, computer security training, information security training, information assurance training, cybersecurity training*, plus *compliance* paired with each of those terms. In addition, use of citation chaining (Cribbin, 2011) allowed discovery of additional relevant references, following citations used in key works, especially dissertations, discovered in the search process.

Over time terminology in the literature dealing with protection of information in the computing environment has included the terms *computer security* (Dodge et al., 2007), *information security* (Shropshire, 2008), *information assurance* (Johnston & Warkentin, 2010a), and *cybersecurity* (Pastor, Diaz, & Castro, 2010) or *cyber security* (Caputo et al. 2014). While these terms do not have identical meanings or connotations, all are closely related; each is relevant to the research proposal, thus all were used as essentially equivalent during the literature search and reviews. For clarification of the similarities and differences of the terms, see *Definitions of Terms* in Chapter 1 for definitions of each term.

Historical Overview

Available literature included reports on two closely related practical aspects of information assurance: IA training methods and effectiveness (Abraham, 2012; Kim, 2010; Shaw et al., 2009) and compliance with that training (Caputo et al., 2014; Dodge et al., 2007; Heckle & Lutters, 2011). The review of literature here examined several methods used to measure both training effectiveness and level of compliance. Each measurement method has pros and cons (see Chapter 3) related to ease of administration, cost of administration, and possible questions concerning validity of the resulting data. Logically, the level of compliance with information assurance protocols should be a principal measure for the effectiveness of the information assurance training.

While the focus of the described research was on the level of compliance with information security protocols, the literature review covered several interrelated topics. To support the selection of methodology for gathering data on information security practice compliance, the review looked at methods used to determine such compliance: self-reporting (Jones & Heinrichs, 2012; Stanton et al., 2005), researcher observation (Heckle & Lutters, 2011;

Koppel et al., 2008; Yang et al., 2012), third party observation (Puhakainen & Siponen, 2010; Shropshire, 2008; Stanton et al., 2005), and system record event analysis (Eminağaoğlu et al., 2009; Heckle & Lutters, 2011; LaRosa et al., 2007; Workman et al., 2008, 2009). Under the logic that compliance with prescribed practices is unlikely, or even impossible, if the user community is unaware of the recommended practices, the review extended into reported research on effectiveness of training for information security. Based on an observation that there are parallels in the question of compliance with security practices, healthcare practices, and safety practices (Brostoff & Sasse, 2001), the literature review extended into topics on safety compliance and safety training effectiveness. Further, searches in the safety literature led to reported studies in the medical and health field, such as Heckle (2011), which addressed both information security and patient safety aspects in the hospital environment. Extending the examination of measuring training effectiveness added studies on general training effectiveness to the review.

The field of information assurance has developed over many years out of the predecessor areas of computer security, network security, and information security. Practitioners have recognized the expanding view of the principles involved and actions necessary to make information reliably usable for decision-making. Today, the classic CIA model of confidentiality, integrity, and availability of information and information systems (Kabay, 2008) is widely accepted as the basic information security framework. However, even before the CIA terminology was in general use, Gasser (1988) described the same concepts, defining *computer security* as including *secrecy* (confidentiality), *integrity*, and protection against *denial of service* (availability, p. 4). Further, Gasser addressed the issue of system security (Ch. 2) with the

observation that, "the problem is people, not computers" (p. 11). Gasser went on to comment that the use of technology to provide computer security is oversold (p.12).

As the practice of computer security matured into the field of information assurance, newer frameworks for IA have come onto the scene, each newer framework building out from the seminal CIA model. Parker (1998, 2002) proposed supplementing CIA with three additional information attributes, resulting in what Kabay (2008) described as the Parkerian Hexad of *confidentiality, possession or control, integrity, authenticity, availability, and usability*. The National Security Agency (NSA, 2002) promulgated an information system security engineering approach to IA (NSA, 2002, Ch. 3). The International Information Systems Security Certification Consortium, (ISC)², developed and continues to maintain the Common Body of Knowledge (CBK; Tipton, 2010). Likewise, the professional organization ISACA developed and maintains the COBIT framework (ISACA, 2012). In 2008 the Department of Homeland Security (DHS) introduced the Essential Body of Knowledge (EBK; Shoemaker & Conklin, 2012), since subsumed into the National Initiative for Cybersecurity Careers and Studies (NICCS), available at <http://niccs.us-cert.gov>. The National Institute of Standards and Technology (NIST) is leading a government and industry partnership for the National Initiative for Cybersecurity Education (NICE), with its own comprehensive framework (<http://csrc.nist.gov/nice/framework>). The list of IA frameworks above is not exhaustive; many other industry-specific and geographic-specific frameworks can be found in a search of the literature. The purpose of cataloging the frameworks is to observe that, while selected frameworks proposed specific uses of technology as part of a recommended approach to information assurance, every one of the frameworks recognized the central importance of people in the people-process-tools system equation (Haskins, 2011), whether or not a specific framework has an explicit systems engineering basis.

Continuing the recognition of the importance of addressing the people component in information security, Herath and Rao (2009a) cited Hamill, Deckro, and Kloeber (2005) as stating that effective information security depends on all three components of people, processes, and technology. Hamill et al.'s declaration reflected an understanding of the systems engineering concept (Haskins, 2011) that obtaining effective results from a system requires people following the proper processes when using the available tools (technology).

Current Findings

Theoretical Frameworks for Worker Compliance with Procedures

Abraham (2012) cataloged a variety of behavioral theories identified in studies of information security. See Appendix G for Abraham's summary table. Research literature demonstrated a broad application of behavioral science theories to information security. Lebek, Uffen, Breitner, Neumann and Hohler (2013) identified 113 studies over a ten year period, featuring 54 different behavioral theories. The discussion below provides a review of several selected studies that focused on particular behavioral theories or frameworks related to compliance with security policies. Described studies include several identified by Abraham as well as additional studies discovered in the course of the literature review.

Similar to the purpose of the described research, Aytes and Connolly (2004) sought to understand why individuals do not follow safe computing practices, even when aware of possible negative consequences. Aytes and Connolly studied a population of business class students at two large universities asking about frequency of engaging in five common unsafe computing practices. Rather than linking the questions to specific security training Aytes and Connolly assumed that the students had been exposed to security advice within the university culture and

environment. The study further asked participants about awareness of safe computing practices and attitudes about possible negative consequences of unsafe actions.

The survey instrument questions on frequency of specific actions presented participants a verbal frequency scale for responses, similar to the described study instrument, with response options of *never, rarely, occasionally, frequently, all the time* (Aytes & Connolly, 2004, p. 37). Additional questions sought to ascertain participants' awareness of safe computing practices, as well as attitudes about likelihood of specifically identified negative consequences occurring (Aytes & Connolly, 2004, Appendix). The Aytes and Connolly survey instrument did not include unstructured questions, which would have allowed for open-ended responses directly answering a question of why.

Aytes and Connolly (2004) interpreted the responses on awareness and attitude, relative to the unsafe action responses, within a framework of a rational choice model. The model presented accounted for participants' awareness of safe practices and negative consequences, modified by perception of the availability of the safe practice, the probability of a negative occurrence, and the severity of negative consequences. In taking a human performance approach with the rational choice model, Aytes and Connolly observed that individuals act unsafely, even when aware of safe practices and possible negative consequences. The authors suggested that more than awareness training on correct practices and negative risks will be necessary to change the level of compliance with security guidelines in a working population. Aytes and Connolly further suggested the need for a more complete performance model, possibly by incorporating aspects of the technology acceptance model with the rational choice model.

Workman et al. (2008, 2009) tested hypotheses relating attitude to compliance performance based on a threat control model (TCM; Workman et al., 2008), comparing the TCM

to protection motivation theory (PMT; Rogers, 1975, 1983). The study was motivated by an interest in the relationship between individual and organizational factors on worker performance. Using a triangulation methodology Workman et al. correlated attitudes about information system security threats, self-efficacy, organizational policies, and self-reported behaviors derived from a survey, with actual practice determined by examination of system logs and records. The perceived threats addressed by the TCM included external threats to the information and organizational threats to the workers if caught not complying. The population studied was a sample of workers in a U.S. technology firm. Workman et al. concluded there is interaction between individual and organizational factors, in terms of organizational procedural justice.

Siponen et al. (2010) studied the relationship between intention and practice in employee compliance with information security policies in four Finnish companies across diverse business sectors. Structuring an anonymous survey based on several theories of motivation and behavior Siponen et al. examined aspects of PMT, rewards, reasoned action, deterrence, and innovation diffusion. The cited article did not provide details on the survey questions, so it was not possible to determine how Siponen et al. distinguished between intention and action among the respondents. The article also did not indicate the specific security policies or related training activities addressed in the survey questions. The reported conclusions dealt with correlating several behavioral theories with employees' compliance actions but did not address possible reasons for non-compliance. Nonetheless, Siponen et al. concluded that managers might benefit from increasing the nature and awareness of rewards to employees for complying with security policies.

Godlove (2012) focused attention on testing applicability of the theory of planned behavior. Surveying teleworkers with an online questionnaire Godlove examined the

participants' attitudes about general information security principles and opinions about organizational security policies. Godlove compared the attitudes and opinions with intentions to follow general security policies as elicited in the questionnaire. The general conclusion reached from the study was that the theory of planned behavior is applicable to information security intention in teleworkers.

Methodologies for Gathering and Analyzing Quantitative Data

The described study examined the level of compliance with information assurance training. In order to understand the available methods for gathering data, the literature review included prior work in areas of evaluating the effectiveness of training, not limited to IA training. Compliance on the job with key training points may be the ultimate measure of training effectiveness but is not the only measure found in the literature. Therefore, the review examined the range of measurements used to measure training effectiveness, including compliance. Researchers have used numerous methods to gather data in order to measure the effectiveness of training. The literature reports a variety of data gathering methods:

- quizzes with knowledge questions (Kim, 2010),
- practical task exercises (Shaw et al., 2009),
- surveys (Puhakainen & Siponen, 2010),
- interviews (Heckle & Lutters, 2011),
- on-the-job performance observation by untrained observers (Stanton et al., 2005),
- on-the-job performance observation by trained observers (i.e., members of the research team, Koppel et al., 2008),
- surreptitious task exercises (Caputo et al., 2014; Dodge et al., 2007),
- and statistics on end-results in organizational performance (LaRosa et al., 2007).

The types of data gathered in prior research studies also varied:

- direct application of the training in task activity (Shropshire, 2008; Jones & Heinrichs, 2012),
- knowledge of the training content (Kim, 2010),
- attitudes about the quality of the training (Kim, 2010),
- attitudes on the participants' ability to apply the training (Johnston & Warkentin, 2010a),
- and attitudes on the participants' intention to apply the training (Stanton et al., 2005).

Appendix E, Measures of Training Effectiveness in Studies, displays specific reviewed studies across the dimensions of types of data collection (survey, quiz, researcher observation, third party observation, record data analysis), participant attitude or performance, and relationship to training recency.

The literature review examined the general subject of measuring training effectiveness and rules compliance, as well as studies that addressed specifically effectiveness in the training for information assurance. Information assurance covers such a broad range of topics that such studies have rarely attempted to measure more than a limited number of IA sub-topics. The table in Appendix F, Study Populations and IA Focus Areas of Prior Research, summarizes the IA subtopics and target populations addressed in reviewed studies.

In a study to examine dimensions of intention and ability to comply with security practices, Stanton et al. (2005) used a combination of surveys on password usage and interviews with managers likely to be familiar with worker security practices on the compliance observed among workers. The workers and managers Stanton et al. studied were from a range of

companies and organizations across the U. S., obtained through the efforts of a commercial survey company. Thus, the data included direct, self-reporting of compliance levels, plus third party observations. Given the range of over 1,000 survey participants across the country, Stanton et al. made no effort to correlate the survey questions with any established training materials. The focus of Stanton et al. was more on a two-dimensional model of compliance than the levels of compliance with security practices. The methodology of surveys for first person reports and interviews for third-person reports combined to inform the study on multiple levels.

The European Network and Information Security Agency (ENISA) surveyed organizations and governments in the European Union (EU) for an evaluation of methods used to assess the effectiveness of security awareness training (ENISA, 2007). From one dozen possible measures, ENISA reported general agreement that the most effective measure was the number of security incidents traced to human behavior. However, there was also general agreement that audit findings, staff surveys, staff testing, and number of staff completed training were all roughly equivalent in measuring training effectiveness. Kim (2010) reviewed the ENISA data and other models of corporate training evaluation, suggesting that such measures may not be the most relevant for measuring information security training effectiveness. Kim observed that collecting survey data after training could help in measuring the impact of training (p. 25).

Dodge et al. (2007) tested user compliance with specific security training directly, rather than asking for self-reporting or using a quiz on the content of the training. Students at the United States Military Academy had received mandatory, recurring IA training that included how to recognize and respond to phishing emails. The researchers sent phishing emails to the student body, containing realistic clues that the emails were fake. Dodge et al. monitored student actions with regard to three potentially dangerous actions when reading malicious e-mail:

clicking on embedded links, providing sensitive information using forms on web pages linked in the e-mail, or opening attachments. Dodge et al. used these phishing exercises to measure the effectiveness of the IA training. The researchers repeated the exercises at intervals across the academic year and across multiple years. The first trial in the academic year was in September, so that new first year students had time to become familiar with the campus computers and network, but had not yet had initial IA training (p. 75). The data collection extended over a two year period, allowing longitudinal analysis of one year group over that period.

Shropshire (2008) defined an overall compliance value as the dependent variable for research, the Information Security Protocol Compliance (ISPC). Using a paired set of surveys, Shropshire asked the subject users (bank tellers) questions concerning attitudes about job and employer (a bank) but no direct questions on security knowledge, attitudes, or practices (Shropshire, 2008, App. A). To assess the employees' ISPC, Shropshire asked the employees' supervisors questions regarding awareness of the individual employee's security practices (Shropshire, 2008, App. B). The security practices addressed in the survey of the managers were fundamental and, while covered in the bank's security training, were not specialized or unique practices. Shropshire's approach was correlation of the reported compliance with recency of training, rather than training content (p. 163). The surveys were not anonymous, and Shropshire matched each employee's attitude survey with the direct supervisor's assessment survey for that employee for statistical analysis.

Shropshire (2008) had assured the employees that all specific input and identities would be kept confidential and also had an understanding with the bank that there would be no administrative actions against the employees for participation (p. 85). Shropshire's work relied on two significant uncontrollable trust items: that the bank tellers trust the confidentiality

promise sufficiently to be truthful in non-anonymous responses, and that the bank supervisors and administrators would follow through with the promise of no adverse actions against the employees. Further, Shropshire's measurement of the component action constituting the dependent variable of ISPC relied on the memory of untrained observers (the tellers' supervisors) of general compliance with a limited list of practices, rather than actively observed and recorded actions.

To further complicate Shropshire's (2008) data gathering, the survey questions administered to the supervisors were a mix of general employee behavior, such as undeserved work breaks and general work attendance rate, with general security practices instead of specific security actions such as securing passwords and neglecting to log off systems (Shropshire, 2008, App. B.). Such a form of combined-purpose questions could be a case of unintended *priming*. Pashler, Rohrer, and Harris (2013) observed that priming with incidental exposure to words or other stimuli have been reported in the literature to affect high level judgments on many topics (p. 959). Thus, combining questions on general employee performance with questions on specific information security practices could have resulted in the answers being an overall employee assessment, instead of reliable data on security practices.

The described research methodology did not emulate the data gathering methods of Shropshire (2008), due to two concerns. First, the lack of anonymity, with the surveyed attitudes and actions directly linked to the participants' employment, may have allowed the employer in Shropshire's study to guess which employee expressed specific attitudes about the job (Walsham, 2006). Loss of anonymity could reduce the level of honesty in the survey responses (Walsham, 2006, p. 329), whereas anonymity can result in frank and honest responses (Ng'ambi & Brown, 2009). Compare Shropshire with Puhakainen and Siponen's (2010) use of strictly anonymous

surveys (pp. 763, 766). Second, the use of the supervisors as untrained observers, asking for the supervisors' general memories of compliance, rather than specific, documented actions, seems likely to result in *halo effect* reporting (Wirtz & Bateson, 1995). The supervisors' responses may have been guided by an overall attitude about each teller, rather than a reliable measure of actual compliance.

Shaw, Chen, Harris, and Huang (2009) tested the effectiveness of various forms of IA training through the use of post training examinations. Shaw et al. developed two alternative training environments. Shaw et al. based one environment on hypertext content. Shaw et al. designed the alternative environment with extensive multimedia content. In the resulting study analysis Shaw et al. compared the effectiveness of the two approaches to training module design. The examinations included questions on content of the training, as well as exercises in applying that training. Thus, the assessment evaluated the short-term retention and comprehension of the training but did not test direct application of that training in day-to-day computer use, for either capability or motivation. One of Shaw et al.'s goals was to test the impact of the level of media richness in the training on the comprehension of the students (p. 95). Thus, limiting the study to short-term effectiveness does not lessen the value of the efforts in understanding the variety of training effectiveness measures reported in the literature.

In a study of the possible correlation between awareness of information security policies, the perceived fairness of those policies, and intent to comply with those policies, Bulgurcu et al. (2009) used a set of surveys as the measurement instrument. The research framework in Bulgurcu et al. focused on the attitudes of the participants, both about the information security policies and about the intent to comply with those policies, rather than any attempt to measure actual compliance. Bulgurcu et al. surveyed employees at multiple U.S. organizations, including

in the data analysis only respondents who acknowledged awareness of formal organizational security policies (p. 4). From the reported information, it did not appear that Bulgurcu et al. derived security policy questions in the survey from specific training. The study provided an example of use of participant surveys to measure an aspect of security compliance.

Subsequently, Bulgurcu et al. (2010) reported on further attitude surveys of participants relative to beliefs of participants and intentions to comply with security protocols. As with the previously reported study (Bulgurcu et al., 2009), Bulgurcu et al. (2010) applied questions on general security awareness aspects to respondents subject to formal security policies and training.

Eminağaoğlu et al. (2009) assessed corporate employee compliance with password policies, usage, and password quality; following corporate-wide security training; and various security awareness promotion programs. For the technical audits of password selection and use, Eminağaoğlu et al. used the password cracking tool L0phtcrack LC5 to analyze passwords in the corporate Microsoft Active Directory domain accounts. The analysis ranked passwords according to percentage of total passwords successfully cracked and time intervals of one minute, 15 minutes, two hours, and 24 hours. Researchers supplemented these technical audits with a non-technical audit consisting of surveys and meetings with employees to elicit the employees' understanding of password rules in the training. Eminağaoğlu et al. stands out among the many cited studies regarding compliance assessment because compliance was inferred, based upon the successful creation of useful passwords, instead of being directly measured. Eminağaoğlu et al. did not attempt to evaluate the specific passwords with password policy, approaching the password strength as an indirect measure of compliance.

Novakovic, McGill, and Dixon (2009) studied aspects of password usage within a framework accounting for both acceptance and use of technology. Using a widely advertised

online survey, Novakovic et al. asked participants to respond on a Likert scale of agreement, from *strongly disagree* to *strongly agree* to statements related to awareness, ability (self-efficacy), behavior intent, availability of assistance, and secure usage of passwords. In contrast to the described research, which asked participants to recall specific compliance, Novakovic et al.'s survey asked about general practice of compliance. The significance of Novakovic et al.'s study to the described research is the recognition of a variety of human performance models and the selection of a unified model of acceptance and use, for correlating attitudes with actions.

In a study focused on students in Turkey, Republic of China, and Nigeria, Lomo-David and Shannon (2009) used a self-reporting compliance survey that professors distributed to students via e-mail. The survey asked questions on familiarity with several information system security and safety practices and the percentage of time students used the specified practices. The survey questions covered familiarity and use of strong passwords, anti-virus software, firewalls, daily security scans of systems, and scanning of e-mail attachments. The survey did not seek reasons for compliance or non-compliance from the participants. The purpose of the study was to determine a possible correlation between familiarity with safety and security measures and actual practice in applying such measures. Lomo-David and Shannon determined a positive relationship between awareness and use of security measures for activities involving simple and complex passwords, system scans, e-mail scans, use of anti-virus software, and use of firewalls. The study results also indicated a lack of significant relationship between awareness and practice in four areas of computer usage: passwords on e-mail attachments, biometric authentication, multifaceted authentication, and use of intrusion detection systems. The study report did not indicate whether Lomo-David and Shannon controlled for the availability of the four security measures not exhibiting a correlation with awareness. Keeping in mind the purpose of the

described research, it is significant that Lomo-David and Shannon did not attempt to determine reasons for the participants' use or non-use of the safety and security measures.

Puhakainen and Siponen (2010) used three methods to collect data on the effectiveness of employee training: interviews, surveys, and observation. In both the interviews and anonymous surveys the researchers asked about the participants' awareness, knowledge, and motivation on security policies and practices but did not ask for self-reporting on compliance. Puhakainen and Siponen used anonymous surveys to supplement the interviews in order to ensure honest responses (Myers & Newman, 2007; Walsham, 2006). The purpose of Puhakainen and Siponen's research was to test the effectiveness of a new training program based on theories of learning and persuasion. Puhakainen and Siponen used surveys and management observers to establish a baseline of worker performance, then conducted two cycles of training with the theory-based training, refining the training from the first cycle based on survey feedback, followed by a second cycle of training and performance evaluation. For actual performance, the researchers used untrained observers (the company information security manager and employee supervisors) to observe and report on the employees' security practices. Relating Puhakainen and Siponen's study to the described research, the described research used participant surveys to gather self-reported compliance information, rather than only knowledge and awareness information. In addition, the described research used the self-reported compliance information as a proxy for effectiveness of ongoing, established training, instead of as a method of testing new, experimental training.

In one of a series of studies on effective methods for teaching protection against e-mail phishing attacks, Kumaraguru et al. (2010) compared alternative training methods of computer-based training and online web training. Kumaraguru et al. reported two separate exercises, each

with participants recruited by advertising. The first exercise involved 28 participants, recruited by local advertising on and near a university campus, in a laboratory training event and immediate performance testing activity (p. 7:21). The second exercise involved an online training activity with follow-up testing activities online with over 4,500 participants recruited through several advertising and news article links (p. 7:24). In both cases, Kumaraguru et al. tested participants' ability to apply the training lessons through performance exercises. The measured performance was an indicator of ability to comply, but not an actual measurement of intent to comply or actual compliance.

Johnston and Warkentin (2010a, 2010b) reported multiple studies examining various influences on university faculty, students, and staff attitudes and intent to comply with security training. In a study on the impact of a fear appeal as a motivation method, Johnston and Warkentin (2010a) administered surveys covering several aspects of participants' attitude, including *response efficacy* (how much the individual believes the response will be effective, 2010a, p. 551), self-efficacy, and performance expectation or intent (2010a, App. A). The university had security tools and training available for the participants, but Johnston and Warkentin did not require completion of such training as a condition for participation in the study. During the study the test group of participants received fear appeal information as a form of training prior to completing the survey; a control group was not exposed to the fear appeal content. Similarly, in a study examining the effect of source credibility on intentions to comply with security practices, Johnston and Warkentin (2010b) surveyed participants before and after exposure to security awareness training materials. In the latter report (2010b), the awareness training material used in the study emphasized the credibility of the source of information as the differentiator between test and control groups.

In a study of information security training effectiveness at a bank, Kim (2010) used short (ten or fewer questions) surveys to assess both employee attitudes and compliance knowledge. Employees completed surveys with questions about general information security knowledge and questions asking for application of that knowledge to simple cases. Kim presented the participating employees with a series of three different surveys with similar types of knowledge and application questions: first a pre-training quiz (App. B), then a survey quiz immediately following the training (App. C), and finally a long-term follow-up survey (App. D). Kim also used the surveys to assess the employees' satisfaction with the quality of the training (App. E), an attitude assessment, as opposed to a knowledge or ability check.

Mensch and Wilkie (2011) reported on a study of computer security attitudes among students at a mid-sized university. While Mensch and Wilkie described the study purpose as measuring security attitudes, the web-based survey used was, in effect, a self-reporting instrument for students to declare compliance with use of security tools and following common security behaviors. Mensch and Wilkie inferred the students' attitudes about the basics of computer security by whether or not the students followed the guidelines. Other questions in the survey asked more directly about attitudes than behaviors, such as toward data privacy (p. 97). In contrast with the university environment of Dodge et al. (2007), Mensch and Wilkie did not report the existence of any required or optional computer security training at the surveyed university. Thus, the study cannot be considered as examining either effectiveness of formal training or of compliance with formally prescribed security practices, only compliance with generally advised security practices.

Warkentin et al. (2011) addressed the concept of training effectiveness indirectly, basing research on the learning environment. The principal measures of effectiveness addressed in the

study were employee intention and self-efficacy. Warkentin et al. gathered data through surveys (App. C) conducted independently of formal training activities at the participating organization. The study purpose was to test correlation of employee attitudes and intentions with external cues in the workplace, as opposed to formal compliance training. The external cues addressed in the study included available learning resources, experiential learning opportunities, and verbal support from both peers and managers (p. 268). Warkentin et al. surveyed healthcare workers in multiple healthcare organizations. The survey asked those workers about attitudes and intent to follow the privacy guidelines imposed by the Healthcare Insurance Portability and Accountability Act (HIPAA), treating HIPAA guidelines as a proxy for HIPAA-required training in the healthcare organizations (p. 271). The questions in the survey asked participants about intent to follow security and privacy guidelines, rather than past behavior. Thus, the work of Warkentin et al. represented in the study provided an indicator of compliance, but not a measure of actual compliance.

Jenkins et al. (2012) compared the effectiveness of lean versus media-rich security training content. To assess the impact of each different training content, Jenkins et al. placed the research subjects in a simulated corporate work environment, in which the subjects had to implement login passwords for several systems, and evaluated the quality of the passwords the participants created, relative to the training received. Jenkins et al. administered prepared training in two alternative forms to the participants as part of the differentiation of training content. Thus, in Jenkins et al., task performance, rather than participant self-reporting, was the measure of compliance. One acknowledged limitation (p. 3293) was that the experiment was in an artificial environment and not a true observational experiment in the field.

As part of a study to develop a framework for privacy situational awareness, Sim et al. (2012) surveyed Facebook users online. Sim et al. limited the sample to Facebook users 18 or older, in the United States, with currently active accounts. A commercial market research firm, Zoomerang, administered the survey to a random selection of respondents (p. 59). Survey questions asked the respondents to self-report on awareness of privacy aspects in the context of privacy-related scenarios on Facebook. Given that the survey participants were widely diverse Facebook users, Sim et al. did not correlate the survey content with any specific information security training.

Abraham (2012) tested study participants' security practice capability through a series of survey questions requiring participants to apply principles from information security training. The security training was specific to the study, administered to undergraduate students in classes at a public university (p. 82). Questions in the survey included recognizing the actual target site of a given URL, or the difference between web pages loaded in http or https (App. D, E, F). Abraham's assessment method evaluated the participants' ability to apply individual learning, showing an understanding of the concepts and an ability to use the concepts on individual practical exercises. However, the method did not necessarily test the actual practice of the participants in daily computer use activities, since the participants knew the test was on the security practices. Abraham did not test for aspects of external distracting influences, motivation, and commitment to using security practices. Abraham included a summary table of behavioral theories used in IA research literature, reproduced with permission in Appendix G of this dissertation, which guided further literature searches for the described study.

Mylonas et al. (2013) were concerned that the literature presented insufficient information on smartphone security practices by users. Mylonas et al. surveyed smartphone users

in Athens, Greece, using a personal interview process (p. 49) interviewing random people on the street and at public transport locations, such as airports, subway and train stations. Survey questions covered the subjects' awareness of security issues and practices, attitudes concerning security and privacy on smartphones, and compliance with common security practices. Mylonas et al. did not attempt to learn the users' reasons for action or inaction with regard to security practices.

Caputo et al. (2014) used practical exercises in two cycles to test compliance with anti-phishing training, in an attempt to evaluate the effectiveness of embedded training. The test method involved sending phishing e-mails to a sample of a target population in two cycles for each of three conditions. In each case, the first cycle involved generating a training event following the participant's action of clicking on the phishing link in the email, consisting of a web page announcing that the e-mail was a phishing e-mail and providing a lesson on how to recognize such an e-mail. The second cycle involved another round of phishing e-mails, which the researchers intended to use as the measure of effectiveness of the training administered in the first round. Caputo et al.'s method has the advantage of testing application of the training principles in what appeared to be, for the participants, real-world situations. Lead author Caputo indicated plans to continue use of the surreptitious phishing technique in further studies, subsequent to those described (personal interview, March, 2012).

Focusing attention on the security practices using smartphones, Jones and Heinrichs (2012) surveyed users directly. The study population consisted of students in a public university in the United States. Differing from the study by Dodge et al. (2007) on several aspects, Jones and Heinrichs used volunteers aware of the study instead of unaware subjects in a surreptitious exercise. The solicited participants for the sample came from a single department (business)

instead of across the student body. There was no specific security training identified for any of the participants to have received. In order to develop the questions for the survey instrument, Jones and Heinrichs examined recommended security practices identified as recurring in popular literature (p. 24). Thus, Jones and Heinrichs assumed training to be from cultural exposure in the students' environment.

Surveys are widely used to collect data in research studies (Fink, 2009). Researchers can use survey questions to gather information from participants on attitudes, opinions, beliefs, intentions, motivations, knowledge, knowledge application (e.g. task exercises), individual participants' own actions (self-reporting), actions of others (observer reporting), et cetera. The literature review examined how surveys have been used in related studies of training effectiveness, general compliance training, and compliance with information assurance training and policies.

Herath and Rao (2009 a, 2009b) surveyed 317 (2009a) or 318 (2009b) employees across 77 (2009a) or 78 (2009b) organizations to determine those employees' perceptions about security threats, expectations of damage from security breaches, the employees' ability to make a difference in protecting information (response efficacy and self-efficacy), and expected consequences of failure to comply with security procedures, along with other related attitudes and intentions to comply with security procedures (2009a, App. A; 2009b, Table A2). Herath and Rao analyzed the correlation of attitudes with intention, concluding that perceptions of threats are likely to affect attitudes toward policies (2009b, p.106). Herath and Rao cited prior research (Gist, 1987; Torkzadeh, Pflughoeft, and Hall, 1999) relating training to self-efficacy, to support one of the study hypotheses, that self-efficacy will positively affect security compliance intentions (Herath & Rao, 2009b, p. 112).

Methodologies for Gathering and Analyzing Qualitative Data

As described previously, a review of the literature identified no research studies addressing reasons for IA policy non-compliance that focused on more than a single component of the overall IA system, such as training effectiveness (Al-Omari et al., 2012), software usability (Sheng et al., 2006), or worker motivation psychology (Boss et al., 2009; Bulgurcu et al., 2010). Further, every study identified in the literature review that asked about reasons for non-compliance limited the available responses to a pre-selected set of responses in closed-end question format.

The described research used open-ended questions to ask participants reasons for non-compliance without limiting the responses or prompting for consideration of a particular IA system element. The data analysis methodology for using the resultant narrative data was that of thematic analysis (Ryan & Bernard, 2003). Since the literature review identified no studies in the IA field using open narrative data and thematic analysis, exemplar studies from other fields provided examples of the thematic analysis. Five such studies are described below.

Brown, Kennedy, Tucker, Golinelli, and Wenzel (2013) studied relationship patterns and sexual activity of homeless men, using a combination of qualitative interviews and structured interviews in a mixed methods study. The data analysis used by Brown et al. on the qualitative data demonstrated an example of thematic analysis of interview content data with an emergent theme approach. Brown et al. began with a sequence of coding responses for five preselected themes, identified in previous research (Kennedy et al., 2013). During the analysis, Brown et al. identified five additional emergent themes discovered in the data, not predicted prior to the data analysis. Brown et al. used structured interviews for data collection. The combination of structured, recorded interviews followed by thematic analysis fit well with the study purpose.

The interviewers were able to elicit information from the participants that fit into the overall framework of the study, while allowing sufficient flexibility in the interview conversations for unforeseen information to emerge. The use of pre-selected themes and elicitation of emergent themes by Brown et al. parallels the data analysis in the described study, in which the preselected themes derive from the IA systems model.

Yu (2012) approached the problem of understanding why college students illegally download copyrighted digital information. Using a sequential qualitative - quantitative mixed methods approach, Yu began with a qualitative inquiry, interviewing 40 students on a college campus, asking about attitudes on digital piracy. Yu performed a content analysis on the recorded interview data, detecting patterns in the participants' justification for digital piracy. Thematic analysis of the narrative replies allowed Yu to identify specific themes, which were the basis for the subsequent quantitative survey stage of the study. The use of narrative data and thematic analysis was appropriate for Yu to establish baseline themes, amenable to further investigation. The qualitative portion of Yu's study correlated to aspects of the described research. Yu examined student justification for violating a rule not to download copyrighted material illegally. The researcher for the described study identified precisely the same rule as one of the ten IA policies examined in detail in the reference training program (DISA, 2013). Further, while justification of and reason for an action are not precisely the same concept, Yu's elicitation of the participant's justification themes parallels the planned thematic analysis of reasons in the described study.

Mazzola, Walker, Shockley, and Spector (2011) conducted a concurrent mixed methods study of graduate students' stressors. Noting that almost all prior research on the topic had used closed-end questions for data collection, Mazzola et al. chose to use open-ended questions for

data collection, expanding the possible themes beyond the researchers' pre-selected categories. In analyzing the qualitative data, Mazzola et al. began with a set of themes identified in prior research, but also used a coding method to identify new themes emergent in the data. The process allowed expansion of themes beyond prior research results. The use of open-ended questions for broad data content followed by thematic analysis recognizing both established and emergent themes in the qualitative data served Mazzola et al. well in meeting the study purpose. The process as described serves as a model for the qualitative portion of the described research study methodology. As with Mazzola et al.'s study, the described study attempted to broaden the themes identified in the research literature addressing a specific research question.

Fay (2011) studied informal communication among co-workers as reported by participants in an online survey. For data collection, Fay designed open-ended questions with structuring information in the content, to elicit participants' memories of specific conversations. The structuring content in the questions derived from prior research on communication modes and themes. For the analysis, Fay used an open coding method based on grounded theory to identify 145 coded units, developing 34 initial categories of communication, further developed into five core themes. The structured information in each of the survey questions established the preliminary themes anticipated in the study design. The open-ended narrative response aspect of the collected data allowed for relevant new themes to emerge during analysis. The use of open-ended questions and cyclic code analysis to develop the five emergent themes supported Fay's study purpose. The structure of Fay's qualitative methodology provides a useful conceptual model for the qualitative analysis methodology in the described study.

Rather than analyzing participants' responses to questions in interviews or surveys, Conaway and Wardrope (2010) used publically accessible annual report letters from corporate

chief executive officers (CEO) for the source data in a study on themes in such communications. The study purpose was to examine cross-cultural comparisons between U.S. and Latin American CEOs in corporate communications. While the topical area of Conway and Wardrope's research is not directly related to the described study's IA focus, the use of thematic analysis can provide an example from research literature of the thematic analysis methodology used. Conway and Wardrope used a grounded theory (Creswell, 2012) basis for analyzing the CEO letters, using an open coding process to identify common themes discovered in the data. With no initial categories to guide the coding, the open coding method allowed Conway and Wardrope to identify emerging themes from the CEO letters. The method worked well in the study, resulting in eight common central themes derived from the data. The use of the open coding method by Conway and Wardrope provides a conceptual model for the discovery and analysis of emergent themes in the described study.

Compliance with Security Guidelines

Work environments include a variety of policies, guidelines, rules, protocols, and procedures specified for workers that are important to the overall work environment and finished product. But the rules may seem peripheral to the immediate task at hand for the workers. Collectively, these rules exist to meet a variety of requirements, enforced by employers, but actually imposed on the workers by employers, customers, unions, regulatory agencies, and governments. The profession of systems engineering has identified many of these external purposes in categories, referred to as *-ilities*, including availability, reliability, supportability, maintainability, environmental, cost-effectiveness, efficiency, safety, health, and security (Haskins, 2011). Common across many of these rules is the reality that workers must voluntarily comply with the stated rules or established procedures; employers cannot assume or expect that

there will be universal compliance with all work rules and prescribed task procedures. Thus, there has been extensive research across several fields regarding aspects of compliance, including theories, frameworks, reasons for compliance, reasons for non-compliance, levels of compliance, and ways to increase compliance. To inform the research described in this dissertation, addressing levels of compliance with information security rules, the literature review examined research in the closely related fields of compliance in security, safety, and health-related activities.

As pointed out by Brostoff and Sasse (2001), compliance with safety guidelines has logical analogs to compliance with security guidelines. Heckle (2011) observed that medical practitioners face daily decisions on whether to comply with security guidelines while providing care to patients. Review of the literature on compliance with both medical safety and medical information security practices provided additional insight into methods to measure compliance among workers. Descriptions of such studies in the medical community follow.

LaRosa et al. (2007) were interested in whether medical staff employed a workaround to avoid having to obtain senior physician approval to prescribe a class of extremely expensive medication, a technique called *stealth dosing*. The study method used was to apply statistical analysis to hospital drug administration records. The use of actual historical data allowed the application of statistical analysis techniques and thus inference within prescribed confidence levels that physicians were engaging in stealth dosing under certain circumstances.

Teer et al. (2007) surveyed undergraduate university students to learn of the students' perceptions about and practices involving computer security. Citing multiple news reports of computer security problems in businesses, Teer et al. described the target population of university students as the next generation of computer users in corporate environments (p. 105).

In a one-page survey, participating students in three specific majors responded to questions on perceptions about computer security and specific practices, such as sharing of passwords. All students at the university had completed a mandatory course in fundamentals of computer security. Teer et al. did not ask the participants for reasons for following or not following security practices.

In a study of a particular category of intentional non-compliance with medical safety protocols, the use of workarounds to specified protocols in the administration of drugs in a hospital, Koppel et al. (2008) gathered extensive information on the staff workarounds. Koppel et al. employed multiple data gathering methods to ensure high validity of the resulting data. Koppel et al. used direct observation of staff on the job, interviews with staff and supervisors, and group discussions in hospital staff meetings, as well as analysis of drug administration record data and participation in a hospital's failure-mode analysis.

In a later hospital-based study, also examining workarounds to medicine administration protocols, Yang et al. (2012) adopted a case study approach. Yang et al. interviewed selected staff to gather data on the use of workarounds in the Electronic Medication Administration System (EMAS). Interview participants included both direct workers and supervisors. Yang et al. also observed staff members during training sessions, to gauge the staff reactions to the EMAS processes, as well on the job in the wards, to see first hand how the staff followed the protocols or implemented workarounds (p. 49).

In contrast to the safety-related studies of EMAS protocol compliance by Koppel et al. (2008) and Yang et al. (2012), Heckle and Lutters (2011) examined information security practice in hospitals. The focus of the study was use of single sign-on (SSO) capability on hospital information systems. Heckle and Lutters used a combination of direct observation, interviews,

and analysis of data system records at a single, large U.S. hospital to accumulate the study data. Conducting the study over the course of the development and fielding of a new SSO system in the hospital, Heckle and Lutters were able to measure employee compliance with the SSO procedures as trained to those employees. As with the cited EMAS studies (Koppel et al., 2008; Yang et al. 2012), Heckle and Lutters observed staff engaging in workarounds as intentional noncompliance with the security protocols for information system access (p. e54).

In a follow-on study to Teer et al. (2007), Kruck and Teer (2008, 2010) examined the computer security practices and perceptions of undergraduate university students across a broad range of study majors, covering 46 majors, compared to the three majors covered in Teer et al. Kruck and Teer used the same one-page survey piloted in the Teer et al. 2007 study. Students in the broader population of the follow-on study had completed the same mandatory computer security training as previously reported (Teer et al. 2007). The survey questions covered attitudes about computer security and specific practices such as password protection. The study did not examine participants' reasons for compliance or non-compliance with computer security training.

Kolkowska and Dhillon (2013) used a data gathering approach similar to that used by Koppel et al. (2008) and LaRosa et al. (2007). Kolkowska and Dhillon combined group interviews of workers and managers with examination of records at a Swedish social services division office. The management of the studied organization had assumed that all necessary security rules were embedded in the provided information system, so there was no explicit security training required. Rather, the employees were expected to comply with proper usage training of the information system (p. 6). The qualitative study examined whether compliance with information security guidelines was related to power relationships in the work environment,

so the information elicited in the interviews focused on reasons for compliance and non-compliance, rather than levels of compliance.

In a study to examine whether cognitive bias affects the perception of levels of compliance with information security guidelines, Rhee et al. (2012) used a survey methodology. Rhee et al. surveyed management information systems (MIS) executives from companies across the United States, asking about perceptions of risk to the executives' companies and levels of employee compliance with information security rules. The MIS executives were, in effect, reporting as third-party observers of workers' levels of compliance. However, the executives' reporting was based on general perceptions, rather than specific events or statistics. Since Rhee et al. asked the MIS executives about general impressions of compliance, and those executives represented a diverse range of organizations, the survey questions were not related to any specific training program.

Conclusion

Examination of the discovered literature on worker compliance with IA policies has demonstrated two gaps in existing published research that the described study will help to close. Human behavior research on general acceptance of technology can be found as early as Davis, et al. (1989). Specific examination of concern for building secure computing technology dates to Gasser (1988), and discussion of humans following IA procedures dates to Adams and Sasse (1999) and Whitten and Tygar (1999). The discovered literature has not addressed the worker population of those working with information systems of the U.S. federal government subject to government IA policies. Further, the literature has not approached the issue of why workers fail to comply with IA policies without assuming a priori some subset of possible environmental,

technological, or human behavioral reasons. No discovered literature approached the question of why system users have not complied with IA policies by simply asking the users.

Across the discovered literature, the dominant defined population studied has been system users associated with universities as students or students and staff (Abraham, 2012; Aytes & Connolly, 2004; Dodge et al., 2007; Jenkins et al., 2012; Johnston & Warkentin, 2010a, 2010b; Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Shaw et al., 2009). Another population type often studied for security practices is composed of healthcare workers (Heckle & Lutters, 2011; Warkentin et al., 2011). In only a limited number of reports were the subject populations from the business environment (Caputo et al., 2014; Eminağaoğlu et al., 2009; Kim, 2010; Puhakainen & Siponen, 2010; Rhee et al., 2012; Shropshire, 2008) or government activities (Kolkowska & Dhillon, 2013). The review of literature uncovered no reports on security practice compliance by system users directly involved with U. S. federal government activities.

Researchers have studied the effectiveness of information assurance practices

- in the general population (Kumaraguru et al., 2010; Mylonas et al., 2013; Sim et al., 2012),
- in selected subsets of the general population (Bulgurcu et al., 2009, 2010; Herath & Rao, 2009a, 2009b), and
- within specifically defined populations (Abraham, 2012; Caputo et al., 2014; Dodge et al., 2007; Eminağaoğlu et al., 2009; Heckle and Lutters, 2011; Jenkins et al., 2012; Johnston & Warkentin, 2010a, 2010b; Jones & Heinrichs, 2012; Kim, 2010; Kolkowska & Dhillon, 2013; Mensch & Wilkie, 2011; Puhakainen & Siponen, 2010; Rhee et al., 2012; Shaw et al., 2009; Shropshire, 2008; Stanton et al., 2005; Warkentin et al., 2011).

Methods used to determine the effectiveness of IA practices included

- audit of actual security events or conditions in an enterprise (Eminağaoğlu et al., 2009; Heckle & Lutters, 2011; LaRosa et al., 2007),
- qualitative assessments by untrained third-party observers (Puhakainen & Siponen, 2010; Rhee et al., 2012; Shropshire, 2008; Stanton et al., 2005),
- measured capability of system users to follow specific security practices (Abraham, 2012; Jenkins et al., 2012; Kim, 2010; Kumaraguru et al., 2009; Sheng et al., 2006; Sim et al., 2012),
- measured intention of system users to follow security practices (Abraham, 2012; Bulgurcu et al., 2009; Herath & Rao, 2009a, 2009b; Johnston & Warkentin, 2010a, 2010b; Kim, P., 2010; Kolskowska & Dhillon, 2013; Mensch & Wilkie, 2011; Mylonas et al., 2013; Shropshire, 2008; Stanton et al., 2005; Warkentin et al., 2011),
- live measurement of system users' compliance with security practices in the enterprise environment (Caputo et al., 2014; Dodge et al., 2007), and
- self-reporting of compliance by system users (Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Mylonas et al., 2013; Stanton et al., 2005).

Studies of compliance with security practice targeted

- generally recommended practices (Bulgurcu et al., 2009, 2010; Herath & Rao, 2009a, 2009b; Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Mylonas et al., 2013; Rhee et al., 2012; Shropshire, 2008; Warkentin et al., 2011),
- custom training used in the study (Abraham, 2012; Jenkins et al., 2012; Johnston & Warkentin, 2010a, 2010b; Kim, 2010; Kumaraguru et al., 2010; Puhakainen &

Siponen, 2010; Shaw et al., 2009; Sim et al., 2012; Stanton et al., 2005), and only in a few cases,

- practices covered in a specifically identified training program already in use by the subjects prior to the study (Caputo et al., 2014; Dodge et al., 2007; Eminağaoğlu et al., 2009; Heckle & Lutters, 2011; Shropshire, 2008).

The described study examined the security practices of a targeted population of users subject to training and requirements specific for the U. S. federal government information systems. The practices examined related directly to the formal training program required of all of those systems users, rather than to general best practices. The study also examined past compliance based on anonymous self-reporting, rather than capability, motivation, or intention to comply in the future. Thus, the described research will add to knowledge in the field by expanding compliance information into a little-studied population, emphasizing actual compliance rates related to specific training. Most significantly, the described study provides a catalog of reasons for user non-compliance with specific IA policies based on the users' own statements, rather than on the researcher's assumptions about any affect of or focus on specific IA system elements.

Summary

Researchers have reported a variety of methods for measuring compliance with established security or safety procedures. Kumaraguru et al. (2010) and Shaw et al. (2009) conducted exercises simulating real world situations, thus measuring the ability to comply with procedures. Caputo et al. (2014) and Dodge et al. (2007) administered covert exercises in the participants' daily environment, effectively masking the fact that the events were research activity rather than actual security events. In four reviewed studies (Puhakainen & Siponen,

2010; Rhee et al., 2012; Shropshire, 2008; Stanton et al., 2005) the researchers relied upon reporting by third party observers, untrained in research methodologies, to assess end-user compliance with procedures. By way of contrast, other researchers (Heckle & Lutters, 2011; Koppel et al., 2008; Yang et al., 2012) used members of the research teams to observe participants' compliance or non-compliance directly. Finally, researchers (Eminağaoğlu et al., 2009; Heckle & Lutters, 2011; LaRosa et al., 2007) analyzed records from the operating environments, assuming final outcomes in the enterprise correlate to general levels of compliance by system users. In all of the reviewed references, researchers selected specific procedures to study. In 18 of 33 reviewed studies the researchers based the selections on implicit or explicit training received by the participants (see Appendix F).

Recognizing a close logical relationship between training and on-the-job compliance, the literature review covered reported research on compliance with specific procedures from three training perspectives. Researchers assumed the participants had been exposed to general information security advice by way of the cultural environment (Bulgurcu et al., 2009, 2010; Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Mylonas et al., 2013; Rhee et al., 2012). Researchers administered training activities integral to the research studies (Kumaraguru et al., 2010; Johnston & Warkentin, 2010a, 2010b; Shaw et al., 2009). Researchers based studies directly on required training participants had previously completed, external to the research activity (Caputo et al., 2014; Dodge et al., 2007; Eminağaoğlu et al., 2009; Heckle & Lutters, 2011). The described study examined compliance with security procedures explicitly identified in mandatory training completed by all participants.

Populations studied in training and compliance literature vary widely from tightly defined groups (Kolkowska & Dhillon, 2013) to a broad range of volunteer participants across the

general population (Kumaraguru et al., 2010). Shropshire (2008) studied the compliance levels of employees of a single financial institution. Kolkowska and Dhillon (2013) studied the employees of a single location of a government activity. Many researchers studied populations associated with institutions of higher learning (Abraham, 2012; Aytes & Connolly, 2004; Dodge et al., 2007; Jenkins et al., 2012, Johnston & Warkentin, 2010a, 2010b; Jones & Heinrichs, 2012; Shaw et al., 2009). The described research targeted a population of working adults who have received specific cyber security training.

A review of the literature describing methods used to measure compliance with security or safety procedures resulted in discovery of several data collection methods available for researchers. Researchers reported using self-reporting (e.g. Jones & Heinrichs, 2012), training exercises (Jenkins et al., 2012), covert exercise (e.g. Caputo et al., 2014), third party observation (e.g. Puhakainen & Siponen, 2010), and researcher observation (e.g. Heckle & Lutters, 2011). See Appendix E for an exposition of the data collection methods across the discovered literature. Based on the review of prior research it is reasonable for the described study to use an anonymous survey of participants in the target population for self-reporting of compliance with prescribed information security practices.

Chapter Three follows presenting detailed discussion of the research methodology followed. The Methodology Chapter addresses appropriateness of the selected methodology for the study purpose, description of the data collection method using an online survey, and the methods for analyzing the collected data. The methodology follows the self-reporting survey process described in multiple studies cited above

CHAPTER 3: METHOD

The purpose of the described study is to determine reasons IA-trained U.S. Federal government workers state for not complying with specific IA policies, using a mixed methods research methodology with an online anonymous survey data collection instrument. The straightforward method to collect data on users' stated reasons for not complying with IA policies is to ask the users. Before asking why an individual had not complied with an IA policy, it was necessary to confirm that the individual had, in fact, not complied with the policy. Thus, a preliminary question must be whether the individual has failed to comply with an IA policy. In order to best inform IA policy decision-makers and IA tools designers, the frequency of non-compliance over time is more meaningful than simply whether participants may have failed to comply only one time. The compliance question for the described study is structured to elicit a statement of frequency as well as compliance. As a mixed methods research design with quantitative and qualitative components (Creswell & Plano Clark, 2011) the data collection sought a statistically significant sample size to allow for meaningful statistical analysis (Fink, 2010; Zafar, 2012). This chapter on method discusses in detail considerations, methodology, and steps for collecting and analyzing the data with respect to the target population, sampling, data collection, and analytical procedures to be used.

Research Method and Design Appropriateness

As stated in Chapter 1, the described study was a concurrent mixed methods study with an embedded design, collecting both quantitative and qualitative data as parallel strands in a single stage (Creswell & Plano Clark, 2011). The purpose of the described study is to determine reasons IA-trained U.S. Federal government workers state for not complying with specific IA policies, using a mixed methods research methodology with an online anonymous survey data

collection instrument. However, the process of confirming that participants have not complied with IA policies, essential to asking for reasons, also elicited useful quantitative data from the population sample. The open-ended questions asking for reasons for non-compliance, the qualitative data, was embedded in a survey with closed-end questions, the quantitative data. Using the notation suggested by Creswell and Plano Clark (2011, p. 109), the described mixed methods research can be summarized as

quan + QUAL = quantified non-compliance with catalog of reasons.

The methodology map procedural diagram in Appendix H, designed following the guidelines of Creswell and Plano Clark (2011, Table 4.1), provides additional detail on the mixed methods study design.

The overall research design for the described study is a cross-sectional survey design, planned to collect data at a single point in time (Creswell, 2012). Creswell described several types of cross-sectional survey designs. The mixed methods study represents aspects of more than one type of cross-sectional survey design. The survey instrument collected information on both actual practices in the quantitative strand and on attitudes or beliefs in the qualitative strand. While the study was designed to compare the practices of two groups, representing users with and without IA job responsibilities, the collected data did not allow such comparison.

The quantitative strand of the described study included both descriptive statistics on the overall responses from the sample, as well as on whether users with IA job responsibilities report different levels and frequencies of IA policy non-compliance than users without IA responsibilities. The researcher was not able to control the proportion of responding participants in either the IA or non-IA groups or whether any given participant is in one group or the other. As a result, the quantitative strand of the described study was a form of observational (Zafar,

2012) or quasi-experimental (Salkind, 2012) research. By way of contrast, the qualitative strand of the described study was non-experimental research (Creswell, 2012; Salkind, 2012).

Creswell (2012, pp. 380-381) listed four key characteristics of survey research: population sampling, use of interviews or questionnaires for data collection, data collection with specifically designed instruments, and obtaining a high response rate. The described study had three of these characteristics. The data was collected from a sample of the population in the form of an online web-based survey using a questionnaire that has been designed specifically for the described study. However, the planned study did not follow Creswell's advice for educational research to seek a high response rate in order to have confidence when generalizing results from the sample to the population. Instead, the research plan was to calculate the goal sample size based on level of confidence and margin of error using standard statistical tools as recommended for scientific research (Zafar, 2012). See the sections on population and sampling frame, below, for further discussion of the sample size.

Research Questions

In the introductory chapter, the basic research question was introduced as, *why have trained users not complied with IA policies, and what proportion of a trained user populations has not complied with IA policies?* This compound question breaks down into several closely related questions:

- R1. Why have users not complied with prescribed IA policies?
- R2. What proportion of the population has failed to comply with prescribed IA policies?
- R3. How often have users failed to comply with prescribed IA policies?

As stated above, the three questions are too broad to study, because the phrase *prescribed IA procedures* does not indicate specifically identified IA policies. However, by inspecting the

content of a broadly required and well-established IA training program, the *Cyber Awareness Challenge* (DISA, 2103), it is possible to identify specific policies for quantifiable study.

Appendix A. IA Training Content provides the complete set of IA policies and guidelines covered in the Cyber Awareness Challenge. The study collected and analyzed data to answer the three generalized research questions for specific IA policies selected from the Cyber Awareness Challenge training materials.

The screen capture images in Appendix A, IA Training Content, show all of the IA policies or guidelines included in the training program, Cyber Awareness Challenge (DISA, 2013). From the full set of IA policies the researcher identified ten specific policies for inclusion in the described study data collection. Selection was based on two criteria for identification of policies for use in the research. First, the wording of the policy statement had to be clearly unambiguous, not subject to questions over interpretation of terminology or context. Second, compliance with the statement had to be binary: actions either comply or not, with no grey area. Here are examples of guidelines in the training not meeting the criteria, each exhibiting ambiguity in the statement:

"Be wary of suspicious e-mails that use your name and/or appear to come from inside your organization or a related organization" (DISA, 2013, Tips About Spear Phishing, Figure A11. *Tips about spear phishing*).

"Don't talk about work outside your workplace, unless it is a specifically designated public meeting environment and is controlled by the event planners" (DISA, 2013, Situational Awareness Tips, Figure A18. *Situational awareness tips*).

"Be alert to and report any suspicious activity or behavior" (DISA, 2013, Challenge Summary Insider Threat, Figure A33. *To protect against the insider threat*).

In the first example, there is no specific action associated with the admonition to *be wary*, and there are no unambiguous guidelines for identifying *suspicious e-mails*. In the second example, the phrasing of *about work* is ambiguous, potentially meaning any topic from duty day report times to specific details of a new budget under development. In the third example, as with *be wary*, the admonition to *be alert to* has no specific related action. In addition, the traits of *suspicious activity or behavior* are not defined. Similarly non-specific or ambiguous guidance statements can be found in other training content in Appendix A.

The researcher identified ten specific policies in the Cyber Awareness Challenge (DISA, 2013) that are basic, straightforward, and for which the question of compliance is easily answered with a simple yes or no. The list is limited to ten total in order to keep the survey short, not overburdening the participants' time in responding. Here are the ten policy rules identified, with the source training content image indicated for each. The policies are grouped into four categories: password related policies, e-mail use policies, data protection policies, and ethical computer use policies.

Password Policies

P1. "Do not use personal information" (DISA, 2013, Th3_P@\$W0rd_Ch@ll3ng3).

From Figure A6. *Password tips, 2*.

P2. "Do not write down your password, memorize it" (DISA, 2013,

Th3_P@\$W0rd_Ch@ll3ng3). From Figure A6. *Password tips, 2*.

E-Mail Policies

P3. "Do not send Chain letters, Jokes, ..., Mass e-mails, Inspirational stories," (DISA, 2013, ETHICAL E_MAIL User Agreement). From Figure A7. *Ethical e-mail user agreement*. and Figure A14. *Summary of security advice for e-mail*.

P4. "Do not access sites by selecting links in e-mails or pop-up messages. Type the address or use bookmarks" (DISA, 2013, To protect against phishing.). From Figure A9.

Tips about phishing: a type of social engineering. To protect against phishing.

Data Protection Policies

P5. "Do not use flash media, unless operationally necessary, owned by your organization, and approved by the appropriate authority in accordance with policy" (DISA, 2013, Use appropriately, if allowed at all.). From Figure A16. *Tips for removable media use.*

P6. "Store sensitive data only on authorized systems. Do not transmit, store, or process sensitive info on non-sensitive systems" (DISA, 2013, Protecting sensitive information tips.). From Figure A26. *Protecting sensitive information.,*

Ethical Computer Use Policies

P7. "Don't view or download pornography" (DISA, 2013, Avoid Computer Misuse.). From Figure A2. *Guidelines for using computer ethically.*

P8. "Don't gamble on the Internet" (DISA, 2013, Avoid Computer Misuse.). From Figure A2. *Guidelines for using computer ethically.*

P9. "Don't conduct private business/money-making ventures" (DISA, 2013, Avoid Computer Misuse.). From Figure A2. *Guidelines for using computer ethically.*

P10. "Don't illegally download copyrighted programs or material" (DISA, 2013, To protect information systems.). From Figure A3. *Tips for peer-to-peer (P2P) and unauthorized software.*

Combining the three general research questions with the ten identified specific IA policies leads to a set of thirty specific research questions for the described study. As discussed in Chapter 1 on study scope, such an extensive set of research questions could be considered

overly ambitious for an initial independent research study. The current study proposal is to select only the two password-related policies for full study, while collecting data on the set of ten for possible future research use. Thus, the described study sought to answer the six research questions, R1₁-3₁ and R1₂-3₂.

R1₁. Why have users *used personal information to select passwords*?

R2₁. What proportion of the population has *used personal information to select passwords*?

R3₁. How often have users *used personal information to select passwords*?

R1₂. Why have users *written down passwords*?

R2₂. What proportion of the population has *written down passwords*?

R3₂. How often have users *written down passwords*?

Variables

The only independent variable to be used in this study was to be whether participants have any assigned IA job responsibilities. The quantitative dependent variables for research questions R2 and R3 was based on the participants' responses to the quantitative questions on frequency of compliance. The response options of *never, rarely, sometimes, very often, or always*, define a verbal frequency scale (Moertl & Scott, 2012) suitable for quantitative analysis.

In the qualitative portion of the study, the dependent variable was the categories or generalized statements of reasons for non-compliance derived by thematic analysis (Creswell & Plano Clark, 2011; Ryan & Bernard, 2003) from the narrative responses in each of the survey questions. The total number of categories cannot be specified a priori. The response data analysis included search for emergent themes (categories) in addition to a baseline set of preliminary categories derived from the systems engineering and IA framework. The collected data may not

reflect identification of all categories in the preliminary set. See the section below on data analysis for further discussion on planning for categorizing the reasons for non-compliance.

Population

There are several groups of people from whom to learn details of behavior with regard to attitude, experience, and decision-making on IA activities. One group is managers who observe the behavior (Shropshire, 2008). Such managers may not be IA professionals but do make decisions on IA requirements and high-level IA policies. Another group is the IA system developers who assume the expected user behavior when deciding what methods and processes to use in design and development sequences as well as in designing the procedures users must follow with the IA systems. The third group encompasses the users (Jones & Heinrichs, 2012; Kruck & Teer, 2008, 2010; Lomo-David & Shannon, 2009), whose behavior is the focus of the question of what users actually do. The described study focused on the third group by asking participants to report on actions in the IA environment and reasons for non-compliant action.

In order to eliminate lack of training as a reason for failing to comply for the specific IA policies used in the survey questions, the target population for the described study was workers who have completed standardized IA awareness training as part of job responsibilities, external to the study. The U.S. federal government has required annual IA awareness training of all workers with access to computer-based information on the job for many years. As described in Chapter 2, U.S. federal government workers represent an under-studied population in the research literature with regard to IA compliance. Further, the IA awareness training program developed by the Department of Defense, the *Cyber Awareness Challenge* (DISA, 2013), has been generalized for use across all departments and agencies. By broadly defining the target population as all adult workers who used U.S. federal government information either in, or for,

the government, the population encompassed several categories of employment as well as a broad range of job specialties.

The employment categories in the population, all found in the defined population, include competitive civil service, excepted civil service, Presidential appointees, uniformed service members, contractors, and consultants. The job specialties in the population range across a broad spectrum from entry-level clerical workers through blue-collar construction and maintenance workers, generalized and specialized white-collar office workers, scientists, engineers, professionals and paraprofessionals in the fields of medicine, law, accounting, finance, law enforcement, and even security forces and combat arms (Office of Personnel Management [OPM], 2009). By design, the study population included only adult workers, defined as those at least 18 years of age, even though there may be workers under 18 in civil service or the uniformed services. Limiting the target population to adults supports proper ethical considerations on human subject research (CITI, 2012).

Sampling Frame

The sampling frame, also called the target population (Creswell, 2012), for the described study was adult workers with access to U.S. federal government information who have completed mandatory annual IA awareness training. The participation announcement and invitation process was via broad distribution of the announcement through multiple channels. The invitation process did not follow the recommendation of Creswell (2012) for educational research to assemble a list of population members and solicit participation from all names on that list. The target population, numbering in the hundreds of thousands, is too large for such an approach. Further, the only demographic questions in the survey asked for confirmation of adult status (over 18), to meet human research ethical considerations; confirmation of membership in

the broadly defined target population, to ensure validity of the study; and whether the participants has IA duties. The web-based survey did not ask for any of the following demographic statistics: age, gender, location, education level, job type, or employer. As a result, it was not possible to design or confirm a stratified sample across the target population for any of the listed demographic measures.

Geographic Location

The study was conducted from the metropolitan Washington, DC, area. However, since the data collection survey was on the Internet with no researcher-established access restrictions, survey participants could potentially be anywhere in the world. Realistically, it is likely that a major proportion of the participating sample was located in the Washington, DC, area for two reasons. First, the use of personal and professional networking by the researcher to solicit participants for the online survey radiated from the researcher's location. Second, the heavy concentration of federal government organizations with headquarters and operating locations across the DC metropolitan area means that the DC area is heavily represented among the target government employees and contractors population. It was not possible to analyze the collected data for geographic locations, due to the minimal demographic information planned for collection, and the assurance to participants that the researcher would not collect Internet Protocol (IP) addresses. As discussed elsewhere, the intent of collecting minimal demographic data from the volunteer participants was to ensure both the perception and actual practice of maximum anonymity and confidentiality of the responses.

Data Collection

Collecting data from multiple people involves using some form of survey (Creswell, 2012; Fink, 2009). Such surveys can be either interviewer-administered or self-administered

(Zafar, 2012). The described study used a self-administered survey for reasons described in more detail below.

Data was collected using an online, web-based survey administration site accessible to the general public. Alternative collection methods considered were paper-based surveys, distributed directly (face-to-face) and by mail; computer document (e.g. word processing file or spreadsheet) surveys distributed by e-mail and web-site download, and submitted by either web-site upload, e-mail, or printing and mailing; and face-to-face interviews, with the interviewer completing the survey form as the participant answers each question. The researcher also considered using a combination of these methods in order to increase overall participation rates among the solicited population by providing a choice of survey formats. The researcher rejected any form of direct personal contact with participants for data collection for several reasons. First, such contact could interfere with the participants' perception of the level of anonymity. Second, face-to-face interaction might reduce the level of truthful responses from participants by introducing a possible intimidation aspect (Creswell, 2012). Third, verbal and non-verbal cues from the interviewing researcher might introduce bias for particular responses, skewing the results (Creswell).

After consultation with experienced research faculty (H. G. Barker, M. G. Gibbs, & J. M. Pittman, personal communication, August 18, 2013), the researcher decided to use only the web-based survey collection method. The web-based survey is the least resource-intensive method among the options considered. Using paper surveys would incur supply and printing costs for the survey forms, as well as mailing costs for distribution of blank forms and submission of completed surveys. Further, compilation of data from the completed forms by manual transcription into computer records would be a time-consuming process, potentially subject to

transcription errors. Use of personal interview would have required extensive time by the researcher, direct access to the target population, and potentially add to concerns by the participants as to the level of anonymity in the survey. Using personal interviews would also have limited the geographic area of the pool of participants. The added convenience participants have by being able to choose the time and place for completing the online survey may have increased the number of population members who volunteered to be part of the study sample group.

Confidentiality, Anonymity, and Participant Trust

Siponen et al. (2010) observed that people do not respond to questions about security policy compliance honestly if afraid an employer could track the respondents of survey answers. Sasse et al. (2001) observed more generally that people say and do different things. Such concern for respondent honesty underlies assumptions and delimitations described in Chapter 1. The study results can only be considered valid if the responses are assumed to be truthful. The respondents can only be assumed to have answered truthfully if it is assumed the respondents trust the assurances of confidentiality and anonymity. The data collection process must be truly anonymous for the researcher to be able to provide participants an assurance of complete confidentiality. Further, the participants must perceive the process as truly anonymous and the data collection as completely confidential to trust the researcher's assurances.

For the data collection instrument used participants were able to observe some of the anonymizing aspects directly. When taking the survey the participants were not asked to sign in or log in to the survey web site. The survey did not ask for any personal identification information such as name, nickname, or e-mail address. The survey did not assign a unique code allowing the participants to pause, leave the site, and return later. The survey did not ask

participants for any of the following demographic data which, in combination, could possibly be used to identify individual respondents: age, gender, education level, employer, location, and job type.

In contrast, the participants were asked to trust the researcher's assurances for other anonymizing aspects of the data collection. The researcher assured participants that the survey has been configured for the data collection at the site not to record and report IP addresses of the participants (SurveyMonkey, 2014). The researcher assured participants that collected data will not be shared, other than with other researchers engaged in approved related research. The researcher assured participants that the collected data would not be stored online once downloaded from the survey web site.

Experienced research scientists may question the decision not to collect traditionally routine demographic data of age, gender, and education level from participants. As described above, the decision was based on providing demonstrable evidence to participants of the true anonymity of the responses. In addition, the researcher suggests that any analysis of the collected responses using such demographic data, while sociologically interesting, would not be useful in any practical manner in applying lessons from the study results to the workplace environment. More specifically, no department, agency, or employer is likely to customize IA policies or training activities based on such demographics. Worker reaction would likely be negative if different sets of IA policies existed for college graduates and non-college graduates. Similarly, announcement of separate IA training programs for males and females would most likely cause questions and protests among the workers, diverting attention from the purpose of the IA training.

Instrumentation

The data collection instrument for the described study was a survey using questions to collect data for both quantitative and qualitative analysis. Since the purpose of the described study is to determine reasons users state for not complying with IA policies, the survey had questions asking participants for such reasons. Initial questions on the survey established the informed consent of the participants when taking the survey. A second set of questions asked demographic information, to be used for two purposes. First, questions on age (18 or over), general employment status (federal employee, uniformed service member, or federal contractor), and completion of IA training were used to confirm participants' eligibility to take the survey and membership in the target population. Second, a question on IA duties was used to identify participants' status with regard to IA knowledge, to be used in planned future studies. The third set of questions was used to gather the quantitative and qualitative data. Each of the ten IA compliance questions begins with the same stem, *As best you recall, within the past two years how often have you ...*, followed by a policy rule statement for a selected IA rule violation, each question derived from a specific IA rule given in the *Cyber Awareness Challenge* (DISA, 2013). See Appendix A for the complete set of IA rules, from which the survey set was selected. The same answer set was provided for each question: a choice from among five frequency statements: *never*, *rarely*, *sometimes*, *very often*, and *always*. Following the quantitative answer set, a follow-up open-ended question asked the participant to briefly explain any reasons for the action violating the stated IA rule.

The set of possible responses are a form of ordinal scale called a verbal frequency scale (Moertl & Scott, 2012), using descriptive words instead of precise numbers for the respondents to select the most appropriate frequency of action. The described study used a Likert-type

response alternative across the verbal frequency scale consisting of the choices, *never, rarely, sometimes, very often, always*, as recommended by Kanusic (2005, p. 123), because the scale is logical, easily understood, and gave the participants a meaningful range from which to select each response. The selected response set is similar to the verbal frequency response set of *never, rarely, occasionally, frequently, all the time*, used by Aytes and Connolly (2004, p. 28). Moertl and Scott prescribed use of a verbal frequency scale when participants are not likely to be able to recall precise values, (p. 76). In addition, using the verbal frequency scale instead of specific numbers avoided inducing an instrumentation bias described by Moertl and Scott as "over-expecting participants' recall ability" (p. 103), which occurs when participants are asked to remember behaviors over an extended period. The study survey asked respondents to recall multiple actions over a two-year period, thus matching the condition that respondents would be unlikely to recall exact numbers. Because the verbal frequency scale includes a true zero value (never) and can be interpreted as having equal intervals across the range from never to always, the scale is a ratio (Creswell, 2012) or rational (Moertl & Scott, 2014) scale. Data from such a rational scale is amenable to quantitative analysis using descriptive statistics (Moertl & Scott, 2014).

The qualitative data were narrative statements from the participants in response to a second paired question for each compliance answer, *If you selected Rarely, Sometimes, Very often, or Always, please briefly explain any reason(s) for your actions*. The response space on the survey web page for each instance of the *why* question was an open field, with no requirements stated for form or format. There was no limit placed on the length of answers. The survey screen presented participants with an answer box sized for 6 lines of 100 characters each, but above each box was the statement, *Type as much as you wish. All of your answer will fit*. See Appendix

B. The respondent was able to type a narrative response as single words, bullet phrases, or complete sentences, without form restriction. The open-ended question as planned is appropriate for qualitative data collection (Creswell, 2012). The resulting narrative data collected from these questions were amenable to thematic analysis (Creswell; Creswell & Plano Clark, 2011; Ryan & Bernard, 2003). The question had no suggested or possible reasons or categories on the page, in order to avoid priming the participants to think along any particular lines in formulating the responses.

Validity and Reliability

The survey used had not been used in previous research. Therefore, it was necessary to establish the validity of the survey prior to soliciting participants for the full study (Fink, 2009). Researchers have used similar surveys to elicit users' self-reporting of IA compliance (Aytes & Connolly, 2004; Jones & Heinrichs, 2012; Kruck & Teer, 2010; Lomo-David & Shannon, 2009; Mensch & Wilkie, 2011; Mylonas et al., 2013; Stanton et al., 2005; Teer et al., 2007). Procedures during the initial stages of the research study established the reliability and validity (Creswell, 2012; Fink; Salkind, 2012) of the survey instrument through use of a pilot study with the instrument.

Survey Reliability

Reliability of the survey was established by administering the survey to a pilot group, prior to administering the survey to participants in the primary target population. Participants in the pilot survey were asked additional questions about the nature and clarity of the questions, as suggested by Pittman (2014a). See Appendix B for the complete survey, including the pilot evaluation questions. The final survey administered for data collection reflected changes in

wording and layout based on feedback from the pilot participants. See Chapter 4 for discussion of the changes.

Content Validity

Content validity of the survey instrument was established by linking each performance question directly to the formal training completed by the participants (DISA, 2013). Active professionals in the IA field, familiar with the general requirements of IA awareness as well as the specifics of the *Cyber Awareness Challenge* (DISA, 2013), reviewed the instrument to confirm the content validity. The researcher did not need to modify the instrument for content based on feedback from the subject matter experts' feedback. See Chapter 4 for discussion.

Internal Validity

Fink (2009), citing Campbell and Stanley (1963), listed seven threats to internal validity. Fink described the following threats to internal validity: selection of participants, history, maturation, testing, instrumentation, statistical regression, and attrition. A discussion follows on how the described research addressed each of those threats to internal validity.

Selection of participants. Selection bias on the part of the researcher may skew the sample characteristics relative to the population (Fink 2009). By using an online survey, broadly advertised, and with no access restrictions, all members of the target population had (theoretically) an opportunity to participate. Realistically, only population members who become aware of the survey, and were motivated to take part, completed the survey as part of the population sample. The open invitation process for participants prevented direct selection bias on the part of the researcher.

History. Events relevant to the survey content may occur during the survey period, potentially changing participants' responses (Fink, 2009). The survey questions asked

participants about past actions and recalled reasons for the actions. The researcher cannot control for external events. However, with the level of detail and the time period specified (two years) in each question, combined with each question asking about actions with reasons and not opinions, the expectation was for history-independent responses.

Maturation. There may be a threat to internal validity caused by the processes of participants maturing physically or emotionally during the data collection process (Fink, 2009). For the described study, all participants were adults, over the age of 18, and in the working environment. Maturation processes as described by Fink were essentially complete among the population. Further, data collection for each individual participant took place in the short time span of completing the survey in a single online session. The sessions were expected to take well under an hour.

Testing. Responses given in an early survey may influence responses given in subsequent related testing (Fink, 2009). For the described research, there were no recurring surveys of participants. Each participant completed the survey only one time, with no expectation of repeated participation. Therefore, the concern over impact of test response memory was not a factor in this study.

Instrumentation. If the instrument or the individual administering the instrument change during the course of conducting the survey, such changes, even slight, may negatively affect the internal validity of the overall data collected (Fink, 2009). For the described study, the planned survey was subject to change only in response to feedback during the pilot study. Once the instrument had been validated with the pilot study, there were no changes to the survey instrument for the period of data collection. Further, since the participants received all instructions from static content web pages on the survey web site, there were no changes in the

process of administering the survey. By holding both the survey instrument and the administration process constant for the entire data collection period, changes in the instrument did not threaten internal validity of the survey instrument in the described study.

Statistical regression. The statistical artifact known as regression to the mean (Zafar, 2012) may impact the internal validity when participants are selected on the basis of extreme scores (Fink, 2009). In the described study, selection of the participants in the population sample was researcher-blind, in that participants self-selected by volunteering to complete the survey. The researcher had no influence in the selection, other than by advertising the study and seeking participants as broadly as possible. See the discussion on advertising the study in the section on sampling frame for details on planned efforts for broad participation among the target population. While the researcher cannot overcome the artifact of regression to the mean completely, the nature of participant recruiting as described was expected to minimize the threat to internal validity.

Attrition. If members of subgroups of the population drop out as participants at different rates before completing the survey or survey sequence, the result may threaten internal validity (Fink, 2009). For the described study, participants were asked to complete the survey only one time, so there was no sequence of surveys. The survey was short, with only three qualifying questions, one demographic question, and ten two-part data collection questions. By providing clear indicators of the estimate of time needed to complete and number of questions remaining to the participants, the researcher expected minimal attrition of participants during the survey, minimizing the threat to internal validity from attrition.

External Validity

As with internal validity, Fink (2009) cited Campbell and Stanley (1963) to describe threats to external validity. Fink observed that external validity could be threatened by the method of participant selection and assignment to groups, and also by taking part in the survey process. For the described study, the former did not apply, because there was no group assignment by the researcher. Affects related to the latter are discussed below.

Interaction effects of selection and treatment. When a program or intervention in a study and a selected population group results in a unique combination relative to the larger population, Fink (2009) suggested a threat to external validity could result. For the described study, there was no intervention or program operating among the sample participants. The survey asked only about past performance and memory. As a result, there was no interaction effect to threaten the external validity of the survey.

Reactive effects of testing. Fink (2009) explained that using a pre-program survey on two groups, only one of which undergoes a program being tested, might sensitize the test group to the program contents, relative to the control group. The reaction of the test group's sensitization to the content of the program could differ from that of the control group. Effectively, differences in post-program performance between the test and control groups would be due to the combination of the survey and program, not to the program alone. In the described study there was no program or intervention with the participants, so reaction to the testing was not a threat to external validity.

Hawthorne effect. Changed patterns of performance caused by the presence of the test environment, which Fink described as the participants reacting to the arrangements of experiment (2009, p. 74) can threaten a study's external validity. The described study did not

involve observation of ongoing behavior, only requesting statements of past performance based on memory. While the survey questions could induce lying, since the responses can involve admission of improper behavior, the researcher expected the careful protection of participant anonymity, discussed in detail elsewhere, to minimize the potential threat to external validity from the experimental arrangements. Further, while the action of completing the survey may have reminded participants of existing IA rules and influence future behavior (noted as a possible benefit of participation), there was no influence on the past behavior being reported.

Multiple program interference. Fink (2009) pointed out that simultaneous participation in more than one program covering the same or overlapping purposes could threaten the external validity of the study testing one of those programs. The described study only asked participants to report on past activities; no ongoing program or activity to change future performance was involved. As a result, there was no threat to external validity from the existence of multiple programs.

Experiment Procedure

The experimental procedure for the described study followed an online survey process. Upon completion of the pilot study and confirmation of the validity of the survey, the web-based survey was made available to the general public. The host domain portion of the URL for the survey remained as that of the web hosting service, surveymonkey.com, and not customized for Capitol College or the researcher for two reasons: First, there was no added cost incurred for a custom domain URL. Second, the potential survey participants were able to recognize the host site company name, and check the reputation of the site for legitimacy. Participants were able to investigate any privacy, safety, or security concerns about using the site by examining the site

documentation (SurveyMonkey 2013a, 2013b). Once the survey site was ready for use, multiple announcements advertised the survey to solicit volunteer participant.

Participant Solicitation

The target population for the study is broad, comprising civilian and military workers in the U.S federal government, as well as government contractors with access to government information or systems. The solicitation of volunteers was across multiple social media networking sites. A standard announcement statement, shown in Appendix C, was sent to the researcher's social media groups as an e-mail or web site posting, requesting both participation and sharing of the announcement with colleagues. The announcement was shared in the following venues, as well as other social media venues that may become available during the data collection phase of the study.

The researcher submitted the volunteer solicitation to the following social media sites.

- LinkedIn:
 - Certified Information Systems Security Professionals (CISSP),
 - USC Institute of Safety and Systems Management (ISSM),
 - INCOSE, the Official Group,
 - INCOSE Washington Metropolitan Area Chapter (INCOSE-WMA),
 - Certification and Accreditation (C&A) Discussion Group,
 - Security through Intelligence,
 - Centenary College of Louisiana Alumni Association,
 - Information Systems Security Association (ISSA) Discussion Group,
 - Information Systems Security Association - Northern Virginia Chapter,
 - Securing the Weakest Link: Changing User Behavior One Click at a Time,

- The Official USC Alumni Association Group;
- TKE Alumni.
- Yahoo! Groups:
 - Official (ISC)2 CISSP Forum,
 - USHPA/USHGA Region 6/11 HG/PG Pilots.
- Independent site forums:
 - OZ Report Forum,
 - CHGPA Forum,
 - HangGliding.org.

Population Sampling

The data collection process depended on participation of volunteers across a widely defined population. The process of broadly soliciting the volunteers while providing maximum possible anonymity precluded using incentives to induce participation. As a result, the study plan could not guaranty a specific sample size for the data analysis. The final report of study results in Chapter 4 includes a discussion of the confidence level in the statistical analysis, based on the actual sample size.

The formula to determine the minimum sample size n needed from a very large population to estimate an interval of a population proportion (Zafar, 2012) or for categorical data (Cochran, 1977) is

$$n = pq \left(\frac{Z}{E} \right)^2$$

where

p = sample proportion, estimated

$q = 1 - p$

Z = the Z value for the selected confidence level

E = margin of error (or confidence interval)

Using a goal margin of error of 10%, and target levels of confidence of 90% and 95%, the above formula provides the sample sizes shown in Table 3. Since the actual proportion of the population is not known, the more conservative value of 0.5 for the sample proportion is used, maximizing the resulting sample size calculation.³

Table 1.

Sample Sizes at Two Levels of Confidence and Margins of Error, $p=0.5$

| E , Margin of Error | 0.1 | | .05 | |
|-------------------------------|-------|-------|--------|--------|
| | 90% | 95% | 90% | 95% |
| CL, Confidence Level | | | | |
| Z value | 1.645 | 1.96 | 1.645 | 1.96 |
| n , Sample size, calculated | 67.65 | 96.04 | 270.60 | 384.16 |
| n , rounded up | 68 | 97 | 271 | 385 |

The above formula to determine sample size is for a large sample. It is necessary to confirm the decision not to adjust the sample size based on population. Bartlett, Kotrlík, and Higgins (2001) showed how to use Cochran's (1977) correction formula, necessary when a sample exceeds 5% of the population. The target population for the described study numbers in the hundreds of thousands. The worker population of DISA, only one agency of the DoD, is approximately 14,000 (DISA, 2010). Considering only the DISA agency size, 5% of the population would be 700; the a priori sample sizes above are far below the 5% threshold. The target population is large enough that it is not necessary to adjust the sample size for a small population.

³ With p estimated as 0.5, $p*q = p*(1-p) = 0.25$. Any other value of p , higher or lower, results in a smaller factor, reducing the minimum sample size. For $p = 0.4$, the multiplier is 0.24; for $p = 0.7$, the multiplier becomes 0.21.

To illustrate, Cochran's correction formula (1977), is

$$N = \frac{n}{1 + \frac{n}{Pop}}$$

Where

n = calculated sample size

N = adjusted sample size

Pop - population size

Table 2.

Demonstration of Lack of Effect of Adjusting for Population

| <i>E</i> , Margin of Error | <i>.1</i> | | <i>.05</i> | |
|---|-----------|-------|------------|--------|
| | 90% | 95% | 90% | 95% |
| CL, Confidence Level | | | | |
| <i>n</i> , Sample size, calculated | 67.65 | 96.04 | 270.60 | 384.16 |
| <i>N</i> , adjusted <i>Pop</i> = 14,000 | 67.32 | 95.38 | 265/47 | 373.90 |
| <i>N</i> , adjusted <i>Pop</i> = 100,00 | 67.60 | 95.94 | 269.87 | 382.69 |

Table 1.

Sample Sizes at Two Levels of Confidence, displays the values used to calculate the lower and upper goal sample sizes, with the values used in the calculation. The table demonstrates the potential impact of adjusting the size for two population sizes, 14,000 and 100,000. The unadjusted sample size, n , is either equal to or more conservative than an adjusted sample size, N . The table also demonstrates the impact of choosing a more rigorous margin of error of 5% instead of 10%. Using the smaller margin of error would mandate samples over three times larger for both selected confidence levels: 271 compared to 68 for 90% CL, and 385 compared to 97 for 95% CL. The selection of 10% for the study margin of error was based on practical consideration of the sampling process. It was not possible to guarantee the total number of participants in advance. Therefore, to limit the total time for data collection, consonant with the academic schedule, while seeking a statistically significant result with acceptable values of E and

CL, the higher $E = 10\%$ was selected. The use of the resulting sample size numbers in data collection timing is described next.

The survey was planned to remain open for viewing and volunteer submissions until one of three alternative conditions had been met, based on a combination of elapsed time and number of completed surveys. The total planned time limit for the open survey period was three months, chosen in order to meet the academic schedule of the research phase in the degree program. However, the actual survey period was planned for the possibility of being shorter, depending on the number of completed surveys submitted by eligible volunteer participants. The researcher planned to close the survey period upon one of the following situations.

1. Less than three months had elapsed and at least 97 participants in each of the two differentiated sub groups (IA duties and no IA duties) had submitted completed surveys, providing the preferred higher level of confidence of 95% for results.
2. Two to three months had elapsed and at least 68 participants in each of the two differentiated sub groups (IA duties and no IA duties) had submitted completed surveys, providing the lower target level of confidence of 90% for results.
3. Three months has elapsed, without regard to the number of participants. In this case, the study results would report on the level of confidence calculated from the number of participants.

The target participation numbers of 68 and 97 in the criteria above derive from calculations of sample size (Zafar, 2012) for confidence levels selected at minimum (90%) and preferred (95%) levels for the described study, with a margin of error of 10%. Because the researcher had no ability to direct, mandate, or incentivize participation levels across the target population, the data collection plan had to allow for the possibility of low participation rate.

Therefore, the data collection plan included a firm limit of three months, selected based on the academic schedule requirements of the researcher and degree program. Were it necessary to complete the study with less than the stated minimum participation level, the qualitative analysis of the collected responses to answer research questions 1, stated reasons for non-compliance, would remain valid and informative to the literature. The quantitative analysis addressing questions 2 and 3, however, would possibly be of low confidence.

Due to unexpected results with regard to the distribution of responses between the two sub groups the researcher modified the data collection plan during the data collection period. The comparison of results between the sub groups was eliminated from the study plan, and the survey closed at six weeks with 103 usable responses from the target population. See the discussion on data collection in Chapter 4 for a complete explanation of the basis for the shift in the data plan.

Data Analysis

Data collected for the described study was in two forms, quantitative data from the level of compliance questions, and qualitative data from the narrative responses to the question *why*. In a mixed methods study, each data type requires use of different analysis methods (Creswell & Plano Clark, 2011). The following sections describe the analytical steps for each data set. Quantitative analysis followed standard statistical methods for descriptive statistics (Moertl & Scott, 2014; Zafar, 2012). Analysis of the narrative responses as qualitative data followed the general steps of qualitative analysis (Creswell, 2012; Creswell & Plano Clark) for thematic analysis (Ryan & Bernard, 2003) using a coding process (Bornmann, 2014a, 2014b). Although the primary purpose of the described research was to learn the reasons for IA policy non-compliance, derived from the qualitative data, the sections below follow the order of question asked of participants, addressing the quantitative analysis, followed by the qualitative analysis.

Response Analysis

The data collection portion of the survey consisted of ten two-part questions, each question asking about level of compliance with a specific IA rule, and reasons for non-compliance. Participants were not required to answer every question. The results report includes the percentage of respondents answering each of the data collection questions. Only the data from questions 1 and 2 were used for full analysis in the described study.

Data from the remaining eight questions will be available for future study. Any observed patterns in the response rate for the individual questions question groups may suggest future research opportunities. For the qualitative questions, the question was considered as answered if the paired quantitative answer is *never* or if any text is found. If the paired quantitative answer is other than *never* but the reply is blank, the question was counted as not answered.

Table 3.

Response Rate for Individual Questions (Example)

| Question | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|--------------|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Policy Group | | P | P | eM | eM | D | D | U | U | U | U |
| Quantitative | | | | | | | | | | | |
| Total | ## | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% |
| Non-IA | NN | N% | N% | N% | N% | N% | N% | N% | N% | N% | N% |
| IA duties | nn | n% | n% | n% | n% | n% | n% | n% | n% | n% | n% |
| Qualitative | | | | | | | | | | | |
| Total | ## | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% | ##% |
| Non-IA | NN | N% | N% | N% | N% | N% | N% | N% | N% | N% | N% |
| IA duties | nn | n% | n% | n% | n% | n% | n% | n% | n% | n% | n% |

Note. Question Policy Groups: **P**assword, **eM**ail, **D**ata protection, ethical computer **U**se

Quantitative Analysis

Descriptive statistics. In order to answer research question R2 for each of the selected IA policies, it was necessary to recast the frequency distribution data as collected into a binary format. For each R2_n, the research question asks *what proportion of the population* have not

complied with an IA policy, without regard to the frequency of non-compliant action. The analysis compared the number of participants who have complied with the number who have not complied. Thus, the responses for each of the survey questions were grouped to compare proportion of responses of *never* with the sum of responses of *rarely*, *sometimes*, *very often*, and *always*. For each of the selected policies the data would show that $x\%$ of the population has failed to comply with the policy within the past two years.

Research question R3 asks the broader question of *how often* have users not complied with each selected IA policy. The data collected in the five-choice verbal frequency scale provided an understanding of the replies by comparing results for all five possible responses. Kanusic (2005) described the verbal frequency scale selected for the described study as *Likert-type* (p. 123). Moertl and Scott (2012) advised analyzing verbal frequency scale data similarly to Likert scale procedures. Pittman (2014b) noted that researchers have treated Likert scale data as either ordinal (numeric) or nominal data types. The verbal frequency scale to be used in the data collection instrument is a ratio (Creswell, 2012) or rational (Moertl & Scott, 2014) scale, with a true zero (*never*) and equal intervals along the scale. As such, the data were subject to statistical analysis, in keeping with the characterization by Kanusic and the advice by Moertl and Scott (2012).

Following the advice of both Kanusic (2005) and Moertl and Scott (2012), collected data for each of the compliance questions were presented in both tabular and graphic format for initial understanding and analysis. Data presentation used both actual count and percent of total for the number of responses from the sample for each of the five possible answers. The original study plan called for data to be displayed for both the total sample responses, and segregated numbers for the demographic selection of users without and with IA job responsibilities. The numeric data

displayed in each table were to be displayed in a pair of bar charts: The first chart as a frequency distribution stacked bar chart for each answer set, providing a simple visual display of the frequency of compliance across the entire study sample. The second bar chart was to be display the same data, but with the paired data side-by-side, rather than stacked, to provide a clearer visualization of the differences between the IA and non-IA participants' responses. Below are examples of the tables and charts planned for the analysis. As discussed in Chapter 4, the required change in data use resulted in final tables and graphics without the sub-group comparisons. Values shown in this Chapter 3 on research method are for illustration only, with no meaning or expectation of the study results.

In order to derive descriptive statistics from the collected verbal frequency scale data, treating the data similarly to interval scale data (Moertl & Scott, 2014), the responses must be represented as numbers. Converting the response terms into effective percentage of occurrences, with the endpoints of 0% of the time (never) and 100% of the time (always), and assuming equal intervals, the five responses across the scale become 0% (never), 25% (rarely), 50% (sometimes), 75% (very often), and 100% (always). Using the values indicated, the distribution of responses was described by calculating the mean and standard deviation of the sample (Zafar, 2012). Tables follow with example data and calculated mean and standard deviation of the sample. The standard deviation for each distribution was calculated using the formula for standard deviation of a sample (Hamburg, 1987):

$$s = \sqrt{\frac{\sum_1^n (x - \bar{x})^2}{n-1}}$$

The tables and charts that follow represent the original research plan to compare results for the sub groups of the target population with and without IA duties. As explained in Chapter 4 the final collected data did not allow for such a comparison. As a result, the data displays in

Chapter 4 represent the analysis of the sample for the target population without sub group differentiation. The tables and charts presented here in Chapter 3 remain as originally proposed, to allowing use of the examples for possible future research studies suggested in Chapter 5..

Table 4.

Compliance Frequency Responses (Example)

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | Total | Mean | StdDev |
|-----------------|-------|--------|-----------|------------|--------|-------|-------|--------|
| % of Time | 0% | 25% | 50% | 75% | 100% | | | |
| Non-IA Duties | 24 | 33 | 65 | 18 | 1 | 141 | 39.2% | 23.6% |
| IA Duties | 33 | 35 | 40 | 10 | 0 | 118 | 30.7% | 23.9% |
| Total responses | 57 | 68 | 105 | 28 | 1 | 259 | 35.3% | 24.1% |

Table 5.

Compliance Frequency Responses by Percentage (Example)

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | Total |
|-----------------|-------|--------|-----------|------------|--------|-------|
| % of Time | 0% | 25% | 50% | 75% | 100% | |
| Non-IA Duties | 17% | 23% | 46% | 13% | 1% | 100% |
| IA Duties | 28% | 30% | 34% | 8% | 0% | 100% |
| Total responses | 22% | 26% | 41% | 11% | 0% | 100% |

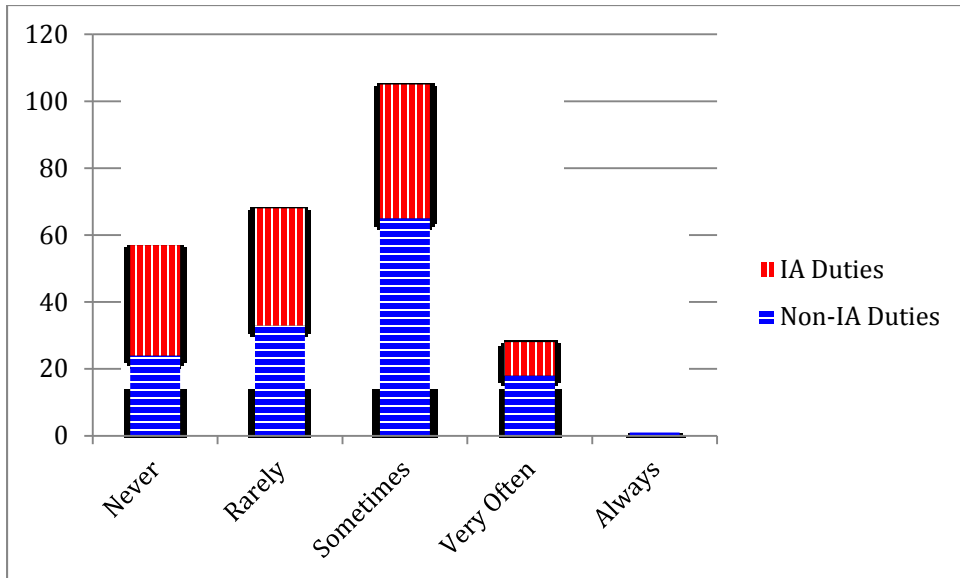


Figure 1. Compliance frequency distribution (example) highlighting the frequency distribution across the entire sample with proportionate contributions of each sub-group (with and without IA duties) visible.

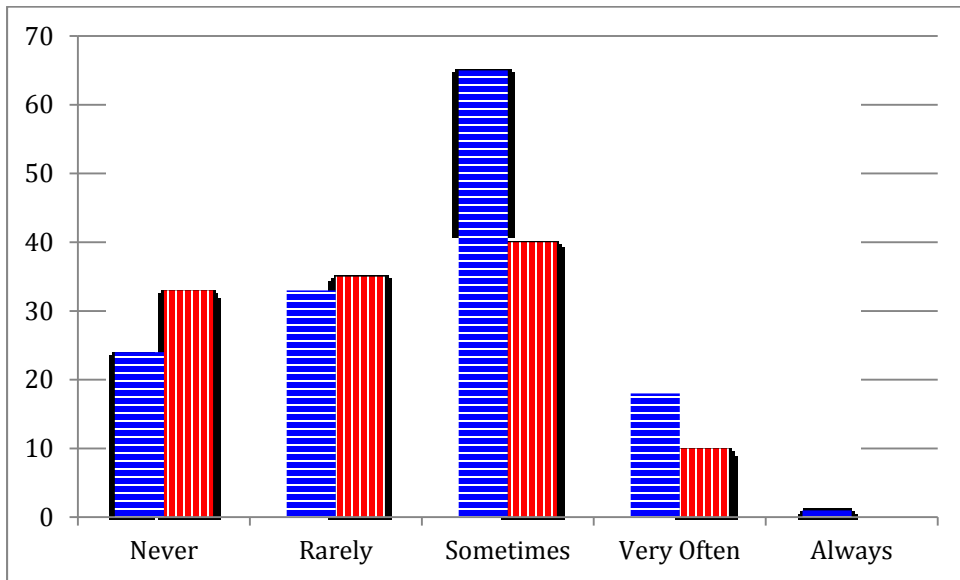


Figure 2. Compliance frequency distribution (example) highlighting the comparison of distribution curves of the two subgroups, with and without IA duties.

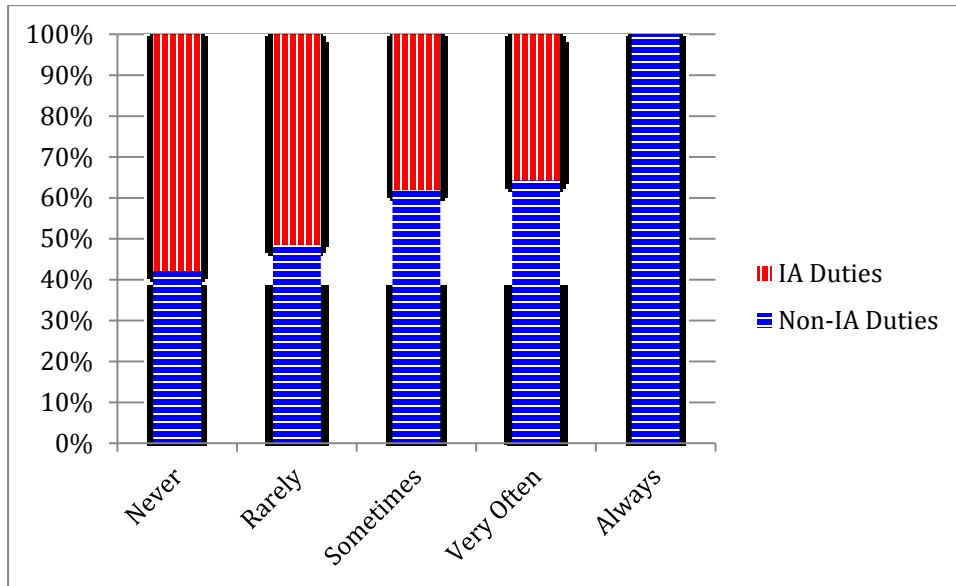


Figure 3. Compliance frequency distribution (example) illustrating the proportion of IA and non-IA subgroups at each declared frequency level.

Within the context of the research questions, there are two possible ways to interpret the data. A basic approach is to consider how often all members of the sample have violated the policy. An alternate way to consider the same data is to examine how often only those who have violated the policy do so. Examining the values for the standard deviation of the sample provides a more complete picture of the amount of time users have not complied with the policy. Tables in the format of *Table 6*.

Mean Amount of Time Users Do Not Comply (using the example data from above) allow direct comparison of the means and standard deviations for each studied subgroup using both alternatives.

Table 6.
Mean Amount of Time Users Do Not Comply

| Survey Response | Entire Sample | | Non-Compliant Users | | Proportion of Sample Who Did Not Comply |
|-----------------|---------------|--------|---------------------|--------|---|
| | Mean | StdDev | Mean | StdDev | |
| Non-IA Duties | 39.2% | 23.6% | 47.2% | 24.3% | 83% |
| IA Duties | 30.7% | 23.9% | 42.6% | 21.6% | 72% |
| Total responses | 35.3% | 24.1% | 45.3% | 23.3% | 78% |

Qualitative Analysis

The analysis of the qualitative narrative data from each of the questions identified common themes across the reasons given by the participants. The analysis procedures followed steps described in Creswell and Plano Clark (2011, Table 7.1). The researcher used a table structure from the original data set in spreadsheet format as downloaded from the SurveyMonkey.com site, supplemented with coding columns for initial and derived thematic coding, to conduct the thematic analysis.

Table 7.
Planned Steps in Qualitative Analysis Process.

| | Step | Actions |
|---|------------------------|---|
| 1 | Prepare the data | Transfer data from survey site report to analytical program |
| 2 | Explore | Read the narratives for themes. Set up a qualitative codebook |
| 3 | Analyze | Code data with labels. Group codes into categories. Review and relate categories, restructuring to a smaller, more abstracted category set if appropriate |
| 4 | Represent the analysis | Describe the set of categories and individual categories in discussion Develop figures for visual representation of the categories |
| 5 | Interpret | Evaluate data relative to the research questions. Compare with literature |
| 6 | Validate | Validate against researcher and reviewer standards. Check reliability [procedure not yet identified] |

Note. Derived from Creswell and Plano Clark (2011), Table 7.1, Recommended Quantitative and Qualitative Data Analysis Procedures for Designing Mixed Methods Studies.

The process of identifying common themes across the narrative data responses followed the procedures detailed by Ryan and Bernard (2003). The process used an a priori list of categories, while also analyzing for additional emergent categories. See *Table 8*.

Themes of Non-Compliance Reasons, a priori for the initial list of themes, annotated with related prior research, when relevant, and aligned with one or more components of the three research frameworks of SE, IA, and human performance described in Chapter 1.

Table 8.
Themes of Non-Compliance Reasons, a priori

| Theme ID | Theme (Category) | SE Major Element (Haskins, 2011) | IA Information Attribute (Parker, 1998, 2002) | Human Performance Theory (Abraham, 2012) |
|----------|--|----------------------------------|---|--|
| 1 | Negative Motivation | People | | Deterrence theory |
| 2 | Positive Motivation | People | | Protection motivation theory |
| 3 | Training | People | | Social cognitive theory |
| 4 | Self-efficacy | People | | |
| 5 | IA policy conflicts with work process | Process | Usability | Rational choice theory |
| 6 | IA tool not accessible in work environment | Tools | Availability | |
| 7 | Tool too difficult to use | Tools | Usability | |
| 8 | Never learned how to use tool (training) | People | Usability | |
| 9 | Process too difficult to follow | Process | Usability | Social cognitive theory |
| 10 | Rule makes no sense | Process | | Technology acceptance model |

Summary

The described study methodology was designed to collect data that would provide answers to the three base research questions, applied to two specific IA policies. Using a mixed methods research design (Creswell & Plano Clark, 2011), the study method supported answering both *what did participants do* and *why did participants do it* research questions. Looking forward to possible future studies, the data collection covered a total of ten IA policies, each derived directly from a specific IA training program (DISA, 2013), aimed at the defined target population.

The data collection instrument and planned analysis process incorporated considerations to ensure internal and external validity (Creswell, 2012; Fink, 2009) of the instrument and the study. The validation process for the instrument included a pilot study prior to the full data collection phase of the research. The pilot study procedures assured validity of the content of the survey instrument, as well as reliability of the overall survey instrument in context (Creswell, 2012).

Chapter 4, Results, follows this chapter on Methodology. The Results chapter displays the statistical charts and tables for the quantitative data, as illustrated above. The chapter also presents the thematic data derived from the qualitative responses to the *why* questions. Throughout the cited literature and this proposal acronyms have been used extensively. Appendix I lists acronyms used in the proposal. For ease of quick reference by readers, the appendix of acronyms is the final appendix in the document.

CHAPTER 4: RESULTS

Once the Institutional Review Board (IRB) had approved the proposed research the researcher began active study. Content validation took place in a one-week period using direct correspondence via e-mail between the researcher and the recruited subject matter experts. Over the following week the researcher conducted a pilot study (Fink, 2009) of the planned data collection instrument on the commercial online survey service SurveyMonkey.com. The researcher changed wording in the data collection survey introduction and selected questions based on pilot participant feedback, initiating full data collection on SurveyMonkey in the third week of the study. For four weeks the researcher monitored survey completion statistics once a week, without inspecting detailed response survey data to confirm how many completed surveys represented usable surveys for the study.

At the end of the fourth week the researcher began inspecting details of the accumulated response data and noted an unexpected result in the one question on participant IA duties. An observed deviation from the expected ratio of IA and non-IA duties for respondents continued into the fifth and sixth weeks. After consultation with and approval of the supervising chair and committee (Van Horn, personal communication, October 27, 2014), and the program dean and the IRB chair (Barker & Maconachy, personal communication, October 31, 2014), the researcher modified the original data collection plan, closing the survey at the end of the sixth week. The Data Plan Modification section of Findings in this Results chapter (pp. 109-110) provides details on the changes in the data collection schedule and data analysis plan.

The remainder of this chapter describes the details of the instrument validation, the pilot study, the data collection process, including the modification to the collection and analysis plan, and an overview of the collected data. The chapter content continues with an exposition of the

quantitative analysis of the collected data, in accordance with the plan shown in the Quantitative Analysis section (Chapter 3, pp. 95-100) except as noted. Finally, the chapter presents the results of the qualitative thematic analysis (Ryan & Bernard, 2003) of the collected data in accordance with the Qualitative Analysis section (Chapter 3, pp. 100-102).

Pilot Study

Content Validation

The pilot study began on September 3, 2014, with the content validation phase of the pilot lasting one week. Five professionals in the field of information assurance reviewed the survey questions. One content reviewer suggested that some participants might not be completely familiar with the meaning of personal identifying information (PII). Another suggested that questions on ethical computer use might not be aspects of information assurance. Otherwise all acknowledged that the question content reflected accurate IA information. The researcher decided to leave the subject questions unchanged, since the wording of each had been extracted directly from the source training materials (DISA, 2013).

Survey Validation

Phase two of the pilot study began on September 10 with 12 participants invited to take the pilot survey online. The pilot study was closed to further responses on September 19, with 9 of the 12 invited participants having submitted comments. Since the pilot survey used the same anonymity protection as the full survey, it was not possible to determine which invited individuals had not completed the pilot.

Feedback from the participants indicated using from 10 to 20 minutes to complete the survey, with one response of "20 to 30 minutes." Using the reported times, the introduction page of the survey was edited to include the statement, "It should take you less than 20 minutes to

complete the survey." Responses for the open comment questions for pilot participants gave added insight into participants' perceptions. However, the researcher changed the final survey based on only some of the comments.

Several comments indicated that the introductory information was too long. One participant acknowledged that the length might be necessary. The introductory information stayed as originally composed to avoid any interference with the essential informed consent requirements for the study. Other comments indicated surprise at the open narrative questions following the quantitative questions. The preliminary description of the survey was modified to more clearly inform survey participants what to expect once beginning the questions. Other comments influenced a change in the structure of the quantitative question stem from "Within the past two years, how often have you ..." to "As best you recall, within the past two years how often have you..." Several pilot participants provided suggestions to eliminate the negative wording of the standard qualitative question asking for reasons for not following policies. The final survey form followed that advice.

One pilot participant provided a comment that would later prove to be more significant than the researcher initially realized. Regarding the survey question "Do your assigned work duties include responsibility in any area of computer security..." the pilot participant stated, "Need to clarify whether this includes regular non-security staff. The official line in most agencies is that 'security is everyone's responsibility', which might include clerical or janitorial staff if taken too literally." The intent of the question was to distinguish between workers with specific IA duties and those with only general security responsibility. For the Defense Department such a distinction is made in a requirement for members of the workforce in the former group to hold specific IA certifications (DoD, 2007). Since other departments and

agencies do not have a similar distinction the question was left unchanged for the published survey. It would not have been appropriate to refer to the DOD Directive 8570.01 (DoD, 2007) in a survey designed for all federal workers. See the section on data collection, below, for further discussion. See Appendix B for the complete survey as executed on SurveyMonkey.com.

Data Collection

Participant Solicitation

The survey opened for data collection on September 19, 2014. The researcher submitted the request for volunteers shown in Appendix C to the social media affinity groups listed in Chapter 3: 12 LinkedIn groups, 2 Yahoo groups, and 3 independent sport hobby forum websites. The affinity groups were chosen based on the researcher's ongoing membership with each group, the moderate to large membership of each, and the expectation that some members of each group either are or know members of the target population of U.S. federal government workers. The alumni and sport hobby groups were included to help broaden the solicitation beyond the researcher's IA professional group affiliations. The moderator of one LinkedIn group never approved the announcement for posting to the community. *Table 9* shows the total membership of each of the 16 groups that saw the announcement. The numbers are not additive due to overlapping membership across multiple groups. In addition, there is no way of determining how many members of each group read the announcement or weekly reminders during the time the survey was open for participants.

Table 9.

Affinity Group Membership Levels

| Group | Membership | Group | Membership |
|-----------------|------------|--------------|------------|
| CISSP, LI | 23,139 | CISSP, Yahoo | 5,758 |
| ISSA | 28,691 | ISSA-NOVA | 662 |
| C&A | 1,363 | Weakest Link | 349 |
| INCOSE | 764 | INCOSE-WMA | 663 |
| USC | 41,643 | USC ISSM | 602 |
| Centenary | 780 | TKE Alumni | 3,525 |
| HangGliding.org | 11,067 | OzReport.com | 4,920 |
| Region 6 HG | 511 | CHGPA.com | 484 |

Participation Timing

After the initial survey announcement on Friday, September 19, the daily rate of survey completion fell off to nearly 0 after about four days. The researcher began posting short weekly reminder notes referring to the original announcement on each affinity group, varying from late Friday to very early Monday. Appendix C, Survey Participant Participation, includes the content of each of the weekly reminders. Each reminder resulted in a number of new survey completions for about three days. Table 10.

Number of Submitted Surveys by Week displays the dates of the announcements and total survey counts reported by SurveyMonkey as of each Monday.

Table 10.

Number of Submitted Surveys by Week

| Announcements | Counts as of | New | Total | Eligible |
|---------------|--------------|-----|-------|----------|
| 9/19/2014 | 9/22/2014 | 9 | 9 | |
| 9/28/2014 | 9/29/2014 | 13 | 22 | |
| 10/6/2014 | 10/6/2014 | 43 | 65 | |
| 10/13/2014 | 10/13/2014 | 46 | 111 | |
| 10/18/2014 | 10/20/2014 | 38 | 149 | 88 |
| 10/26/2104 | 10/27/2014 | 21 | 170 | 99 |
| 10/31/2014 | 10/31/2014 | 8 | 178 | 103 |

Findings

Data Plan Modification

Preliminary data analysis after one month caused the researcher to modify the original data plan for the study. During the first four weeks of data collection the researcher monitored only the total number of surveys submitted, without examining the detailed data. On October 18 the collected data showed that only 88 of the submitted surveys represented members of the target population. The remainder had been disqualified by responding that they were not employed as a federal worker, contractor, or military. Further, 78 of the usable surveys indicated having IA duties, and only 10 indicated no IA duties. By October 26 there were 99 usable surveys, 89 with IA duties and still only 10 without. The unexpected imbalance of IA and non-IA participants caused a re-evaluation of the data plan.

The fall off of weekly participation from 46 to 38 to 21 indicated it was very unlikely that a statistically significant number of non-IA participants would be seen, even if the survey were left open the full 90 days as originally planned. In addition, the unexpected imbalance between sub-groups brought to mind the pilot participant comment, quoted above in the Survey Validation section (p. 106), suggesting that prior training on responsibility for security would cause many workers to claim IA duties. The researcher decided to eliminate the planned comparison of IA and non-IA workers, using the collected data as a single undifferentiated sample from the target population. The change in interpretation of the IA duties question required statement of a new assumption, not originally included in the Assumptions section (pp. 23-24) of Chapter 1:

Assumption 5: Federal workers trained in IA responsibilities and rules may consider themselves to have general IA duties, even without specific assigned IA duties.

By eliminating the IA and non-IA subgroups from the data plan, and treating the entire data set as a single undifferentiated sample from the target population, the use of the data collection rules presented in Chapter 3 changed. The calculation in Population Sampling section (pp. 89-92) of Chapter 3 demonstrated that for a very large population a sample of at least 97 provides a 95% confidence level with a margin of error of 0.1. The researcher applied a modified survey closure criteria 1 (p. 92) from Chapter 3, calling for closing the data collection when at least 97 surveys had been submitted, providing the desired 95% confidence level for the statistical analysis. Therefore, the survey was closed and data collection ended on Friday, October 31, six weeks after the initial September 19 announcement, with 103 usable survey responses out of a total of 178 survey participants.

Sample Size

Of the 178 survey participants, only 105 indicated that they were members of the target population, at least 18 years old and working with U.S. Federal government information as civil service, uniformed service, or contractors. Two surveys of the 105 were discarded, leaving a valid sample of 103 responses. One of the otherwise qualified workers left the informed consent agreement question unanswered. The other discarded survey showed that the respondent had not completed required IA training within two years. Of the 103 surveys indicating respondents were part of the target population and consenting to participate, 4 answered none of the data collection questions. The resulting sample size for the survey consisted of 99 surveys with at least one data collection question answered.

Response Rate

The survey instrument did not require participants to respond on any question. *Table 11* below shows the rate of participation among participants for the 20 data collection questions. As

stated in the Scope and Scale section (pp. 25-26) of Chapter 1, the results presented in the remainder of this paper address only the data from the four password-related questions. Data from the questions related to e-mail use, data protection, and ethical computer use will be available for analysis in future studies.

Table 11.

Response Rate for Each Data Collection Question for Entire Survey

| Question | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|--------------|----|-----|------|-----|-----|-----|-----|-----|-----|-----|-----|
| Policy Group | P | P | eM | eM | D | D | U | U | U | U | |
| Quantitative | | | | | | | | | | | |
| Total | 99 | 99% | 100% | 99% | 98% | 97% | 97% | 97% | 97% | 96% | 96% |
| Qualitative | | | | | | | | | | | |
| Total | 99 | 26% | 60% | 17% | 20% | 29% | 15% | 7% | 6% | 9% | 8% |

Note. Question Policy Groups: **P**assword, **eM**ail, **D**ata protection, ethical computer **U**se

Quantitative Results

The Quantitative Analysis section (pp. 95-100) of Chapter 3 presented the structure of data analysis as originally planned. The discussion below in this Quantitative Results section presents the use of the plan as changed in accordance with the Data Plan Modification section (pp. 109-110) above. As described in the Descriptive Statistics section of Chapter 3 (pp. 95-97) the responses available in each survey question asking *how often have you...?* define a verbal frequency scale that is also rational scale with a defined zero and equal intervals between values (Moertl & Scott, 2012, 2014). In the case of the study survey questions, not only does the response selection of *Never* define a zero point, but also the selection of *Always* defines a value of 100%. Using the understanding of equal intervals across the scale from 0 to 100%, responses of *Rarely*, *Sometimes*, and *Very often* are transformed into values of 25%, 50%, and 75%. This transformation of verbal statements of frequency, even fully understanding that a participant

selecting *Sometimes* was not indicating an answer of *precisely half the time*, allowed calculation of means and standard deviations of the sample based on the collected data. Values in the tables shown for standard deviation, represented as StdDev, are standard deviation of the sample (Hamburg, 1987). As advised by Kanusic (2005) and Moertl and Scott (2012), the data presentation below is in both tabular and graphical format.

Password Composition

The first quantitative data collection question asked participants how often they have violated the trained guidance "Do not use personal information" (DISA, 2013, Th3_P@\$W0rd_Ch@ll3ng3): **7. As best as you recall, within the past two years how often have you created any computer system or account passwords using personal information?** Of the 99 completed surveys, 98 responded to the question. Figure 4 below displays the source page from the training program for both this and the next password question in the survey. *Table 12*, *Table 13*, and Figure 5 below display the detail of the responses.



Figure 4. Th3 P@\$W0rd_Ch@ll3ng3 summary page from the Cyber Awareness Challenge 2.0 training (DISA 2013).

Table 12.

Compliance Frequency Responses for Password Composition

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | Total | Mean | StdDev |
|-----------------|-------|--------|-----------|------------|--------|-------|-------|--------|
| % of Time | 0% | 25% | 50% | 75% | 100% | | | |
| Responses | 69 | 7 | 13 | 7 | 2 | 98 | 15.8% | 27.2% |

Table 12 presents the actual count of responses across the available response range.

Following the original data analysis plan described in the Descriptive Statistics section of Chapter 3 (p. 97) Table 13 recasts the same data as percentages of responses. Tables 12 and 13 parallel the example Tables 4 and 5 (p. 97). The coincidence of a sample size of 98 for the data cases the tables for count and percentage to appear almost identical.

Table 13.

Compliance Frequency Responses by Percentage for Password Composition

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | Total |
|-----------------|-------|--------|-----------|------------|--------|-------|
| % of Time | 0% | 25% | 50% | 75% | 100% | |
| Responses | 70% | 7% | 13% | 7% | 2% | 100% |

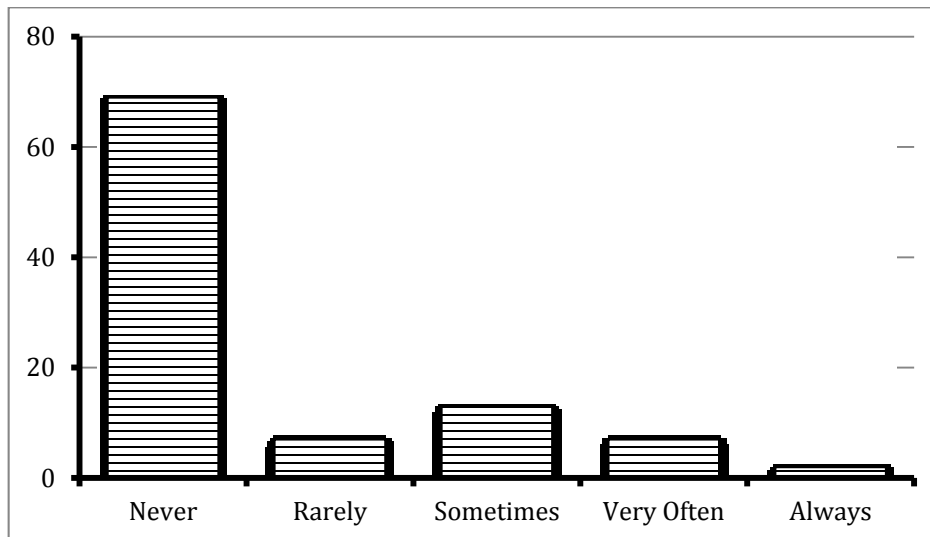


Figure 5. Compliance frequency distribution for password composition showing the approximate proportion of time personal information was used to develop passwords.

Password Storage

The second quantitative data collection question asked participants how often they have violated the trained guidance "Do not write down your password, memorize it" (DISA, 2013, Th3_P@\$W0rd_Ch@ll3ng3): **9. As best you can recall, within the past two years how often have you written down any computer system or account password?** Figure 4 above shows the source page for the quoted guidance. All 99 participants responded. *Table 14, Table 15,* and Figure 6 below display the detail of the responses.

Table 14.

Compliance Frequency Responses for Password Storage

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | Total | | |
|-----------------|-------|--------|-----------|------------|--------|-------|-------|--------|
| % of Time | 0% | 25% | 50% | 75% | 100% | | Mean | StdDev |
| Total responses | 34 | 26 | 18 | 14 | 7 | 99 | 33.3% | 31.9% |

Table 15.

Compliance Frequency Responses by Percentage for Password Storage

| Survey Response | Never | Rarely | Sometimes | Very Often | Always | |
|-----------------|-------|--------|-----------|------------|--------|-------|
| % of Time | 0% | 25% | 50% | 75% | 100% | Total |
| Total responses | 34% | 26% | 18% | 14% | 7% | 100% |

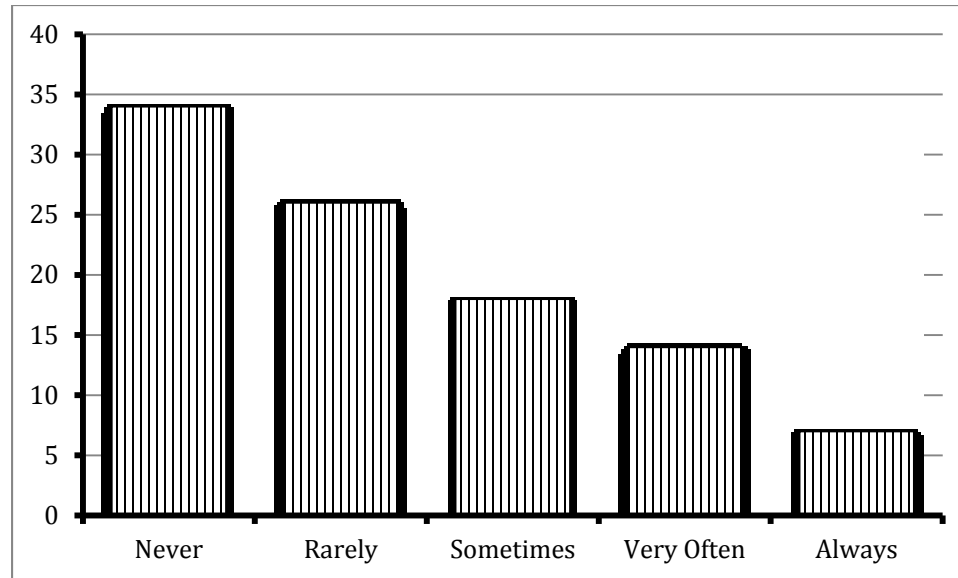


Figure 6. Compliance frequency distribution for password storage showing the approximate proportion of time passwords were written down,

As discussed on pages 99-100 of the Quantitative Analysis section of Chapter 3 and demonstrated in Table 6 on page 100, the collected data allowed comparison of non-compliance levels for the entire sample with the non-compliance levels for the portion of the sample that did not comply with each of the two password guidelines. *Table 16* displays the comparative values and standard deviation of the sample for each question for the entire sample and the non-compliant subset of the sample.

Table 16.

Mean Amount of Time Users Have Not Complied with Password Guidance

| Survey Question | Entire Sample | | Non-Compliant Users | | Proportion of Sample Who Did Not Comply |
|-------------------------|---------------|--------|---------------------|--------|---|
| | Mean | StdDev | Mean | StdDev | |
| P1- Personal Info in PW | 15.8% | 27.2% | 53.4% | 21.9% | 30% |
| P2- Recorded PW | 33.3% | 31.9% | 50.8% | 25.8% | 66% |

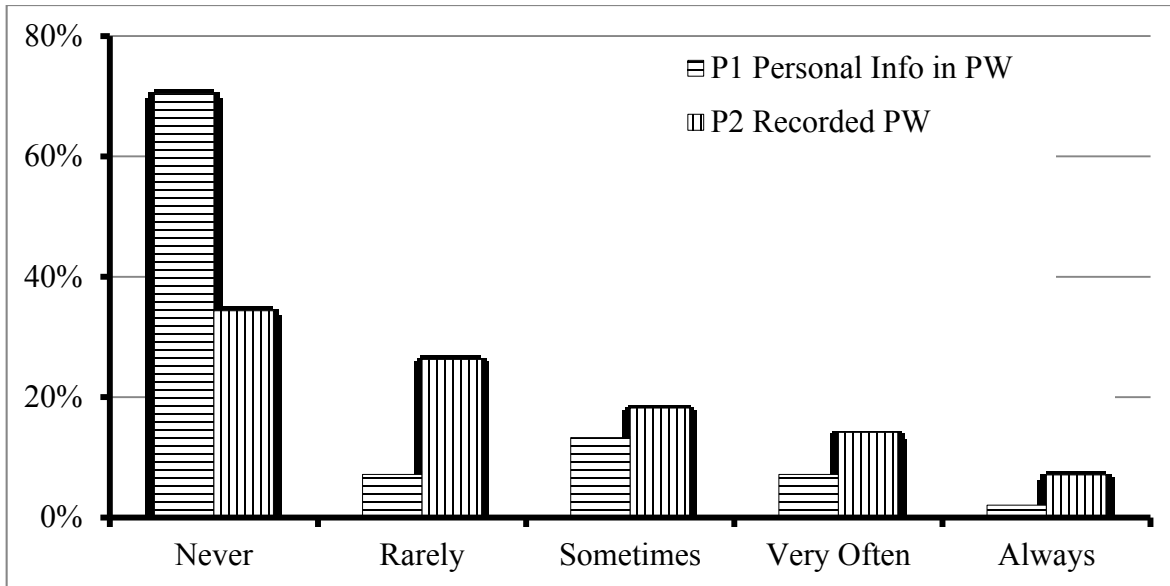


Figure 7. Comparison by proportion of the sample of the frequency of failing to comply with password formation and password storage guidelines.

Correlation of Responses

Of the 98 participants who responded to both of the password policy frequency questions, 22 admitted both to having used personal information for password composition and to recording passwords for storage. Thus, 22 out of 30, or 73%, who used personal information to form passwords also admitted to having recorded passwords instead of only memorizing the passwords. Conversely, 22 of the 60, or 37%, who recorded passwords also admitted having used personal information to compose passwords.

Some of the responses to the *why* questions, analyzed in detail in the next section, may shed light on the relationship between the use of personal information and the decision to write down passwords. A few examples follow.

- "I have an encrypted program and file to manage my passwords, with one password that is not written down to access them. Why? There are too many to remember, especially with the complexity requirements on top of that."

- "I have an encrypted program and file to manage my passwords, with one password that is not written down to access them. Why? There are too many to remember, especially with the complexity requirements on top of that."
- "I manage well over 20 accounts, including service accounts and test/dev accounts. I could not remember them all."
- "On occasion, the password requirements are so bizarre and/or over the top that is it impossible to remember the password. Most of us have from 20-40 passwords in our lives, and sometimes you just have no choice but to write down that one system, don't use it very often, password."

Qualitative Results

The structure introduced in *Table 8*.

Themes of Non-Compliance Reasons, a priori (p. 102) suggested ten possible themes that might be found in reasons stated for non-compliance aligned with three frameworks for analyzing the narrative data responses: a systems engineering framework, an information assurance framework, and a human performance framework. In that structure, the researcher identified ten possible themes that could appear in reasons stated for not following an IA policy. During the thematic analysis process the researcher identified two additional themes not originally contemplated.

The first newly identified theme was a nuanced variation of theme 4, *self-efficacy*, and theme 9, *process too difficult to follow*. Themes 4 and 9 are themselves only subtly different. Self-efficacy in theme 4 relates to statements of belief in personal ability to complete a task. In comparison, statements indicating an opinion that a process is too difficult for anyone, not just the responding individual, fall into theme 9. The difference between theme 4 and theme 9 is

comparable to the difference between *I can't do it that way* and *no one can do it that way*. Labeled as theme 11, the added theme was described as *ease of use of alternative process actually used*. While theme 4 had been correlated with a statement of self-efficacy, that is, a belief of inability to comply, the new theme 11 applied to statements indicating use of an easier alternative (although non-compliant) process, without being justified based on perceived level of ability to follow a compliant process. Paraphrasing the themes, theme 4 responses say *I can't do it that way*, while theme 11 responses say *I used an easier way to do it*. In Table 8 themes 4 and 9 were correlated with Social Cognitive Theory (Bulgurcu et al., 2010). Theme 11, indicating an ease of use perception, correlates more closely with the Technology Acceptance Model (TAM) as shown by Abraham (2012) in Appendix G. The final theme added during analysis, theme 12, was not related to a reason given for the noncompliant behavior. Instead, the researcher established theme 12 for those responses that explained *how* the participant violated the policy, a process statement, without answering the question of *why*. Table 17 displays the expanded list of themes.

Table 17.
Themes for Possible Reasons for Non-Compliance

| Theme ID | Theme (Category) | Theme ID | Theme (Category) |
|----------|--|----------|--|
| 1 | Negative Motivation | 7 | Tool too difficult to use |
| 2 | Positive Motivation | 8 | Never learned how to use tool (training) |
| 3 | Training | 9 | Process too difficult to follow |
| 4 | Self-efficacy | 10 | Rule makes no sense |
| 5 | IA policy conflicts with work process | 11 | Ease of use of alternative process actually used |
| 6 | IA tool not accessible in work environment | 12 | Explain how instead of why |

The reasons that participants gave for non-compliance can be related to a systems engineering framework, identified as relating to one of the three major components of any system of people, processes, or tools (Haskins, 2011). An alternative analysis of the responses uses themes from Parker's (1998, 2002) six assurance attributes of information: confidentiality, possession or control, integrity, authenticity, availability, and usability. Finally, the stated reasons for failure to comply with IA guidelines may be correlated with any of the eleven human performance theories identified across the information security literature by Abraham (2012). The theories are listed below in Table 18; Abraham's complete literature-linked exposition of the theories is reproduced in Appendix G. With no reason to treat these three frameworks as mutually exclusive, the discussion below presents an analysis of responses for the two password management questions based on the identified themes and all three frameworks.

Table 18.

Behavioral Theories in Information Security Studies (Abraham, 2012)

| | |
|-----------------------------|------------------------------|
| Theory of Reasoned Action | Protection Motivation Theory |
| Theory of Planned Behavior | Health Belief Model |
| Social Cognitive Theory | Value Focused Thinking |
| Technology Acceptance Model | Agency Theory |
| Deterrence Theory | Rational Choice Theory |
| Neutralization Theory | |

Password Composition

Of the total sample of 99 completed surveys, 98 participants responded to the question on frequency of using personal information to form passwords. 30 participants admitted to having used personal information to form passwords within the past two years. Out of that 30, 21 provided narrative responses answering the follow-on question to explain why they had done so. One comment of the 21 was an anomalous statement indicating a local rule in contradiction of the standard policy: "Because it was required at my new work location." A 22nd comment indicated an unwillingness to claim "never" but asserted recalling no specific instance. *Table 19* shows the distribution of the four themes identified across the 20 usable responses for password composition. A discussion of each framework follows.

Table 19.

Distribution of Themes in Reasons for Using Personal Information in Passwords

| Theme ID | Theme | # of Responses |
|----------|--|----------------|
| 4 | Self-efficacy | 1 |
| 9 | Process too difficult to follow | 4 |
| 11 | Ease of use of alternative process actually used | 8 |
| 12 | Explain how instead of why | 7 |

Systems engineering framework analysis. Relating each of the responses to one of the three system elements of people, processes, or tools (Haskins, 2011) provided a breakdown of 8 responses related to people, and 12 responses related to processes. It was not possible to relate any responses to the third system component of *tools*. Haskins used the term *product* as synonymous for *tool* in the current study, and described *product* as "hardware, software, firmware" (Haskins, 2011, p. 5)

With respect to the *people* element, it should be apparent that "the human is an element of every system" (Haskins, 2011, p. 326). Further explaining the nature of the *people* element, "humans possess particular knowledge, skills, abilities, expertise, and cultural experiences" (Haskins, 2011, p. 326). The 8 *people* responses all dealt with the use of personal information in passwords as a form of memory aid. For instance, one participant commented, "I have a hard time remembering multiple passwords, so I incorporate personal 'tidbits' that I'll remember."

A *process* is a "set of interrelated or interacting activities which transforms inputs into outputs" (Haskins, 2011, p. 5). The 12 *process* responses each approached the processes of using personal information to build passwords. For example, one participant admitted, "Sometime use pet name with combination of numbers and special characters."

Table 20.

Distribution of System Components in Reasons for Using Personal Information in Passwords

| System Component | # | System Component | # | System Component | # |
|------------------|---|------------------|----|------------------|---|
| People | 8 | Processes | 12 | Tools | - |

Information assurance framework analysis. When categorizing the password composition responses using the Parkerian Hexad (Kabay, 2008; Parker, 1998, 2002) as the framework, 21 responses fell into the theme of usability. Kabay provided concise descriptions for each of Parker's assurance attributes:

- Confidentiality - "Restricting access to data" (p. 6)
- Possession - "Control over information" (p. 7)
- Integrity - "Internal consistency, validity, fitness for use" (p. 9)
- Authenticity - "Correspondence to intended meaning" (p. 11)
- Availability - "Timely access to data" (p. 13)
- Utility (Usability) - "Usefulness for specific purposes" (p. 15)

Whether the justification for using personal information was to aid in memorization, or as a tool in building the passwords, the workers were making the password process more usable. The reader can infer the usability aspect of survey responses such as, "Users have a hard time remembering their own name much less some randomly generated character sequence that means nothing to them." The workers' intent was not to make the passwords more or less confidential, or to establish a different level of control or possession of the passwords. From the viewpoint of those workers, both the integrity and authenticity of the passwords were established by each worker designing the passwords for personal use. *Table 21* presents the IA element distribution in a standard layout, to allow comparison with the same representation for password composition in *Table 26*.

Table 21.

Distribution of IA Elements in Reasons for Using Personal Information in Passwords

| IA Attribute | # | IA Attribute | # |
|-----------------|---|-----------------------|----|
| Confidentiality | - | Possession or Control | - |
| Integrity | - | Authenticity | - |
| Availability | - | Usability | 21 |

Human performance framework analysis. Only 12 of the participants' stated reasons for using personal information to form passwords could be categorized from a human

performance theory perspective. Four respondents mentioned an inability to recall passwords with statements like, "I have a hard time remembering multiple passwords" , a *self-efficacy* statement that relates to Social Cognitive Theory (Abraham, 2012; Bulgurcu et al., 2010). Self-efficacy is also a component of Protection Motivation Theory (Workman et al., 2008), but the responses did not indicate a concern over protection from risk, a central role of protection motivation. Eight respondents stated the personal information use was to make the passwords easier to remember with comments such as, "at times I'll create passwords based on things that have meaning or value to me," an ease of use reason that relates to the Technology Acceptance Model (Cannoy & Salam, 2010). In addition, seven participants explained how they used the personal information in forming passwords, a process (SE) locus, without saying why. See the section on Theoretical Frameworks for Worker Compliance with Procedures beginning on page 36 in Chapter 2, Review of the Literature, for descriptions of Abraham's overview of theories found in the information security literature, as well as descriptions of several specific studies included in Abraham's listings.

Table 22. Distribution of Performance Theories in Reasons for Using Personal Information in Passwords

| Human Performance Theory | # |
|---|---|
| Social Cognitive Theory (self-efficacy) | 4 |
| TAM (ease of use) | 8 |

Table 23 below summarizes for direct comparison the distribution of categories across all three frameworks as identified in the study sample.

Table 23.
Distribution of Framework Categories in Reasons for Using Personal Information to Form Passwords

| System Components | # | IA Attributes | # | Human Performance Theory | # |
|-------------------|----|-----------------------|----|--------------------------|---|
| People | 8 | Confidentiality | - | Social Cognitive Theory | 4 |
| Processes | 12 | Possession or Control | - | TAM | 8 |
| Tools | - | Integrity | - | | |
| | | Authenticity | - | | |
| | | Availability | - | | |
| | | Usability | 21 | | |

Password Storage

All 99 participants in the sample responded to the question on frequency of writing down passwords. 65 participants admitted to having written down passwords within the past two years. Out of that 65, 58 provided narrative responses answering the follow-on question to explain why they had done so. *Table 24* shows the distribution of the four themes identified across the 56 usable responses for password storage. A discussion of each framework follows.

Table 24.
Distribution of Themes in Reasons for Writing Down Passwords

| Theme ID | Theme | # of Responses |
|----------|--|----------------|
| 4 | Self-efficacy | 16 |
| 9 | Process too difficult to follow | 7 |
| 11 | Ease of use of alternative process actually used | 24 |
| 12 | Explain how instead of why | 9 |

Systems engineering framework analysis. Viewing the responses from a systems engineering perspective, 28 respondents touched on the *people* element of the system, 48 of the 58 comments described some aspect of the *process* element of the system, and 10 referred to *tools* used to circumvent the policy. The majority of process-related responses described processes the respondents had chosen as a means of implementing the policy violation. However, 4 responses described surrounding work processes that necessitated the non-compliant action of recording passwords, such as situations of password resets and system administrator accounts where multiple individuals use the same account. One such example from a participant's response was, "When personally resetting a password for another user, which they will be forced to change at first login." Of the 10 responses mentioning tools, 6 describe the use of password vaults, encrypted files or drives, and even a secure storage safe. Such tools, while violating the letter of the policy, could be considered as meeting the intent of the policy to protect passwords from outside discovery while simultaneously meeting the IA attributes of *availability* and *possession or control* as well as *confidentiality* (Parker, 1998, 2002). See Kabay's (2008) simple exposition of the attributes on page 122.

Table 25.

Distribution of System Components in Reasons for Writing Down Passwords

| System Component | # | System Component | # | System Component | # |
|------------------|----|------------------|----|------------------|----|
| People | 28 | Processes | 48 | Tools | 10 |

Information assurance framework analysis. When categorizing the password storage responses using Parker's six IA attributes (1998, 2002) 39 participants addressed issues of *usability* while 7 participant described a process involving *possession or control*, 6 of which were the comments categorized as tool-related under the SE perspective. Within the 39 *usability* responses, further information was available as 17 referred to the challenge of memorizing

passwords meeting complexity of composition policies and 15 referred explicitly to the problem of having to remember multiple passwords. Typical of the references to password multiplicity and complexity was one participant's statement, "There are too many to remember, especially with the complexity requirements on top of that." See Figure 8 and Figure 9 for examples of password complexity recommendations that may be found as formal requirements in some systems. The same images are in Appendix A as Figures A5 and A6 (DISA 2013) as part of the complete source training materials. Compliance with password complexity policies was not included in this study because, in the researcher's experience on multiple networks, complexity policies are generally enforced on government systems by system software, and thus not subject to user decision. *Table 26* presents the distribution of IA element in password storage responses in the same layout as *Table 21* for ease of comparison between the two rules.



Figure 8. Th3 P@\$\$WOrd_Ch@ll3ng3 practice screen providing two examples of password complexity guidelines (DISA, 2013).



Figure 9. Th3 P@\$\$WOrd_Ch@ll3ng3 summary screen showing the mandatory password complexity policy used in the intelligence community (DISA, 2013).

Table 26.

Distribution of IA Elements in Reasons for Writing Down Passwords

| IA Attribute | # | IA Attribute | # |
|-----------------|---|-----------------------|-------------------------------------|
| Confidentiality | - | Possession or Control | 7 |
| Integrity | - | Authenticity | - |
| Availability | - | Usability | 39 (17 Complexity, 15 Multiplicity) |

Human performance framework analysis. In reviewing the narrative responses for indications of human performance theory the researcher identified indicators for the same two theories as for password composition, Social Cognitive Theory indicated by statements of self-efficacy, and Technology Acceptance Model indicated by statements on ease of use. Twenty-three respondents indicated an inability to memorize the required passwords, an issue with self-efficacy, indicating a relationship to the Social Cognitive Theory. A typical statement of self-efficacy from one respondent was, "I have so many work related passwords and logins to

Government acquisition portals, that I can't remember them." All but 4 of the 23 statements on self-efficacy mentioned password complexity or multiple passwords as contributing to the inability to memorize the passwords. An almost equal number, 24 participants, indicated writing down passwords or password hints as being easier than memorizing the passwords, without declaring an inability to remember the passwords. One example of such an ease of use statement: "Sometimes I'll write one down as I'm creating it to help me ensure I remember it correctly, or to make sure I record it correctly in my secure password manager." *Table 27* shows the distribution of performance theories found in the sample.

Table 27.

Distribution of Performance Theories in Reasons for Writing Down Passwords

| Human Performance Theory | # |
|---|----|
| Social Cognitive Theory (self-efficacy) | 23 |
| TAM (ease of use) | 24 |

Table 28 below summarizes for direct comparison the distribution of categories across all three frameworks as identified in the study sample.

Table 28. Distribution of Framework Categories in Reasons for Writing Down Passwords

| System Components | # | IA Attributes | # | Human Performance Theory | # |
|-------------------|----|-----------------------|----|--------------------------|----|
| People | 28 | Confidentiality | - | Social Cognitive Theory | 23 |
| Processes | 48 | Possession or Control | 7 | TAM | 24 |
| Tools | 10 | Integrity | - | | |
| | | Authenticity | - | | |
| | | Availability | - | | |
| | | Usability | 39 | | |
| | | PW Complexity | 17 | | |
| | | Multiple PWs | 15 | | |

One participant's statement of a reason for writing down passwords stood out and is worthy of quoting here: "Writing them down to convey them to other people, as special characters are easier to write than say sometimes. Also writing them down to convey them avoids email." The statement indicates either ignorance of the concept of keeping passwords confidential, or is related to the situation of password resets by administrators, addressed above. Without further context from the participant it is impossible to distinguish. Similarly, another participant stated, "I sometimes write down system password to ensure that I implement the same password across multiple systems." The statement appears to indicate ignorance of the risks of reusing passwords across systems (Das, Bonneau, Caesar, Borisov, & Wang, 2014).

Summary

Data collected from 99 participants showed that more participants will answer simple quantitative questions on frequency than will provide narrative responses on reasons for not complying with IA policies. The rate of non-compliance with the password composition policy not to use personal information is half that of the password storage policy not to write down passwords, for both proportion of the population, and frequency of non-compliance. 30% of the sample has used personal information in passwords, compared to 60% of the population who have written down passwords. Likewise, across the population passwords had been formed with personal information 16% of the time, while passwords had been written down 34% of the time. Interestingly, among those who chose to break either policy, they did so half the time.

The researcher identified only three common themes among the reasons for noncompliance with the two password policies: statements indicating the prescribed process was too difficult for the respondent to follow (self-efficacy), statements indicating the prescribed process was too difficult for anyone to follow, and statements describing a choice to follow an

easier process than prescribed without commenting on the difficulty of the prescribed process. For the policy not to use personal information the choice of an easier process occurred roughly two-thirds of the time, 8 of 13 responses. For the policy not to write down passwords the choice of an easier process occurred roughly half the time, 24 of 47 responses. In addition to identifying the three broad themes, the researcher categorized the responses from the perspectives of three established frameworks, systems engineering, information assurance, and human performance.

The review of participants' stated reasons for not complying with the two password policies revealed slight differences between the two policies with regard to a systems engineering viewpoint, but similar themes identified when analyzed from information assurance and human performance theory perspectives. Using a systems approach, reasons for non-compliance were found at roughly equal levels for *people* and *process* elements of the system, with no mention of *tools*. In contrast, reasons stated for writing down passwords were twice as often related to *processes* as to *people*, and the reasons related to *people* were nearly three times as prominent as those for *tools*. When analyzed with an information assurance perspective, issues of Parker's (1998, 2002) sixth attribute of *usability* dominated the responses for both password policies, although a smaller number of *possession or control* reasons appeared among reasons for writing down passwords. Using the human performance framework, reasons given for failing to comply with both password policies included statements of self-efficacy, indicating possible interpretation relevance of Social Cognitive Theory and ease of use, indicating the Technology Acceptance Model may be relevant. However, while TAM appeared twice as often as Social Cognitive Theory in reasons for using personal information for passwords, the two theories appeared in effectively equal numbers in reasons for writing down passwords.

Results from the data collection and analysis in this chapter allow for several conclusions and recommendations for IA practice and further research. In some ways the results presented open up more questions than answered. The next and concluding chapter presents the researcher's observations, conclusions, and recommendations.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

The research described in this study addressed the general topic of IA practices and compliance with basic IA policies. In an effort to learn more about why people do not follow IA policies when regularly trained on the policies, the study quantified two dimensions of policy compliance, that is, what proportion of a population has failed to comply with basic policies, and how often the policies are violated. The study has examined in detail only two specific IA policies, both integral to password management, but has laid the groundwork for extending the methodology used to a wider range of IA policies. Data collected in the course of the study will be available to support such an extension of the study goal. The remainder of this chapter addresses conclusions the researcher has reached from the analysis completed, along with recommendations for practical use of the results presented here, as well as potential future studies. The discussion begins with an acknowledgement of limitations found in the study itself.

Limitations

The first limitation experienced during the conduct of this research was the difficulty in obtaining participation from an open community. *Table 9* (p. 108) shows the prospective number of potential participants in the solicitation process. Compare those numbers with the rate of participation shown in *Table 10* (p. 108). While tens of thousands of potential participants were in the solicitation groups, only tens of volunteers completed the survey each of the six weeks that the survey was open. It is not known what proportion of the groups solicited to participate consisted of members of the target population, workers involved with the handling of the federal government information.

Another limitation discovered during the conduct of the study was the inability to confirm accurate differentiation between participants who have IA duties and those who do not.

The impact of this limitation was discussed in the section on Data Plan Modification in Chapter 4 (pp. 109-110). The limitation caused a shift in the research plan and a reduction in the amount of information that could be developed from the results relative to the originally proposed research. The section on suggested future research below includes possible means of correcting for this limitation in follow-on research with more targeted populations.

Findings and Interpretations

Chapter 1 introduced three general research questions for study (p. 13). Chapter 3 presented a discussion of various IA policies derived from a specific training source (DISA, 2013) and a decision on how to scope the present study. The selection and scoping decisions led to a set of six specific research questions (p. 73) for the present study. The collected data analyzed in Chapter 4 have provided answers to the specific research questions.

Answers to the Research Questions

R1₁. Why have users *used personal information to select passwords*?

A1₁. Because they feel they cannot remember passwords otherwise or to make the passwords easier to remember.

R2₁. What proportion of the population has *used personal information to select passwords*?

A2₁. 30%, just under one-third, of the population admitted to using personal information to form passwords.

R3₁. How often have users *used personal information to select passwords*?

A3₁. Personal information was used to form passwords about 16% of the time (Table 16, p. 116).

R1₂. Why have users *written down passwords*?

A1₂. To make the passwords easier to retrieve and use, or because passwords are too difficult to memorize. The difficulty in memorizing passwords is primarily due to requirements to memorize a large number of passwords, and to construct complex passwords.

R2₂. What proportion of the population has *written down passwords*?

A2₂. Two-thirds (66%) of the sample had written down passwords in the past two years.

R3₂. How often have users *written down passwords*?

A3₂. Passwords were written down about 33% of the time (Table 16, p. 116).

Password Composition

A significant majority, 70%, of respondents reported complying at all times with the policy to avoid use of personal information in forming passwords. Of the 30% who admitted to using personal information, all of the reasons given addressed aspects of usability, either ease of use, or a declared inability to remember passwords without such an assist. The reasons given were divided equally between aspects of the people involved in the system (the respondents themselves) and the processes they follow to form passwords. The researcher observed that in no case was there any mention of a lack positive motivation to comply with the policy, or negative motivation in the form of negative consequences for not complying. A preliminary conclusion from this observation is that would be a waste of time to pursue reward or punishment methods as motivational processes to gain compliance from the worker population. Applying human performance theories such as Deterrence Theory, Theory of Planned Behavior, or Protection Motivation Theory, all observed in IA compliance literature by Abraham (2012), is not likely to change the level of compliance. On the other hand, applying principles of Agency Theory or Rational Choice Theory, also reported by Abraham as extant in the information security literature, may still provide benefit in building levels of compliance.

Password Storage

Only 40% of the sample claimed complete compliance with the policy not to write down passwords, compared to 70% who claimed full compliance with the policy not to use personal information to form passwords. Further, the frequency distribution of noncompliance from rarely to always showed a consistent smooth curve. The display in Figure 7 (p. 116) provides a convenient comparison of the two results. The comparison suggests that the population is generally more willing to violate the password storage policy than the password composition policy.

The researcher suggests that the usability aspects highlighted in the reasons given, complex password requirements and a large number of passwords to remember, make it much harder to comply with the password storage policy. Further, there may be a logical relationship between the two practices. That is, the harder passwords are to recall, whether due to multiplicity of passwords or complexity of individual passwords, the more likely users will be to record passwords. Such a relationship is suggested by the difference in levels of compliance: approximately twice as many in the sample wrote down passwords than composed passwords with personal information, 60% compared to 30%.

As discussed above for the password composition policy, none of the reasons given for writing down passwords hinted at either positive or negative motivation concerns on the part of respondents. The researcher has concluded that for the password storage policy, just as for the password composition policy, there is no indication in this study that trying to increase compliance levels by applying either reward or punishment theories in the workplace. The researcher recognizes that the study is not a study in psychology. As such, the data collected reflects reasons stated by the participants, which could be challenged from a psychological

perspective as not reflecting true reasons for participants' actions. The researcher leaves pursuit of the line of thought for discovery of "true" reasons for actions, if different from stated reasons, to competent researchers in the human behavior fields such as psychology and sociology.

Conclusions Related to the Frameworks

Chapter 1 of this dissertation introduced a set of structural and theoretical frameworks for the study. The three frameworks described were a systems engineering framework, an information assurance framework, and a human performance framework. The following sections describe the interpretation and use of the results of the study relative to each of the three frameworks.

System Engineering Framework

The fundamental approach to systems engineering is consideration of the three basic elements of any system, *people*, *processes*, and *tools* (Haskins, 2011). In the study described here the focus has been on the system elements of people and the processes people follow. The study has examined what people have done and reasons they state for their actions. For example, one participant stated, "I have used and continue to use the last four of my SSN to meet the password requirements for numerics (sic) because it's easy to remember." In the context of password management the two IA policies studied do not provide processes for password composition or for password storage. Rather, each rule restricts people from using one specific process, without prescribing alternative processes or tools.

IA policy P1 was "Do not use personal information" (DISA, 2013, Th3_P@\$W0rd_Ch@ll3ng3), restricting people from using one available process for composing passwords. The official training used to promulgate policy P1 suggested no

alternative processes people might have available to compose memorable passwords. The requirement for memorable passwords is a direct result of policy P2.

IA policy P2 was "Do not write down your password, memorize it" (DISA, 2013, Th3_P@\$W0rd_Ch@ll3ng3). The training suggested no processes to assist in memorizing passwords. In addition, the training did not mention any usable tools for recording passwords securely. Clearly, several study participants were aware of such tools, mentioning the use of password vaults, physical safes, and encrypted files as alternative means of protecting the confidentiality of passwords.

The researcher has concluded that the existing IA training is too narrowly focused on the people element of the system and on traditional IA guidelines, and has not kept up with a full systems approach to meeting the actual IA goals in the enterprise. The researcher further inferred an assumption about the approach to developing IA policies and the resultant training: Aspects such as password management have been addressed in isolation from the overall IA system environment. The two policies studied may seem reasonable if applied only to a single password of reasonably memorable composition. However, as many study participants pointed out, the actual environment is much more complex. Workers must create dozens of passwords using some on a daily basis but others only infrequently. Further, password complexity rules, created to avoid password-guessing attacks, combine to make passwords even harder to recall.

Information Assurance Framework

Responses for reasons for not complying with both studied policies tied heavily to the IA attribute of usability. Participants gave evidence of the usability challenge with statements such as the following:

- "I have a hard time remembering multiple passwords."

- "It is nearly impossible to use a wide array of passwords for so many different applications and change them as often as required without either using personal information to prod the memory yet remember them without writing any down."
- "I use obsolete PII as a memory trigger."
- "Complexity requirements make it necessary to use some data to create strong pw that can be remembered."
- "Complex passwords can be difficult to learn"
- "There are too many to remember, especially with the complexity requirements on top of that."
- "I cannot remember them all"

The researcher has concluded that password policies have not been developed with a complete consideration of the full set of essential information attributes laid out by Parker (1998, 2002). The password composition policy has incorporated consideration of neither usability nor availability, seemingly focused entirely on confidentiality. Similarly, the password storage policy seems to be lacking by not having incorporated an understanding of the attributes of possession or control and availability.

The IA policy to avoid using personal information in passwords exists to make passwords difficult for others to guess. The IA policy not to write down passwords exists to make passwords difficult for others to find. Both IA policies exist to assure only one IA attribute of passwords and the systems protected: *confidentiality*. However, these two policies not only work at cross-purposes to each other, they also fail to consider other IA attributes such as *availability* and *usability*. Forming passwords that are difficult to guess results in passwords that are also difficult to remember. Easily memorable passwords have high usability but easily forgettable

passwords have low usability. Forgotten passwords, if not recorded, have lost *availability*. In attempting to protect confidentiality without considering usability and availability, the two studied IA password policies together make operations more difficult and less likely to find compliance with the policies.

Taking a different approach, the policy not to write down passwords, especially when the companion policy makes passwords less memorable, is a failed protection of confidentiality. However, if a password management policy were to be built considering the real goal, protection of information, with a combined use of the attributes of confidentiality and possession or control, the environment could enhance the protection goal more effectively. Many participants in the study provided a possible solution, that is, give users a *tool*, a password vault, either physical or digital, as a SE complement to the failed attempt to rely on the SE elements of *people* required to follow demonstrably unworkable *policies*. Survey responses such as the following point to such a solution:

- "Store in a password vault."
- "I would like to have it on a password manager or TrueCrypted file."
- "I have an encrypted program and file to manage my passwords, with one password that is not written down to access them."
- "Account information in an encrypted store."
- "I might store them in a file on an encrypted drive."
- "All of my passwords are stored in a password vault (commercial product)."
- "Passwords are written on a plain white paper ... sealed with a signature placed on the sealed envelope. The envelope is placed in a GSA fire-resistant safe."
- "Passwords were contained within a (sic) approved safe."

Human Performance Framework

Abraham (2012) identified 11 theories of human performance applied across the IA compliance motivation literature, listed both in Table 17 (p. 118) and in Appendix G. The preliminary results from this study suggest that many of those theories may be insufficient to improve levels of worker compliance with the specific IA policies on passwords examined in the current study. The researcher has concluded that more research is needed along the lines of this study, determining first why people have not been complying with IA policies, which may not be the same as the reasons the people may state, concerning passwords before there is full value in trying to mold an implementation to fit a pre-selected theory. The researcher noted on page 134 that no responses gave evidence of other theories of performance than two, suggesting that theories on positive or negative motivation may not be relevant. However, it is poor logic to assume that *no evidence is evidence*. To counteract such an assumption, the researcher suggests a need for further research to ask why people *have*, as opposed to *have not*, complied with specific IA policies.

The Overarching Framework

In Chapter 1 the Overarching Framework section (p. 18) described a systems engineering approach, informed by IA principles and human performance theories. The study described in this paper suggests that such an approach to IA can work for improving an understanding of the nature the IA status in an enterprise. However, the information gleaned from this study on password management only indicates that there is promise in such an approach. The researcher has concluded that further use of the approach described here is essential across a broader range of IA policies. Extending the methods of the current study across broader policies and populations is discussed further below in the section on recommended future studies.

Recommendations

The fundamental recommendation from this study is that planning for IA in an enterprise should be approached by looking at all elements of the IA system: people processes, and tools. When designing IA policies, it is essential that both the capabilities and motivations of the affected people be incorporated into the decision process. Further, when seeking to meet any given IA goal, the reasonable availability of tools that could meet the goal without involving people following processes should be considered. When the combined processes and people demonstrate an inability of the enterprise to meet an IA goal, as this study has shown for password management, then planning should proceed to develop tools which can by pass the need for people to follow IA processes.

Recommendations for Future Research

Use of Collected Data

The data collection instrument used for the present study provided data on frequency of non-compliance and stated reasons for eight IA rules beyond the two password rules analyzed here. The data is available for analysis in a future study, using the same procedure as in the current research. Future research can use the data already collected to extend an understanding of the reasons users give for failing to follow known IA guidelines. Once the qualitative analysis on all ten IA rules is complete, another level of study will be possible.

For instance, future research could examine whether the set of categories for non-compliance for the memory-based password policies developed in the described study is the same as the set of categories found in the personal-gain ethics related policies. Future research could use the data analysis from the complete data set collected to examine whether different types of IA guidelines elicit variant reasons for non-compliance.

Follow On Quantitative Studies

As described in Chapter 1 the qualitative analysis described here may set the stage for a follow-on quantitative study. The present study would become the first stage of a larger exploratory sequential mixed methods design (Creswell & Plano Clark, 2011). The study described here presented categorized and normalized reasons for non-compliance with specific IA rules. The follow on study could survey members of a defined population asking participants to select from list of reasons derived from this and similar future studies, rather than asking the open-ended question of why. The suggested study would support a quantitative analysis of the selection of the reasons derived in the study described here. Here are suggested questions and response sets for such quantitative studies:

1. If you have used personal information to create passwords in the past two years, which of the following reasons best expresses why? (You can select one or more answers.)

- It makes them easier to remember.
- I cannot remember them without some kind of personal memory hook.
- I have too many passwords to remember.
- My passwords have to be too complex to remember without some personal information.
- I'm not allowed to write down my passwords, so I have to make them memorable.
- No one checks to make sure I haven't, so I can't be punished for it.
- There is no prize for "best password of the quarter."

2. If you have written down any passwords in the past two years, which of the following reasons best expresses why? (You can select one or more answers.)

- I have too many passwords to memorize all of them.

- My passwords have to be too complex to memorize.
- I have no encrypted password program where I could store passwords safely.
- I have some passwords I have to be able to share with other team members or administrators.
- I have to provide new passwords to users in a form they can use.
- No one can find where I write them down, so I cannot be caught and punished for it.
- There is no prize for "most passwords accurately memorized."

Comparing IA and Non-IA Workers

The shift in the research plan described in chapter 4 demonstrated the difficulty in obtaining clarification of whether individuals have specific information assurance duties. Future research involving sponsored, approved study within a single organization of the Defense Department could provide an accurate comparison of the two groups by using reference to Department of Defense Directive 8570.01 (DoD, 2007). By conducting the survey with a single target population of one Defense Department service or agency, and changing the wording of the question concerning IA duties, the research study would be able to gain a more accurate comparison of the compliance performance of workers with and without IA duties. The research recommendation is to use the survey is presented in Appendix B but change the wording of question number six as shown in the current survey. The question should be reworded as follows: "Are you required under the provisions of DoD Directive 8570.01 (DoD) to hold a professional certification in information assurance or cyber security?" Should other federal agencies adopt IA or cybersecurity certification provisions similar to the Defense Department's 8570 requirements

(DoD), the same sort of study should be conducted in those other organizations with a similarly worded question to the one proposed above.

Ask the Counterpoint Questions

As suggested on page 140, the current study only examined on side of a two-sided question: why have people *not* followed specific IA policies? For the full story, research using a similar methodology should ask people why they *have* followed specific IA policies. The same instrument used for the current study could be used, but the second part of each compliance question (Appendix B, p. 192) would become, *If you selected Never please briefly explain any reasons(s) for your actions.* With a similar thematic analysis of responses, especially with regard to human performance theories, a comparison of reasons for complying and reasons for not complying with the same policies could be very enlightening.

Improving the Qualitative Data

The findings discussed above highlighted the very low response rate for the qualitative questions on ethical computer use. Research studies using personal interview methods (Creswell, 2012; Fink, 2009) instead of an online survey form may elicit more complete information from participants for reasons for failing to follow computer usage guidelines. The design of such a survey would need to include strong protections for participant anonymity to encourage full open information from the participants.

Another suggestion for improving the quantity of narrative responses is to arrange for a study such as this one to be officially sponsored by individual enterprises, such as a single large business entity, or a single large government agency. Official announcements and inducements to participate may greatly increase the rate of participation over what was seen in this study. However, if a researcher is able to arrange for such sponsored research, special caution will be

needed to assure both real and perceived levels of anonymity and confidentiality for participants. If workers in an enterprise suspect that their responses will be used to discipline them for non-compliance, they will not be likely to provide complete and honest answers.

Response Rate in Data Collection

The data displayed in *Table 11* (p. 111) shows that almost the entire the sample group was willing to answer all of the quantitative questions asking *how often have you violated a rule*. At the same time there was a rapid fall off in willingness to provide narrative information answering the question of *why*. The observation that fewer than 10% of the participants provided responses to the reasons for violating ethical computer use guidelines, compared to a range of 17% to 60% for the other IA guidelines, suggest that the change in response rate is not simply a matter of survey fatigue. It is intuitive that it is easier to click a single selection box than to write a narrative answer to a survey question. Yet well over half the participants in the current study took time to write answers for the password composition question. By comparison, well under 1/10th of the participants were willing to write answers for the four ethical computer use questions. Response rate for email use and data protection questions fell between those extremes.

There may be discernable differences in the nature of the several policy groups addressed in the current study survey. The first step in future research should be to complete the full analysis of the eight remaining policy question data sets, using the same methods as for the password questions. With data on all four policy groups analyzed for recurrent themes, it may be possible to relate the nature of the policies to the response rates. In addition, future studies could use the same question set as the current study, gathering parallel data form an different or expanded population, but randomize the order of the ten question pairs across the participants.

Such a randomizing order process could correct for an inadvertent survey fatigue affect, which might cause fewer answers to open ended questions at the end of a survey than at the beginning.

Summary

This study has introduced a novel approach to examining reasons for non-compliance with IA policies. Asking directly for open ended narrative, instead of assuming a set of possible reasons, usually tied to a chosen behavior theory, had not been found in prior research literature on IA compliance. This study has demonstrated that the approach is workable, and has provided preliminary information about a limited set of IA polices focused on password management. Further, the study has pointed out possible benefits of approaching IA goals from a systems engineering perspective, informed by human performance theories. The researcher suggests that this study can become a starting point for further research that will eventually result in significant improvements to the IA posture of many enterprises, both governmental and commercial.

REFERENCES

- Abraham, S. (2012). *Exploring the effectiveness of information security training and persuasive messages* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses. (UMI 3553544) <http://search.proquest.com/login/capitol-college.edu:2048/docview/1315238988/6E1BD2C09E094536PQ/1?accountid=44888>
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12), 41–46. <http://dx.doi.org/10.1145/322796.322806> Reprinted in L. F. Cranor & S. Garfinkel (Eds.) (2005), *Security and usability: Designing secure systems that people can use* (pp. 639-649). Sebastopol, CA: O'Reilly Media, Inc.
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. *Proceedings of the 45th Hawaii International Conference on System Sciences* (pp. 3317-3326). <http://dx.doi.org/10.1109/HICSS.2012.516>
- Al-Saleh, M. I. (2011). *Fine-grained reasoning about the security and usability trade-off in modern security tools* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses. (UMI 3473135) <http://search.proquest.com/login/capitol-college.edu:2048/docview/902636782/62DD9FB0274D4F0EPQ/1?accountid=44888>
- Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: a rational choice perspective. *Journal of Organizational and End User Computing* 16(3). 22-40. <http://dx.doi.org/10.4018/joeuc.2004070102>
- Baron, M. A. (2008). *Guidelines for writing research proposals and dissertations*. Retrieved from http://www.regent.edu/acad/schedu/pdfs/residency/su09/dissertation_guidelines.pdf

- Bartlett, J. E. II, Kotrlik, J. W., & Higgins, C. C. (2001). Organizational Research: determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19(1), 43-50. Retrieved from http://intranet.mekonginstitute.org/2010/5.Regional_research_development_and_methodology_3_21may_2010/documents/About_Programme/Modules/Module3/Reading_Sample_Size.pdf
- Blythe, J., Koppel, R., & Smith, Sean W. (2013). Circumvention of security: Good users do bad things. *IEEE Security & Privacy*, 11(5), 80-83. <http://dx.doi.org/10.1109/MSP.2013.110>
- Bornmann, J. W. (2014a). *Qualitative Data Analysis - TSE079*. Recorded video of lecture conducted from The MITRE Institute, McLean, VA.
- Bornmann, J. W. (2014b). *Methods & Tools for Analyzing Qualitative Data - TSE582*. McLean, VA: The MITRE Institute.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. A. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18, 151-164. Retrieved from <http://www.palgrave-journals.com/doi/10.1057/ejis.2009.8>
- Brostoff, S., & Sasse, A. M. (2001). Safe and sound: A safety-critical approach to security design. *Proceedings of the New Security Paradigms Workshop 2001*, 41-50. Retrieved from <http://www.nspw.org/proceedings>
- Brown, R. A., Kennedy, D. P., Tucker, J. S., Golinelli, D., & Wenzel, S. L. (2013). Monogamy on the street: A mixed method study of homeless men. *Journal of Mixed Methods Research*, 7(4), 328-346. <http://dx.doi.org/10.1177/1558689813480000>

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*. Paper 419. Retrieved from <http://aisel.aisnet.org/amcis2009/419/>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. Retrieved from http://www.academia.edu/3059288/Information_Security_Policy_Compliance_An_Empirical_Study_of_Rationality-Based_Beliefs_and_Information_Security_Awareness
- Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research*. Chicago, IL: Rand McNally. As cited in Fink, A. (2009). *How to conduct surveys: A step-by-step guide* (4th ed.). Los Angeles: Sage.
- Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*, 53(3), 126-131. <http://dx.doi.org/10.1145/1666420.1666453>
- Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *Security & Privacy*, 12(1), 28-38. <http://dx.doi.org/10.1109/MSP.2013.106>
- Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). New York: John Wiley & Sons. As cited in Bartlett, J. E. II, Kotrlik, J. W., & Higgins, C. C. (2001). Organizational Research: determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19(1), 43-50. Retrieved from http://intranet.mekonginstitute.org/2010/5.Regional_research_development_and_method

[ology_3_21may_2010/documents/About_Programme/Modules/Module3/Reading_Sample_Size.pdf](#)

Collaborative Institutional Training Initiative (CITI). (2012). *Capitol College IA doctorates curriculum*. Retrieved from <http://www.citiprogram.org>

Committee on National Security Systems (CNSS). (2010). *National information assurance (IA) glossary* (CNSS Instruction No. 4009). Retrieved from <http://www.cnss.gov>

Committee on Pre-Milestone A Systems Engineering. (2009). *Pre-milestone a and early-phase systems engineering: A retrospective review and benefits for future air force acquisition*. Washington, DC: The National Academies Press. Retrieved from http://www.nap.edu/catalog.php?record_id=12065

Conaway, R. N., & Wardrope, W. J. (2010). Do their words really matter? Thematic analysis of U.S. And Latin American CEO letters. *Journal of Business Communication*, 47(141), 141-168. <http://dx.doi.org/10.1177/0021943610364523>

Cranor, L. F., & Garfinkel, S. (2004). Secure or Usable? *Security & Privacy*, 2(5), 16-18. <http://dx.doi.org/10.1109/MSP.2004.69>

Cranor, L. F., & Garfinkel, S. (Eds.) (2005). *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly Media, Inc.

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Upper Saddle River, NJ: Pearson.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research*. (2nd ed.). Los Angeles, CA: SAGE Publications.

- Cribbin, T. (2011). Citation chain aggregation: An interaction model to support citation cycling. *CIKM '11 Proceedings of the 20th ACM International Conference on Information and Knowledge management* (pp. 2149-2152). <http://dx.doi.org/10.1145/2063576.2063913>
- D'Arcy, J. & Hovav, A. (2007). Deterring internal information systems misuse: Deterring employee intentions to misuse computer systems requires complementary technical and procedural controls. *Communications of the ACM*, 50(10), 113-117.
<http://dx.doi.org/10.1145/1290958.1290971>
- D'Arcy, J., Hovav, A., & Galleta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98. <http://dx.doi.org/10.1287/isre.1070.0160>
- Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. F. (2014). The tangled web of password reuse. *Proceedings of the NDSS*. <http://dx.doi.org/10.14722/ndss.2014.23357>
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
<http://dx.doi.org/10.1287/mnsc.35.8.982>
- Defense Information Systems Agency (DISA). (2010). *Our history: 2010s*. Retrieved from <http://www.disa.mil/About/Our-History/2010s>
- Defense Information Systems Agency. (2013). *Cyber awareness challenge v2.0* [Interactive computer-based training]. Retrieved from <http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>
- Department of Defense (DoD). (n.d.). *About the Department of Defense (DOD)*. Retrieved from <http://www.defense.gov/about/>

Department of Defense. (2014). *Cybersecurity*. DoD Instruction 8500.01. Washington, DC:

DoD. Retrieved from <http://www.dtic.mil/whs/directives/corres/ins1.html>

Department of Defense. (2007). *Information assurance training, certification, and workforce*

management. DoD Directive 8570.01. Washington, DC: DoD. Retrieved from

<http://www.dtic.mil/whs/directives/corres/dir.html>

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness

Computers & Security, 26(1), 73-80. <http://dx.doi.org/10.1016/j.cose.2006.10.009>

Eminağaoğlu, M. , Uçar, E., & Eren, S. (2009). The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*,

14(4), 223-220. <http://dx.doi.org/10.1016/j.istr.2010.05.002>

European Network and Information Security Agency (ENISA). (2007). *Information security*

awareness initiatives: Current practice and the measure of success. July 2007. Retrieved

from <http://www.itu.int/osg/csd/cybersecurity/WSIS/>

Federal Policy for the Protection of Human Subjects, 45 C.F.R. § 690 (1991). Retrieved from

<http://www.hhs.gov/ohrp/humansubjects/commonrule/>

Fay, M. J. (2011). Informal communication of co-workers: a thematic analysis of messages.

Qualitative Research in Organizations and Management, 6(3), 212-229.

<http://dx.doi.org/10.1108/17465641111188394>

Fink, A. (2009). *How to conduct surveys: A step-by-step guide* (4th ed.). Los Angeles: Sage.

Garamone, J. (2013). Defense contractors will share burdens of furloughs, Hagel says. *Armed*

Forces Press Service. Retrieved from

<http://www.defense.gov/news/newsarticle.aspx?id=120256>

- Gasser, M. (1988). *Building a Secure Computer System*. New York: Van Nostrand Reinhold.
Retrieved from <http://cs.unomaha.edu/~stanw/gasserbook.pdf>
- Gist, M. (1987). Self-efficacy: implications for organizational behavior and human resource management. *Academy of Management Review*, 12(3), 472–485.
<http://dx.doi.org/10.2307/258514>
- Godlove, T. (2012). Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective*, 21(4), 216-229. <http://dx.doi.org/10.1080/19393555.2012.668747>
- Goo, J., Yim, M-S., & Kim, D. J. (2013). A path way to successful management of individual intention to security compliance: A role of organizational security climate. *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS)*. (pp. 2959-2968). <http://dx.doi.org/10.1109/HICSS.2013.51>
- Goodman, L. A. (2011). Comment: On respondent-driven sampling and snowball sampling in hard-to-reach populations and snowball sampling not in hard-to-reach populations. *Sociological Methodology*, 41(1), 347-353. <http://dx.doi.org/10.1111/j.1467-9531.2011.01242.x>
- Hamburg, M. (1987). *Statistical analysis for decision making* (4th ed.). San Diego, CA: Harcourt Brace Jovanovich.
- Hamill, J. T., Deckro, R. F., & Kloeber, Jr., J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, 39, 463-484.
<http://dx.doi.org/10.1016/j.dss.2003.11.004>

- Haskins, C. (Ed.) (2011). *System engineering handbook* (Version 3.2.2). San Diego, CA: International Council on Systems Engineering (INCOSE). Retrieved from <http://www.incose.org/ProductsPubs/products/sehandbook.aspx>
- Heckathorn, D. D. (2011). Snowball versus respondent-driven sampling. *Sociological Methodology*, 41(1), 355-356. <http://dx.doi.org/10.1111/j.1467-9531.2011.01244.x>
- Heckle, R. R. (2011). Security dilemma: Healthcare clinicians at work. *Security & Privacy*, 9(6), 14-19. <http://dx.doi.org/10.1109/MSP.2011.74>
- Heckle, R. R., & Lutters, W. G. (2011). Tensions of network security and collaborative work practice: Understanding a single sign-on deployment in a regional hospital. *International Journal of Medical Informatics*, 80(8), e49-e61. <http://dx.doi.org/10.1016/j.ijmedinf.2011.02.001>
- Heckle, R., Lutters, W. G., & Gurzick, D. (2008). Network authentication using single sign-on: The challenge of aligning mental models. *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*, Article No. 6. <http://dx.doi.org/10.1145/1477973.1477982>
- Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. <http://dx.doi.org/10.1016/j.dss.2009.02.005>
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125. <http://dx.doi.org/10.1057/ejis.2009.6>

- Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 Workshop on New Security Paradigms*. (pp. 133-144). <http://dx.doi.org/10.1145/1719030.1719050>
- Hicks, L. (n.d. a). Informed consent - SBE. *Collaborative Institutional Training Initiative*. [Web-based computer-based training; member login required.] Retrieved from <https://www.citiprogram.org/>
- Hicks, L. (n.d. b). Privacy and confidentiality - SBE. *Collaborative Institutional Training Initiative*. [Web-based computer-based training; member login required.] Retrieved from <https://www.citiprogram.org/>
- ISACA (2012). *COBIT5: A business framework for the governance and management of enterprise IT*. Rolling Meadows, IL: ISACA. Retrieved from <http://www.isaca.org/cobit>
- ISO/IEC/IEEE. (2008). *Standard 15288: Systems and software engineering - system life cycle processes*. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers. ISO/IEC/IEEE 15288:2008 (E). Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=43564
- ISO/IEC/IEEE. (2010). *Standard 24765: Systems and software engineering - system and software engineering vocabulary (SEVocab)*. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE). ISO/IEC/IEEE 24765:2010. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50518

- Jaafar, N. I., & Ajis, A. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science*, 4(10), 118-130. Retrieved from <http://search.proquest.com/login/capitol-college.edu:2048/docview/1437608905?accountid=44888>
- Jenkins, J. L., Durcikova, A., & Burns, M. B. (2012). Forget the fluff: Examining how media richness influences the impact of information security training on secure behavior. *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS)* (pp. 3288-3296). <http://dx.doi.org/10.1109/HICSS.2012.285>
- Johnston, A., and Warkentin, M. (2010a). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566. Retrieved from <http://thecenter.uab.edu/media/2011/12/FEAR-APPEALS-AND-INFORMATION-SECURITY-BEHAVIORS-AN-EMPIRICAL-STUDY.pdf>
- Johnston, A. C., and Warkentin, M. (2010b). The influence of perceived source credibility on end-user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing* 22(3), 1-21. <http://dx.doi.org/10.4018/joeuc.2010070101>
- Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *The Journal of Computer Information Systems*, 53(2), pp. 22-30. Retrieved from <http://search.proquest.com/login/capitol-college.edu:2048/docview/1293109741?accountid=44888>
- Kabay, M. E. (2008). *The Parkerian hexad*. Northfield, VT: Norwich University. Retrieved from <http://www.mekabay.com/overviews/hexad.ppt>

- Kanusic, M. (2005). *Designing an effective survey* (CMU/SEI-2005-HB-004). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7277>
- Kennedy, D. P., Brown, R. A., Golinelli, D., Wenzel, S. L., Tucker, J. S., & Wertheimer, S. R. (2013). Masculinity and HIV risk among homeless men in Los Angeles. *Psychology of Men & Masculinity*, 14(2) 156-167. <http://dx.doi.org/10.1037/a0027570>
- Kim, P. (2010). *Measuring the effectiveness of information security training: a comparative analysis of computer-based training and instructor-based training* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses. (UMI 3425879) <http://search.proquest.com/login.capitol-college.edu:2048/docview/759244312/A2F2BDAAA54349E4PQ/1?accountid=44888>
- Kissel, R. (Ed.) (2013). *Glossary of key information security terms, NISTIR 7298 Rev. 2*. Bethesda, MD: National Institute of Standards & Technology (NIST). Retrieved from <http://csrc.nist.gov/publications/PubsNISTIRs.html>
- Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33, 3-11. <http://dx.doi.org/10.1016/j.cose.2012.07.001>
- Koppel, R., Wetterneck, T., Telles, J. L., & Karsh, B. (2008). Workarounds to barcode medication administration systems: Their occurrences, causes, and threats to patient safety. *Journal of the American Medical Informatics Association*, 15(4), 408-423. <http://dx.doi.org/10.1197/jamia.M2616>

- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38, 143-154. <http://dx.doi.org/10.1016/j.apergo.2006.03.010>
- Kruck, S. E., & Teer, F. P. (2008). Computer security practices and perceptions of the next generation of corporate computer users. *International Journal of Information Security and Privacy*, 2(1), 80-90. Retrieved from <http://search.proquest.com/login/capitol-college.edu:2048/docview/223743170?accountid=44888>
- Kruck, S. E., & Teer, F. P. (2010). Computer security practices and perceptions of the next generation of corporate computer users. In H. R. Nemati (Ed.), *Pervasive Information Security and Privacy Developments: Trends and Advancements* (pp. 255-265). IGI Global. <http://dx.doi.org/10.4018/978-1-61692-000-5.ch017> [Extract retrieved from <http://books.google.com>]
- Kumaraguru, O., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 7:1-7:31. <http://doi.acm.org/10.1145/1754393.1754396>
- LaRosa, L. A., Fishman, N. O., Lautenbach, E., Koppel, R., Morales, K. H., Linkin, D. R. (2007). Evaluation of antimicrobial therapy orders circumventing an antimicrobial stewardship program: Investigating the strategy of “stealth dosing.” *Infection Control and Hospital Epidemiology*, 28(5), 551-556. <http://dx.doi.org/10.1086/513535>
- Lebek, B. Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS)*. (pp. 2978-2987). <http://dx.doi.org/10.1109/HICSS.2013.192>

- Lomo-David, E. & Shannon, L. (2009). Information systems security and safety measures: The dichotomy between students' familiarity and practice. *Academy of Information and Management Sciences Journal*, 12(1), 2009, 29-47. Retrieved from <http://www.proquest.com> [ProQuest document ID 214623612]
<http://search.proquest.com/login/capitol-college.edu:2048/docview/214623612/B9D2818E76FD4EB8PQ/1?accountid=44888>
- Martinez, A. (n.d.). Internet research - SBE. *Collaborative Institutional Training Initiative*. [Web-based computer-based training; member login required.] Retrieved from <https://www.citiprogram.org/>
- Mazzola, J. J., Walker, E. J., Shockley, K. M., and Spector, P. E. (2011). Examining stress in graduate assistants: Combining qualitative and quantitative survey methods. *Journal of Mixed Methods Research*, 5(3), 198-211. <http://dx.doi.org/10.1177/1558689811402086>
- Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91-116. Retrieved from <http://search.proquest.com/login/capitol-college.edu:2048/docview/886806258/F7AADCB97BAB4329PQ/1?accountid=44888>
- MITRE Corporation (2012). *Systems engineering guide* (Version 1.0) [ePub version]. Bedford MA: The MITRE Corporation. Retrieved from <http://www.mitre.org/publications/systems-engineering-guide/systems-engineering-guide>
- Moertl, P., & Scott, S. (2012). *Survey design in systems engineering - TSE228*. McLean, VA: The MITRE Institute.
- Moertl, P., & Scott, S. (2014). *Recommended practices for the development of surveys: A guidebook for systems engineers*. McLean, VA: The MITRE Corporation.

- Myers, M. M., and Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and Organization*, 17(1), 2-26.
<http://dx.doi.org/10.1016/j.infoandorg.2006.11.001> Retrieved from
<http://www.academia.edu/957291/> [Free registration required]
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34. 47-66.
<http://dx.doi.org/10.1016/j.cose.2012.11.004>
- National Institute of Standards & Technology (NIST). (2014). *Framework for improving critical infrastructure cybersecurity*. Retrieved from <http://www.nist.gov/cyberframework/>
- National Security Agency (NSA) (2002). *Information assurance technical framework*, release 3.1. Ft. Meade, MD: National Security Agency. Retrieved from
<https://www.iad.gov/iad/documents.cfm?zBI+E5+sBQ8I785Hms9M3TTGZMqX89HtgARktF8oEX0=>
- Ng'ambi, D., & Brown, I. (2009). Intended and unintended consequences of student use of an online questioning environment. *British Journal of Educational Technology*, 40(2). 316-328. <http://dx.doi.org/10.1111/j.1467-8535.2008.00899.x>
- Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modelling [*sic*]. *International Journal of Information Security and Privacy*, 3(1). 11-29. Retrieved from
<http://search.proquest.com/login.capitol-college.edu:2048/docview/223741891?accountid=44888>
- Office of Personnel Management (OPM). (2009). *Handbook of occupational groups and families*. Washington, DC: OPM. Retrieved from <http://www.opm.gov/policy-data->

[oversight/classification-qualifications/classifying-general-schedule-positions/occupationalhandbook.pdf](#)

Parker, D. B. (1998). *Fighting computer crime*. New York, NY: John Wiley & Sons. ISBN 0-471-16378-3.

Parker, D. B. (2002). Toward a new framework for information security, in Bosworth, S., & Kabay, M. E.. *The computer security handbook* (4th ed.). New York, NY: John Wiley & Sons. ISBN 0-471-41258-9. Retrieved from <http://www.computersecurityhandbook.com/csh4/chapter5.html>

Pashler, H., Rohrer, D., & Harris, C. R. (2013). Can the goal of honesty be primed? *Journal of Experimental Social Psychology*, 49(6), 959-964. <http://dx.doi.org/10.1016/j.jesp.2013.05.011>

Pastor, V., Diaz, G., & Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. *Education Engineering (EDUCON) 2010 IEEE*, 1907-1916. <http://dx.doi.org/10.1109/EDUCON.2010.5492435>

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4). 597-611. <http://dx.doi.org/10.1016/j.cose.2011.12.010>

Pittman, J. M. (2014a). Pilot study design and implementation. *RSC 812 Professional Research Theory & Practice II*. Lecture conducted from Capitol College, Laurel, MD.

Pittman, J. M. (2014b). Variable types and Likert scales. *RSC 812 Professional Research Theory & Practice II*. Lecture conducted from Capitol College, Laurel, MD.

Policy (n.d.). In *Merriam-Webster online dictionary*. Retrieved from <http://www.merriam-webster.com/dictionary/policy>

- Procedure (n.d.). In *Merriam-Webster online dictionary*. Retrieved from <http://www.merriam-webster.com/dictionary/procedure>
- Publish (n.d.). In *Merriam-Webster online dictionary*. Retrieved from <http://www.merriam-webster.com/dictionary/publish>
- Puhakainen, P. & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-A4. Retrieved from <http://misq.org/improving-employees-compliance-through-information-systems-security-training-an-action-research-study.html>
- Pyster, A. & Olwell, D. (Eds). (2013). *Guide to the systems engineering body of knowledge (SEBoK)*, v. 1.2. Hoboken, NJ: The Trustees of the Stevens Institute of Technology. Retrieved from [http://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_\(SEBoK\)](http://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK))
- Rhee, H-S., Ryu, Y. U., & Kim, C-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232. <http://dx.doi.org/10.1016/j.cose.2011.12.001>
- Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114. <http://dx.doi.org/10.1080/00223980.1975.9915803>
- Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: J. Cacioppo and R. Petty, eds. *Social psychophysiology*. NY: Guilford Press, 153–176. As cited in Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat

- control model of information systems security behaviours. *Behaviour & Information Technology*, 28(6). 563–575. <http://dx.doi.org/10.1080/01449290802556021>
- Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field Methods*, 15(1), 85-109. <http://dx.doi.org/10.1177/1525822X02239569> Retrieved from <http://crlte.engin.umich.edu/wp-content/uploads/sites/7/2013/06/Ryan-and-Bernard-Techniques-to-Identify-Themes.pdf>
- Salkind, N. J. (2012). *Exploring Research* (8th ed.). Boston, MA: Pearson.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3). 122-131. <http://dx.doi.org/10.1023/A:1011902718709> Retrieved from http://hornbeam.cs.ucl.ac.uk/hcs/publications/Sasse+Brostoff+Weirich_Transforming_the_weakest_link_Technology_Journal2001.pdf
- Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor & S. Garfinkel (Eds.) (2005). *Security and usability: Designing secure systems that people can use* (pp. 13-30). Sebastopol, CA: O'Reilly Media, Inc.
- Schneier, B. (2000). *Secrets & lies: Digital security in a networked world*. New York: John Wiley & Sons, Inc.
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education* 52(1), 92-100. <http://dx.doi.org/10.1016/j.compedu.2008.06.011>
- Sheng, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006). *Why Johnny still can't encrypt: Evaluating the usability of email encryption software*. Paper presented at the poster

session of the second Symposium On Usable Privacy and Security, Pittsburgh, PA.

Retrieved from <http://cups.cs.cmu.edu/soups/2006/program.html - posters>

Shoemaker, D., & Conklin, W. A. (2012). *Cybersecurity: The essential body of knowledge*.

Boston, MA: Course Technology Cengage Learning.

Shropshire, J. D. (2008). *Predicting compliance with prescribed organizational information security protocols* (Doctoral dissertation). Retrieved from ProQuest Dissertations &

Theses (UMI 3331297). <http://search.proquest.com/login/capitol-college.edu:2048/docview/304515111/E4E72CE0C48A40C5PQ/1?accountid=44888>

Sim, I., Liginlal, D., & Khansa, L. (2012). Information privacy situation awareness: Construct and validation. *The Journal of Computer Information Systems*, 53(1), 57-64. Retrieved

from ProQuest (Document ID 1231586958). <http://search.proquest.com/login/capitol-college.edu:2048/docview/1231586958/B0EEA6CE75724B7CPQ/1?accountid=44888>

Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64-71.

<http://dx.doi.org/10.1109/MC.2010.35>

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24, 124-133.

<http://dx.doi.org/doi:10.1016/j.cose.2004.07.001>

SurveyMonkey. (2013a). *Privacy policy*. Retrieved from

<https://www.surveymonkey.com/mp/policy/privacy-policy/>

SurveyMonkey. (2013b). *Security statement*. Retrieved from

<https://www.surveymonkey.com/mp/policy/security/>

SurveyMonkey. (2014). *Making surveys anonymous*. Retrieved from

http://help.surveymonkey.com/articles/en_US/kb/How-do-I-make-surveys-anonymous

Susarapu, S. R. (2012). *Aligning security and usability objectives for computer based*

information systems (Doctoral dissertation). Retrieved from ProQuest Dissertations and

Theses. (UMI 3542940) <http://search.proquest.com/login/capitol->

college.edu:2048/docview/1170997543/EE1A3F7480744CB9PQ/1?accountid=44888

Systems Engineering Body of Knowledge (SEBoK) Authors (2013). Systems engineering

overview. In Pyster, A. & Olwell, D. (Eds). (2013). *Guide to the systems engineering*

body of knowledge (SEBoK), v. 1.2. Hoboken, NJ: The Trustees of the Stevens Institute

of Technology. Retrieved from

http://www.sebokwiki.org/wiki/Systems_Engineering_Overview

Teer, F., Kruck, S., & Kruck, G. (2007). Empirical [*sic*] study of students' computer security

practices/perceptions. *Journal of Computer Information Systems*, Spring 2007, pp. 105-

110. Retrieved from <http://search.proquest.com/login/capitol->

college.edu:2048/docview/232583860?accountid=44888

Tipton, H. F. (Ed.) (2010). *Official (ISC)²® guide to the CISSP® CBK®* 2nd ed. Boca Raton,

FL: CRC Press.

Torkzadeh, R., Pflughoeft, K., & Hall, L. (1999). Computer self-efficacy, training effectiveness

and user attitudes: an empirical study. *Behaviour and Information Technology*, 18(4),

299–309. <http://dx.doi.org/10.1080/014492999119039>

Uffen, J. & Breitner, M. H. (2013). Management of technical security measures: An empirical

examination of personality traits and behavioral intentions. *Proceedings of the 46th*

Hawaii International Conference on System Sciences (HICSS). (pp. 4551-4560)

<http://dx.doi.org/10.1109/HICSS.2013.388>

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*.

15(3), 320-330. <http://dx.doi.org/10.1057/palgrave.ejis.3000589>

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20, 267-284.

<http://dx.doi.org/10.1057/ejis.2010.72>

Whitten, A., & Tygar, J. D. (1999). *Why Johnny can't encrypt: A usability evaluation of PGP 5.0*. Proceedings of the 8th USENIX Security Symposium, 169-184. Reprinted in L. F. Cranor & S. Garfinkel (Eds.) (2005), *Security and usability: Designing secure systems that people can use* (pp. 669-692). Sebastopol, CA: O'Reilly Media, Inc.

Wirtz, J. & Bateson, J. E. G. (1995). An experimental investigation of halo effects in satisfaction measures of service attributes. *International Journal of Service Industry Management*, 6(3). 84-92. Retrieved from ProQuest (Document ID 233643904).

<http://search.proquest.com/login.capitol-college.edu:2048/docview/233643904/D3B864FAFC9D4CD7PQ/1?accountid=44888>

Workman, M., Bommer, W.H., & Straub, D. (2008). Security lapses and the omission of information security measures: an empirical test of the threat control model. *Journal of Computers in Human Behavior*, 24(6), 2799-2816.

<http://dx.doi.org/10.1016/j.chb.2008.04.005>

Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour*

& Information Technology, 28(6). 563–575.

<http://dx.doi.org/10.1080/01449290802556021>

Yang, Z., Ng, B.-Y., Kankanhalli, A., & Yip, J. W. L. (2012). Workarounds in the use of IS in healthcare: A case study of an electronic medication administration system. *International Journal of Human-Computer Studies*, 70(1), 43-65.

<http://dx.doi.org/10.1016/j.ijhcs.2011.08.002>

Yu, S. (2012). College students' justification for digital piracy: A mixed methods study. *Journal of Mixed Methods Research*, 6(4), 364-378. <http://dx.doi.org/10.1177/1558689812451790>

Zafar, S. U. (2012). *Data analysis for engineers & scientists- TSE534*. McLean, VA: The MITRE Institute.

APPENDIX A: IA TRAINING CONTENT

The figures below illustrate the training content in *Cyber Awareness Challenge* (DISA, 2013), the information assurance awareness training developed by the Defense Information Assurance Agency (DISA) for the U.S. Department of Defense (DoD). DISA offers variant versions for DoD employees, federal employees, and intelligence community employees. The figures here are from the DoD employee version, however, the core guidance on IA practices is identical across the three versions. The *Cyber Awareness Challenge* is available to the general public online. All figures here were obtained by screen capture while taking the training. While survey questions derive from only eight of the figures (See Appendix B), the entire set of images is presented in order to preserve the point-in-time content of the course, which is updated annually. Future researchers building on the results of the described study may find it beneficial to refer to the entire set, or selected guidance not addressed explicitly in the survey instrument.



Figure A1. Contents of Cyber Awareness Challenge by major topic.



Figure A2. Guidelines for using computer ethically.

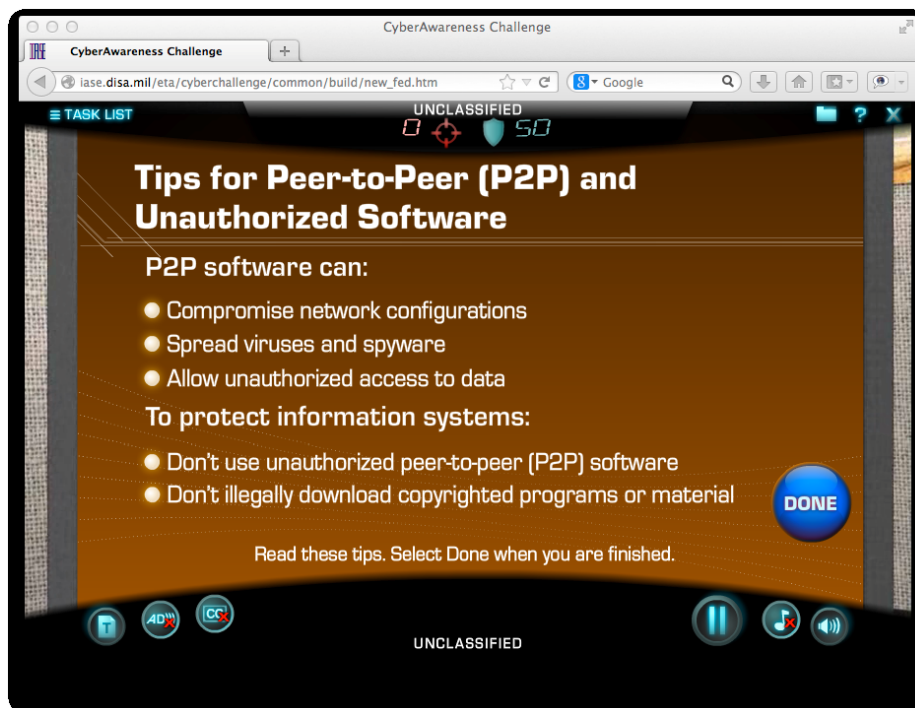


Figure A3. Tips for peer-to-peer (P2P) and unauthorized software.

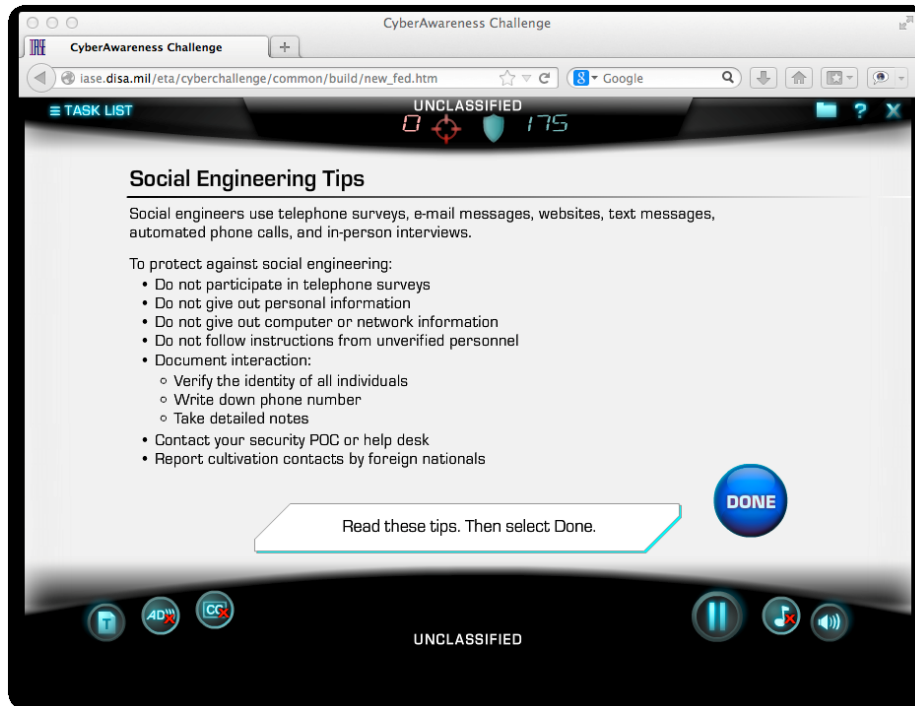


Figure A4. Social engineering tips.



Figure A5. Password tips.



Figure A6. Password tips, 2.

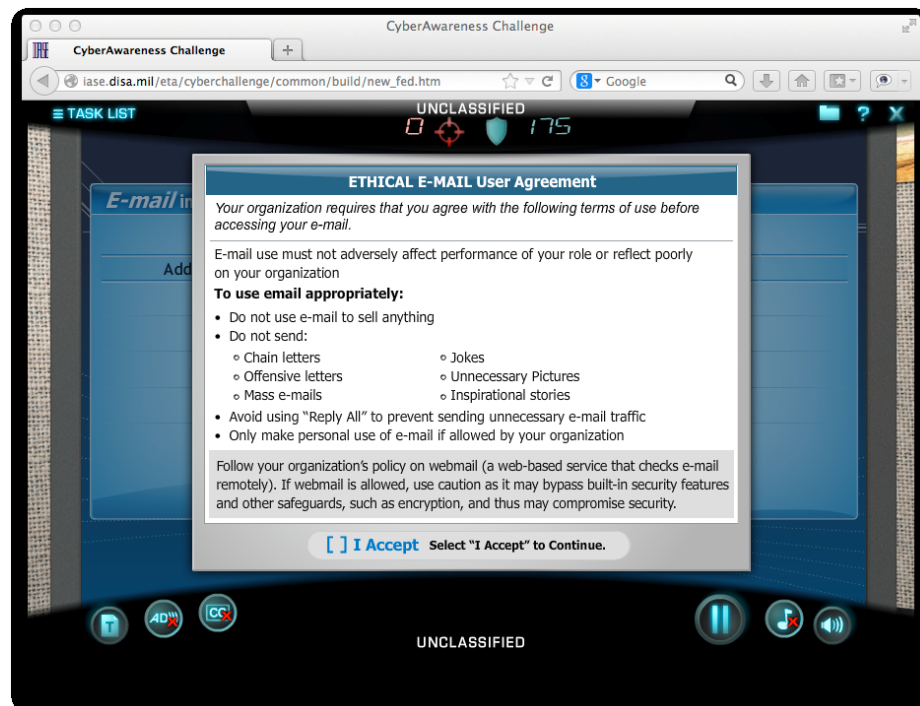


Figure A7. Ethical e-mail user agreement.



Figure A8. Tips about phishing: a type of social engineering. Phishing attempts use suspicious e-mails or pop-ups.



Figure A9. Tips about phishing: a type of social engineering. To protect against phishing.

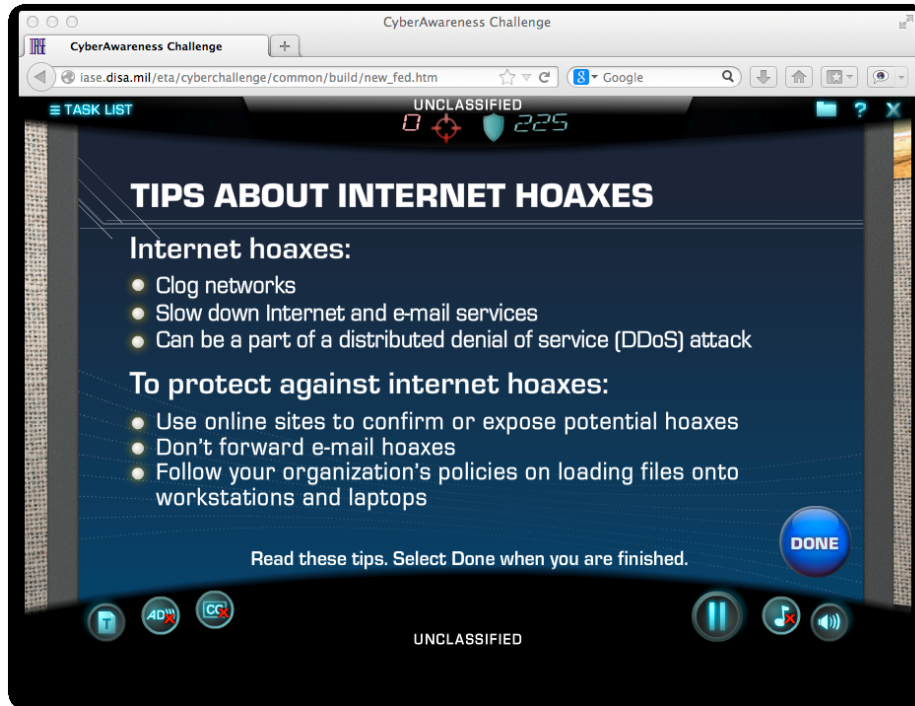


Figure A10. Tips about internet hoaxes.



Figure A11. Tips about spear phishing

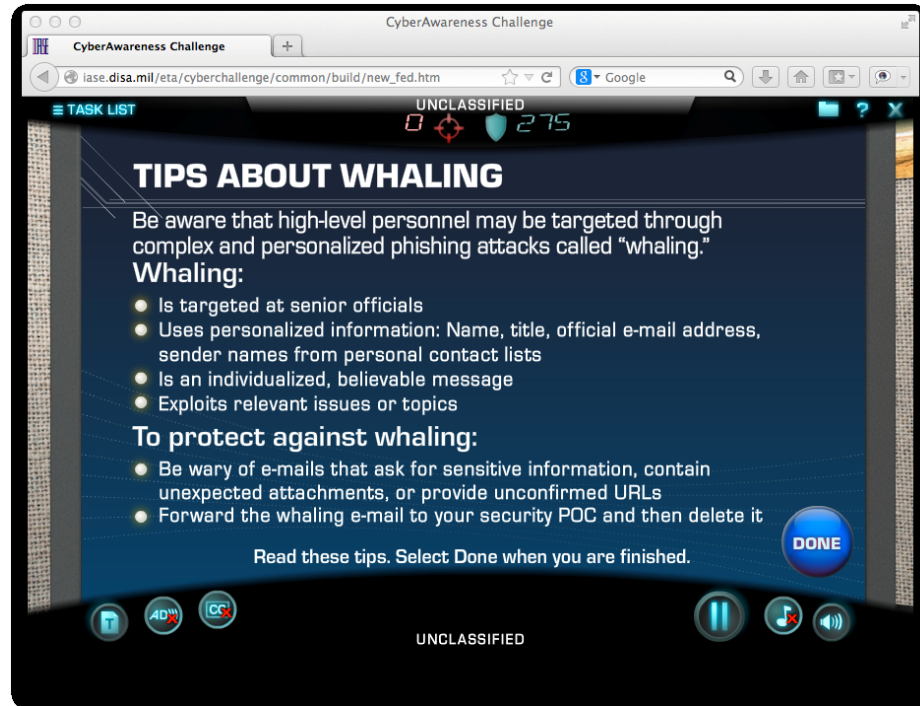


Figure A12. Tips about whaling.

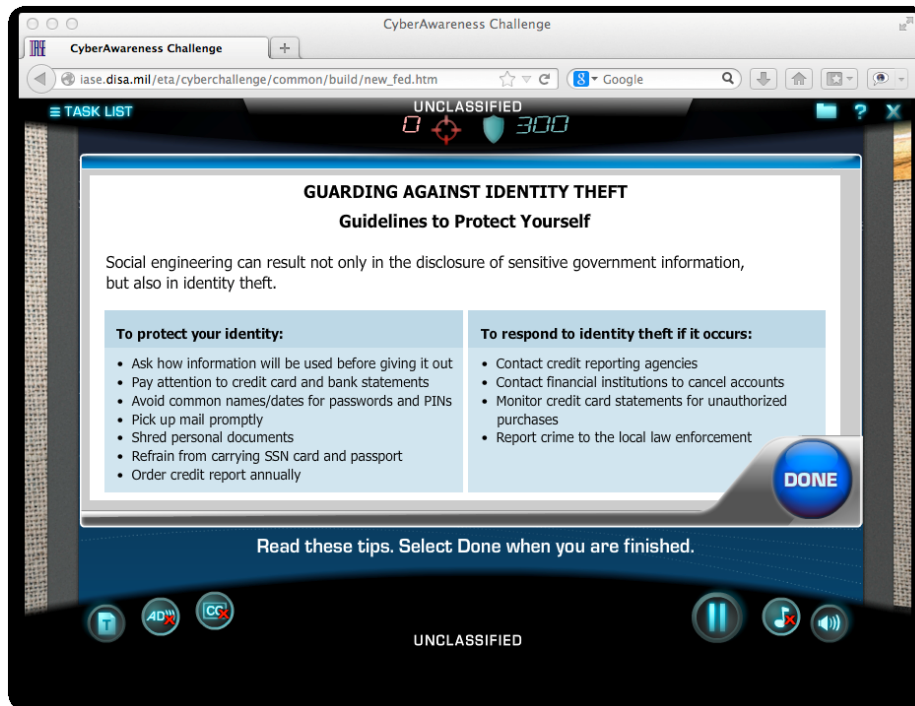


Figure A13. Guarding against identity theft. Guidelines to protect yourself.

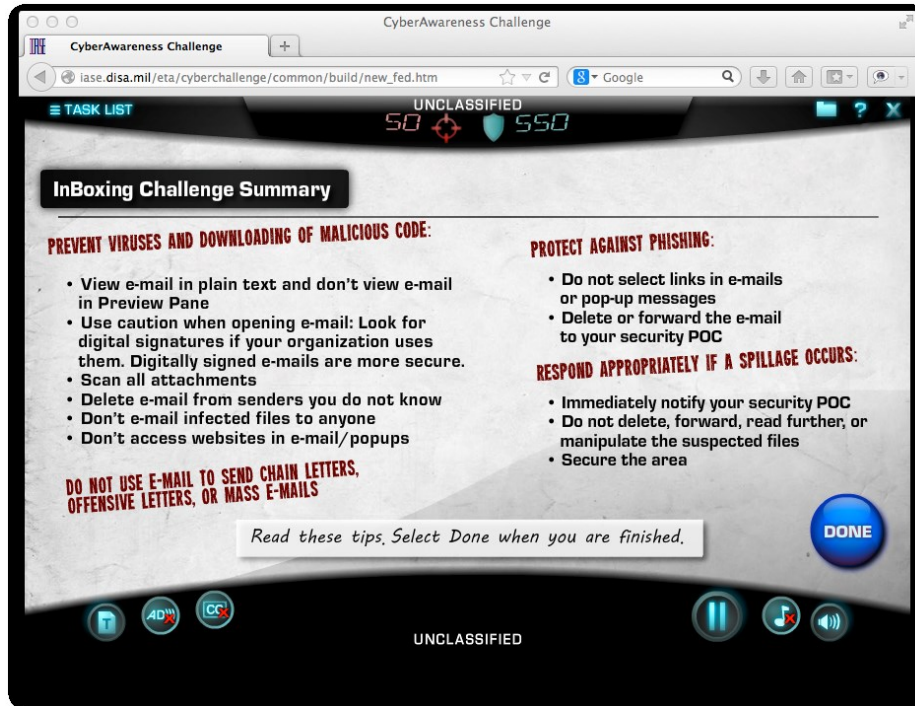


Figure A14. Summary of security advice for e-mail.

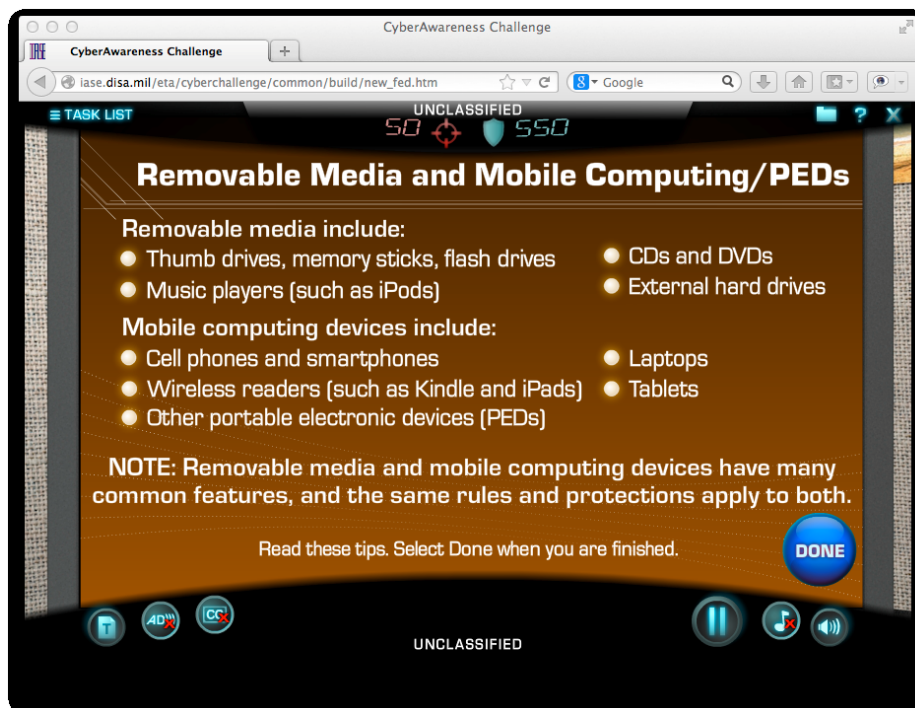


Figure A15. Removable media and mobile computing/PEDs.

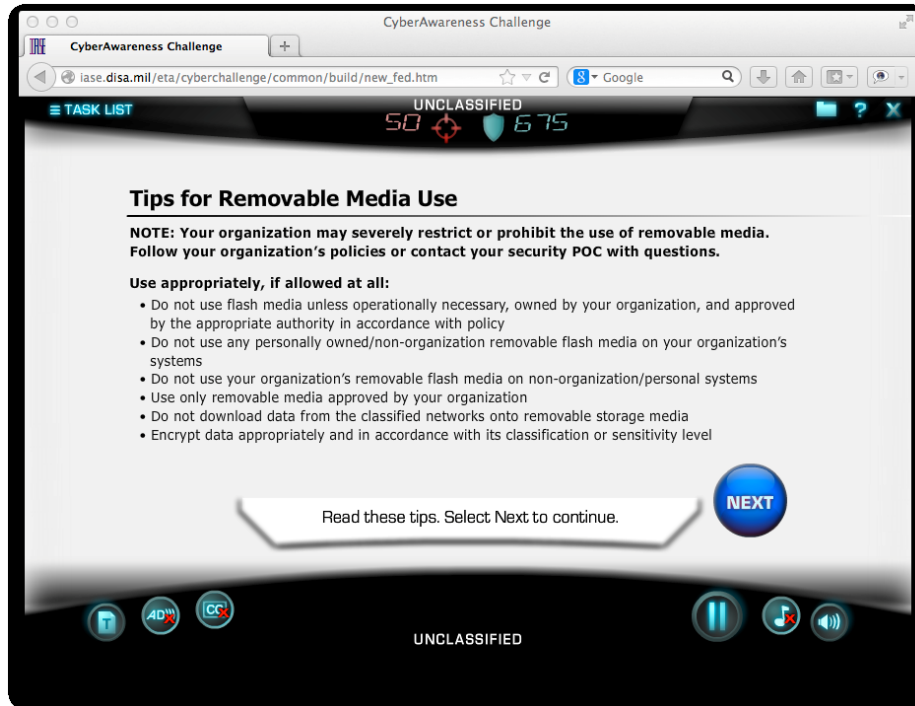


Figure A16. Tips for removable media use.

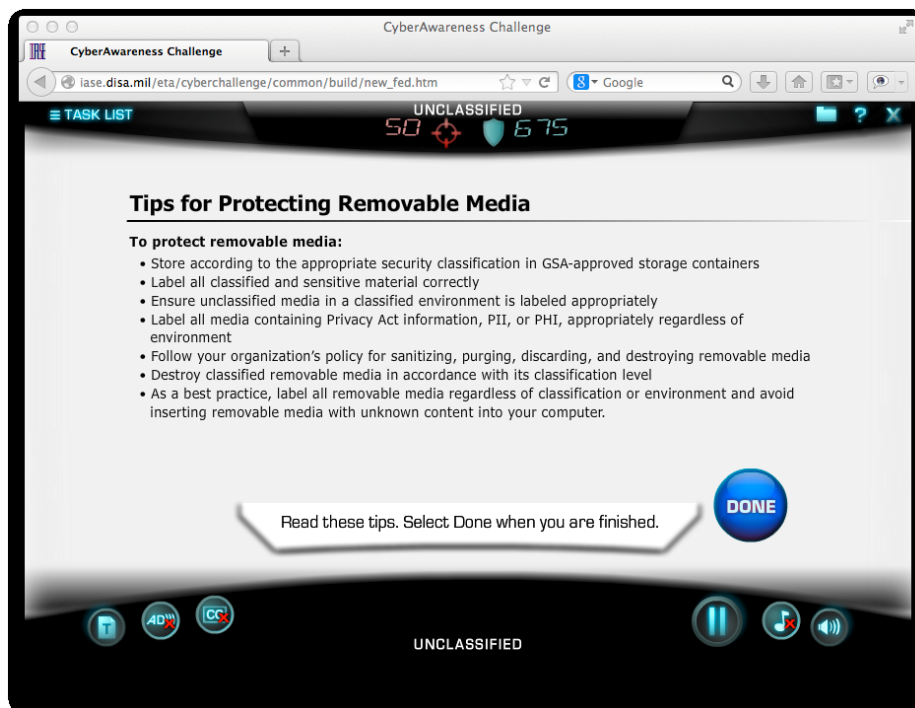


Figure A17. To protect removable media.

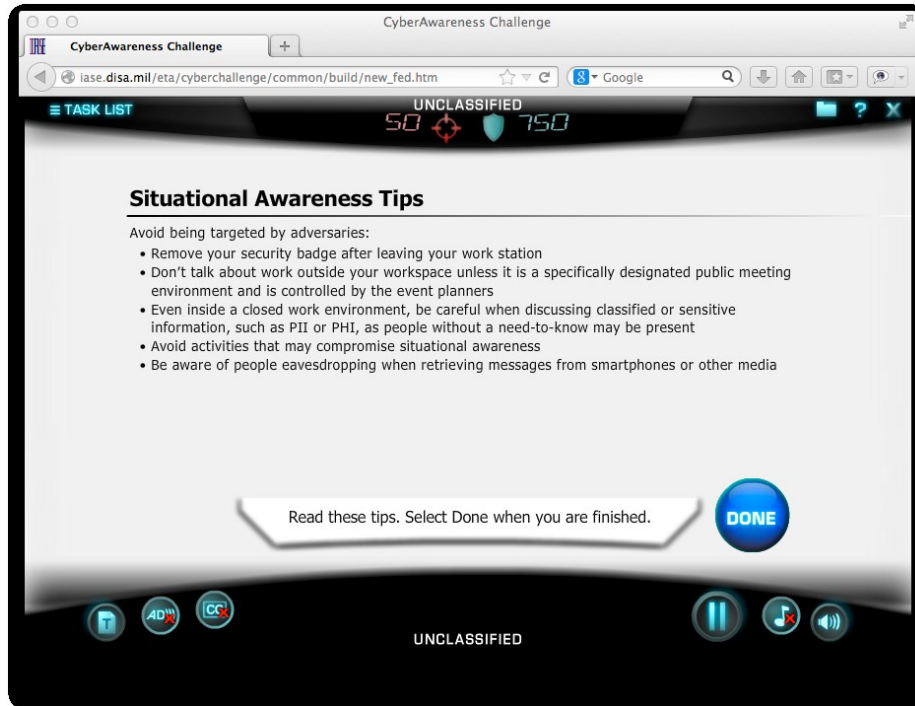


Figure A18. Situational awareness tips.

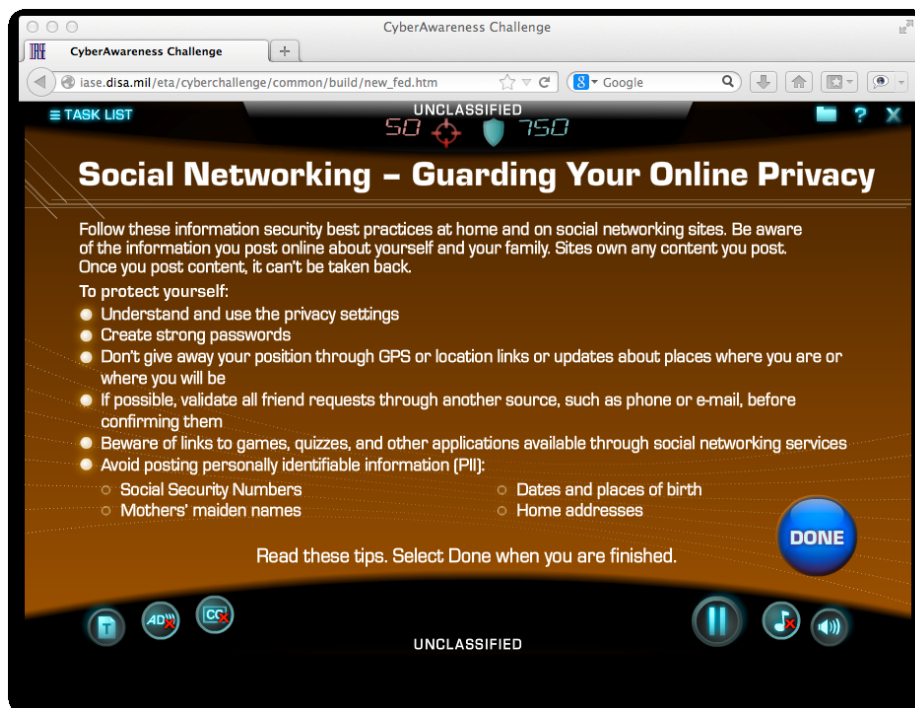


Figure A19. Social networking - guarding your online privacy.



Figure A20. Social networking tips - protecting your organization.

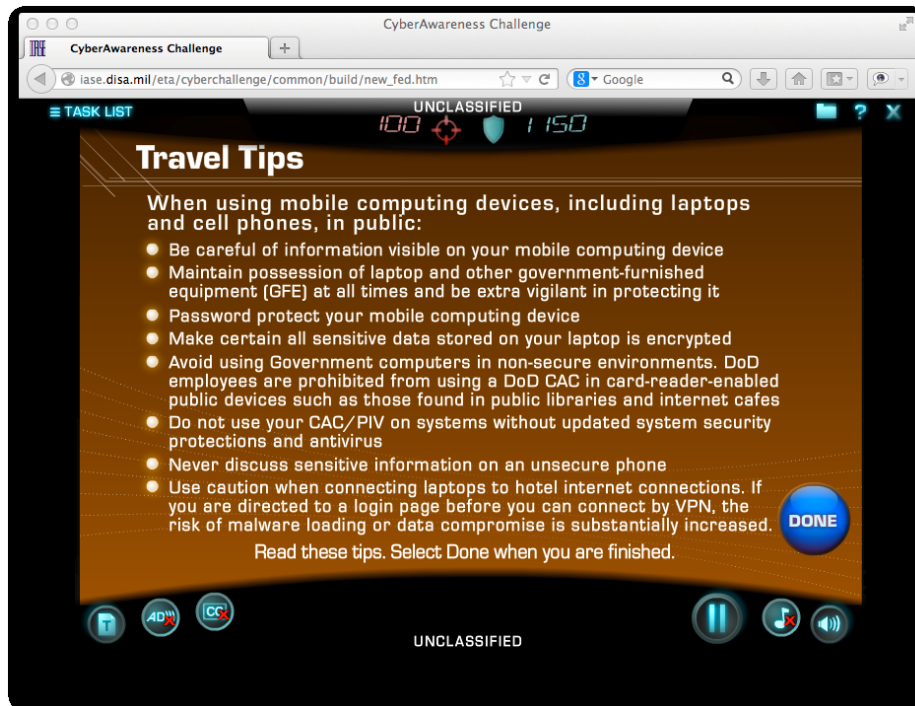


Figure A21. Travel tips, when using mobile computing devices in public.

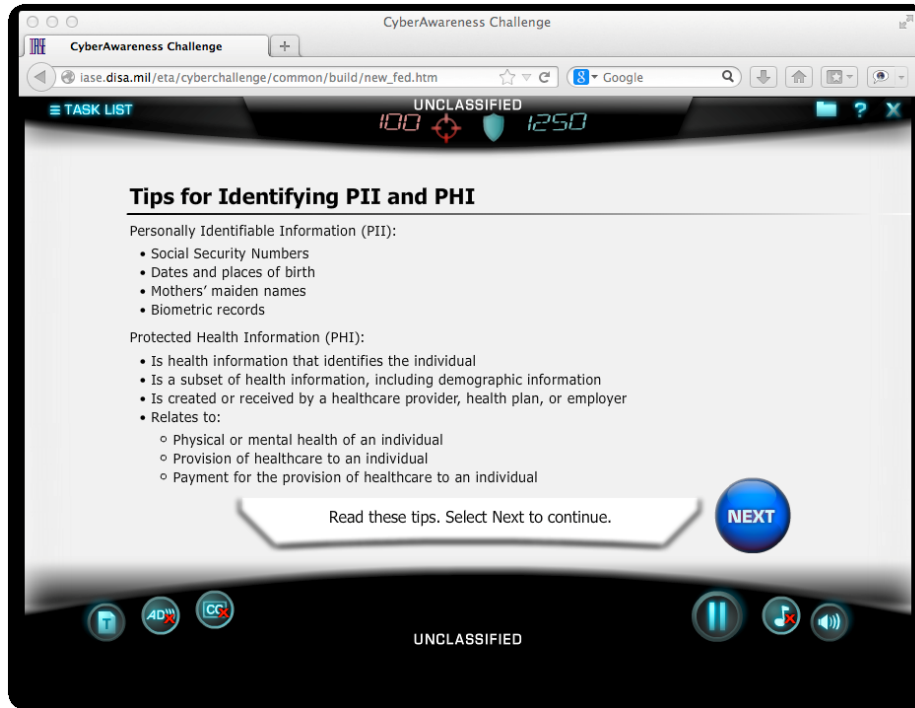


Figure A22. Tips for identifying personal identity information (PII) and personal health information (PHI).

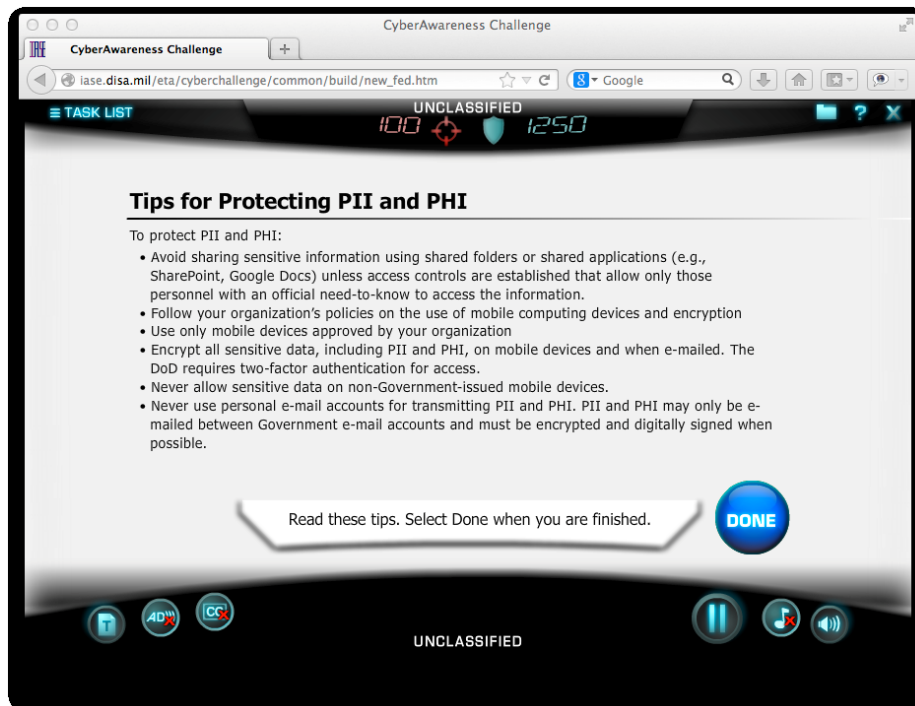


Figure A23. Tips for protecting personal identity information (PII) and personal health information (PHI).

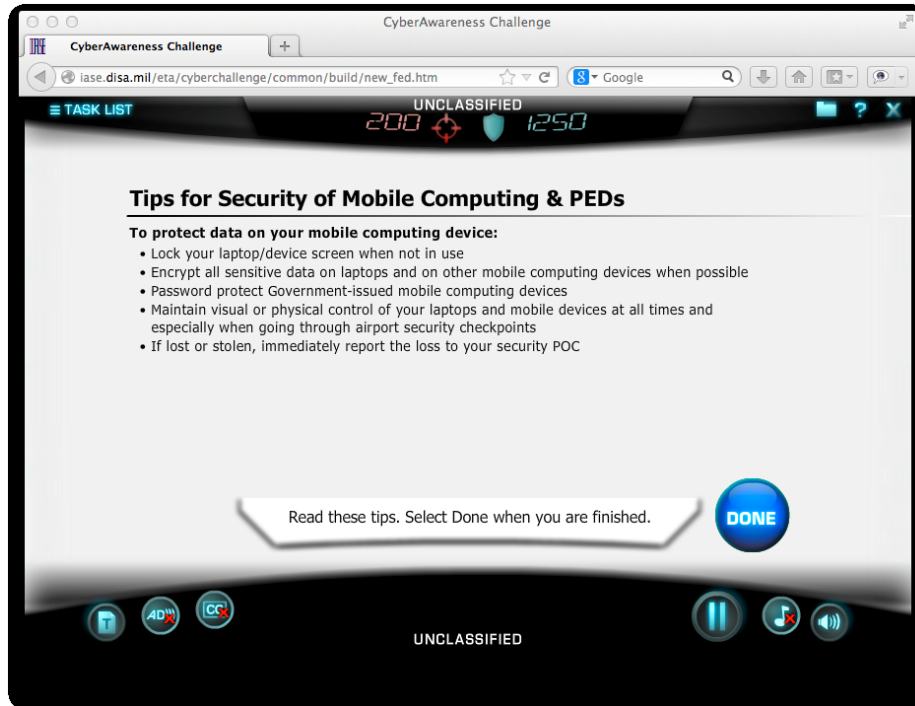


Figure A24. Tips for security of mobile computing and PEDs.

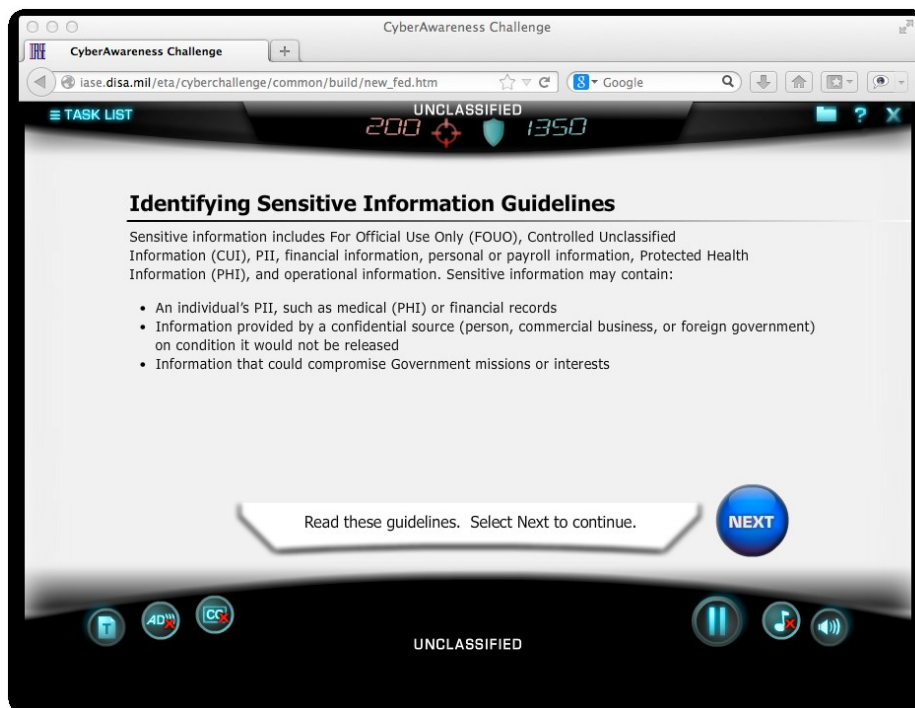


Figure A25. Guidelines for identifying sensitive information.

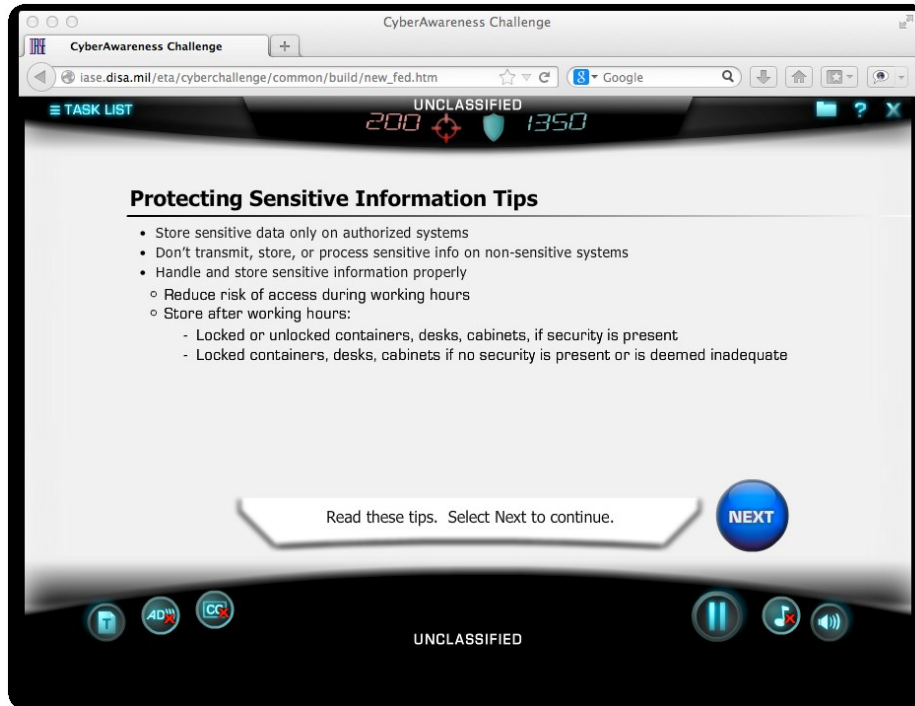


Figure A26. Protecting sensitive information.

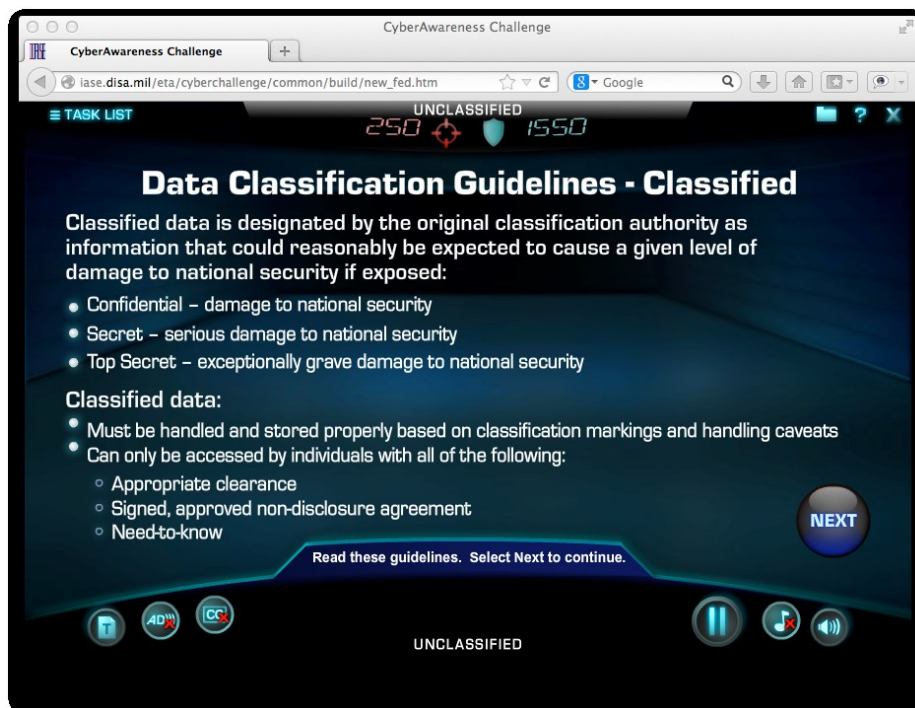


Figure A27. Data classification guidelines for classified information.

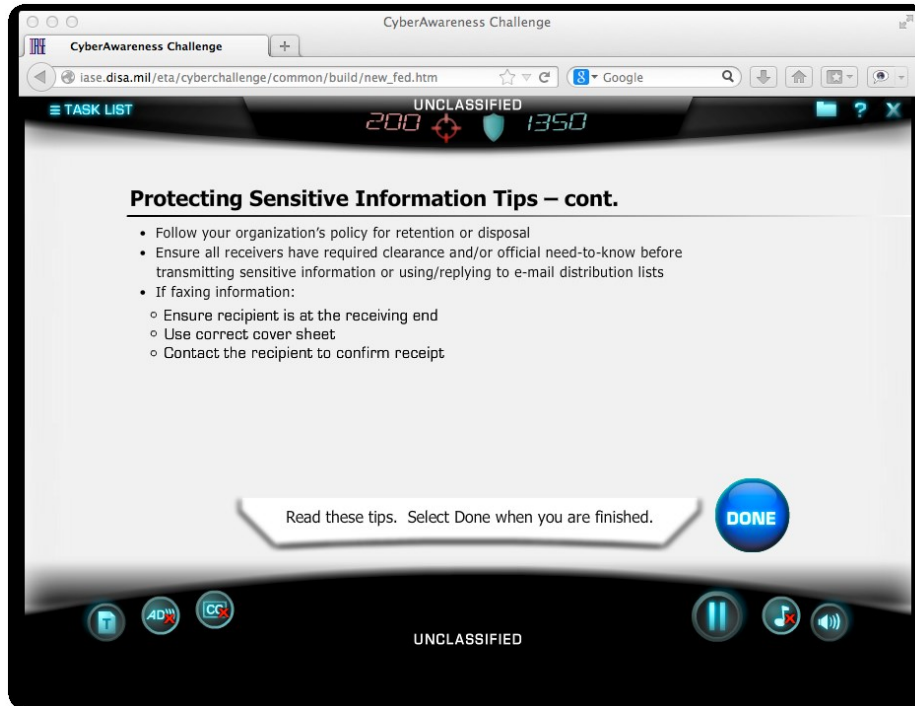


Figure A28. Protecting sensitive information, continued.

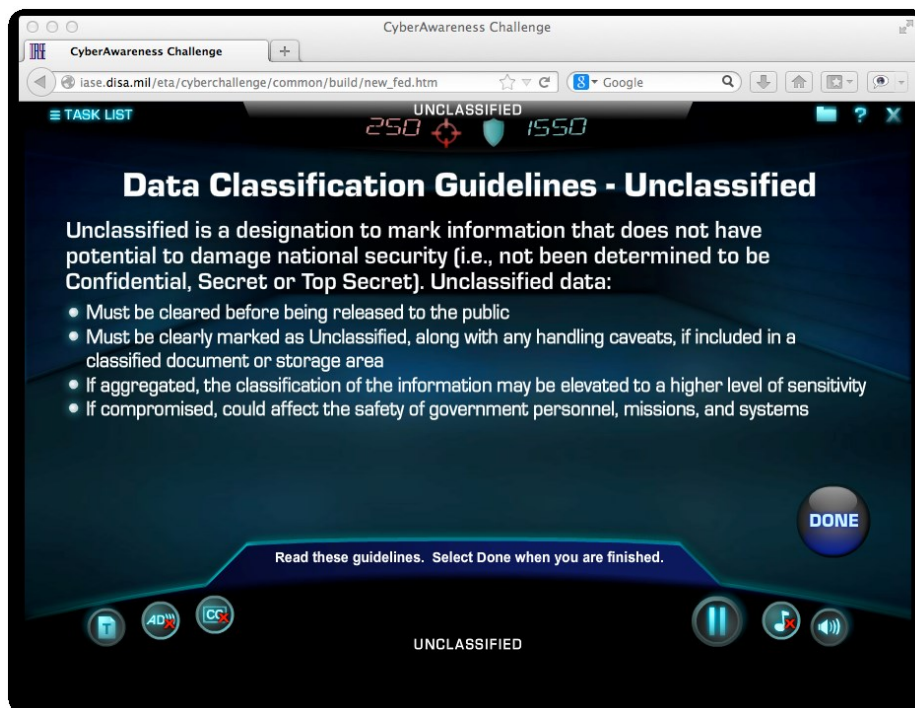


Figure A29. Data classification guidelines - Unclassified.

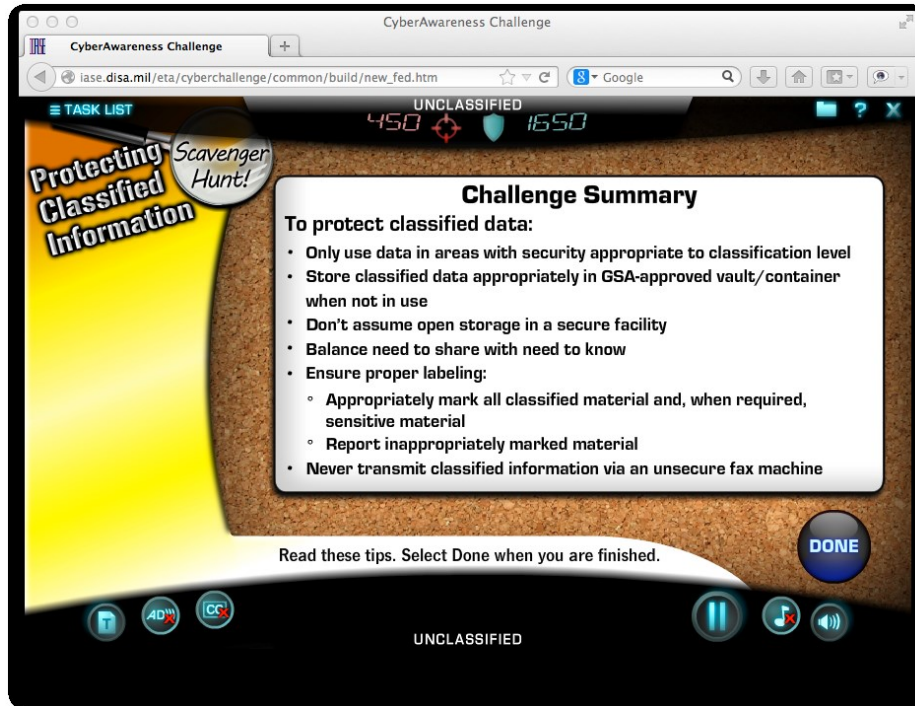


Figure A30. To protect classified data - summary.

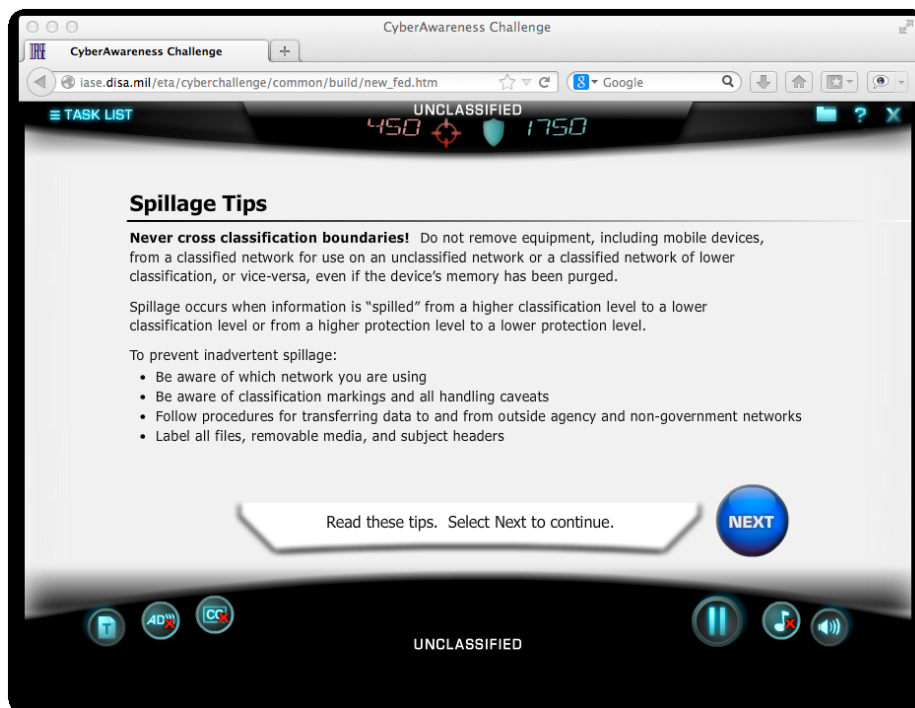


Figure A31. Spillage tips.

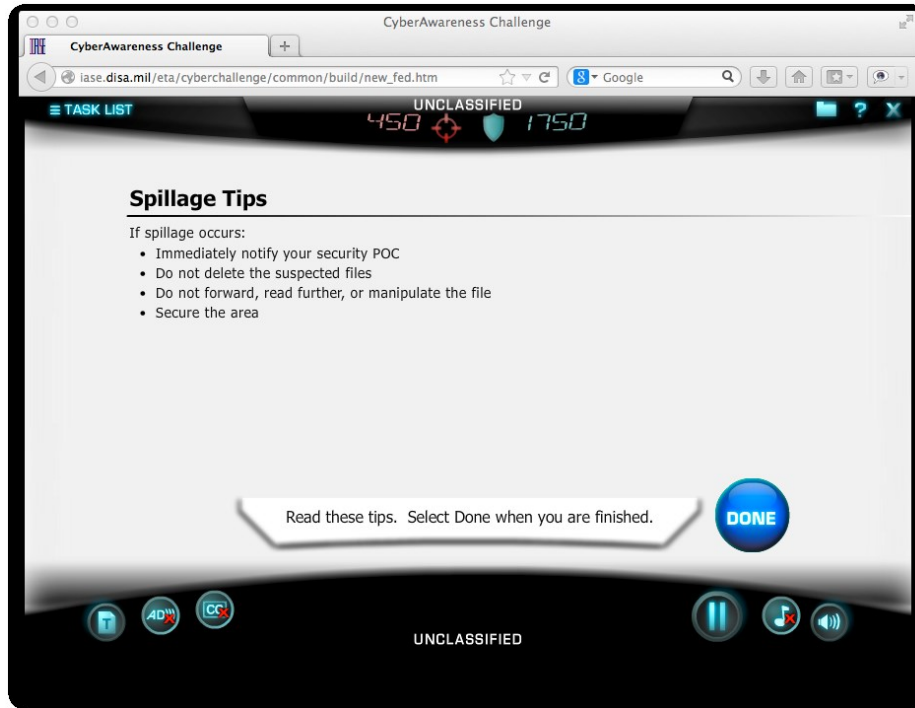


Figure A32. Spillage tips - if a spillage occurs.

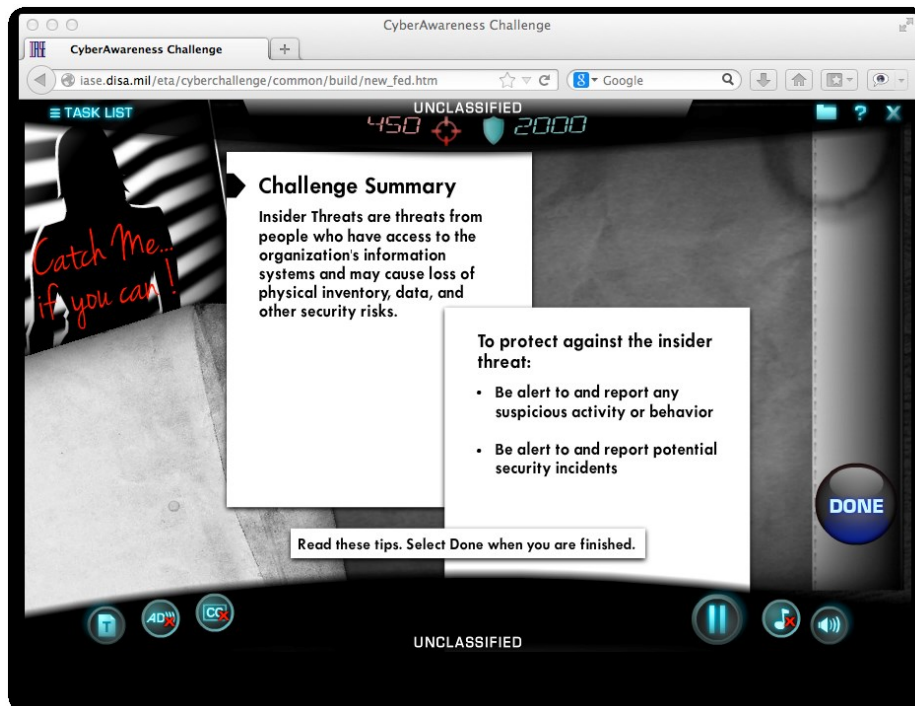


Figure A33. To protect against the insider threat.

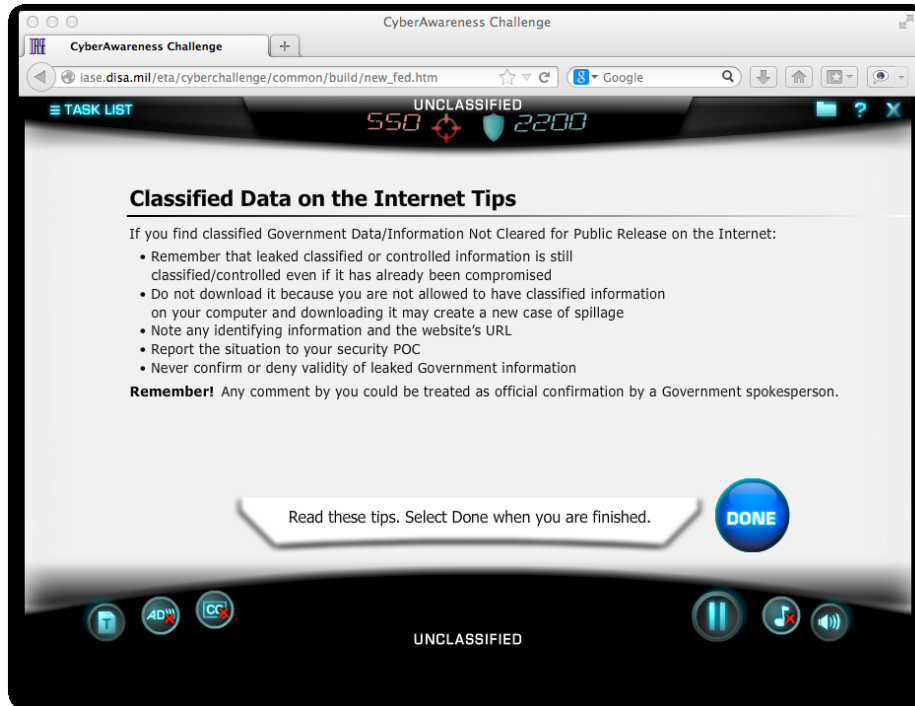


Figure A34. Classified data on the Internet tips.

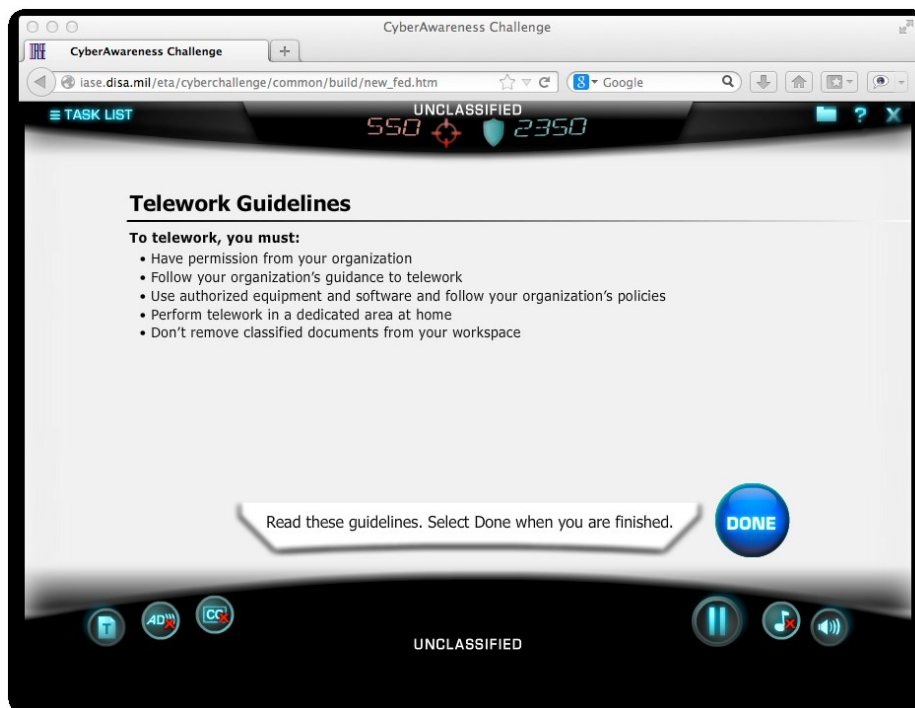


Figure A35. Telework guidelines.

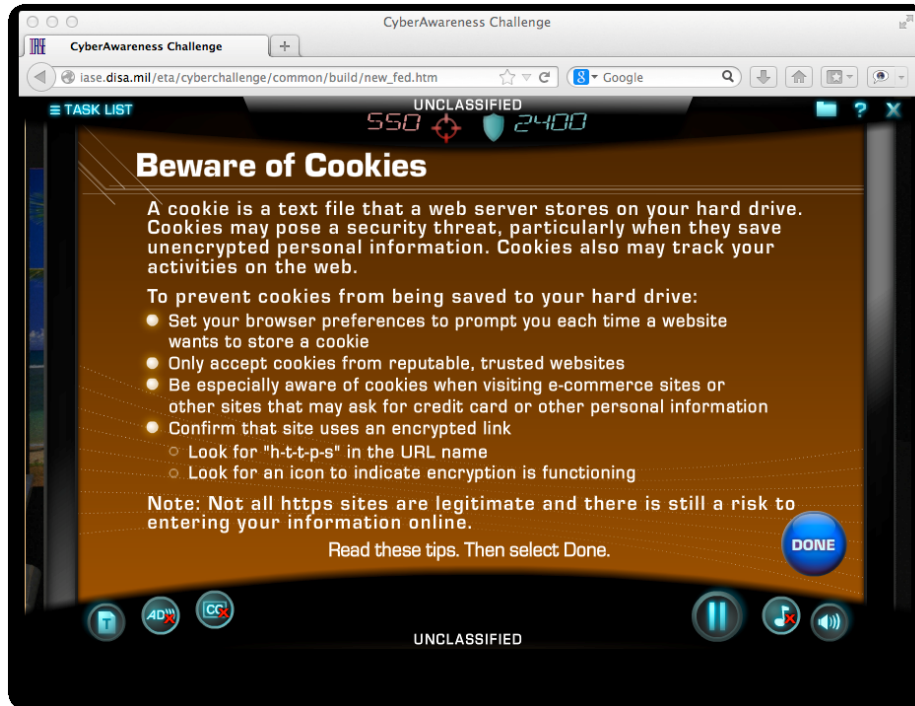


Figure A36. Beware of cookies.

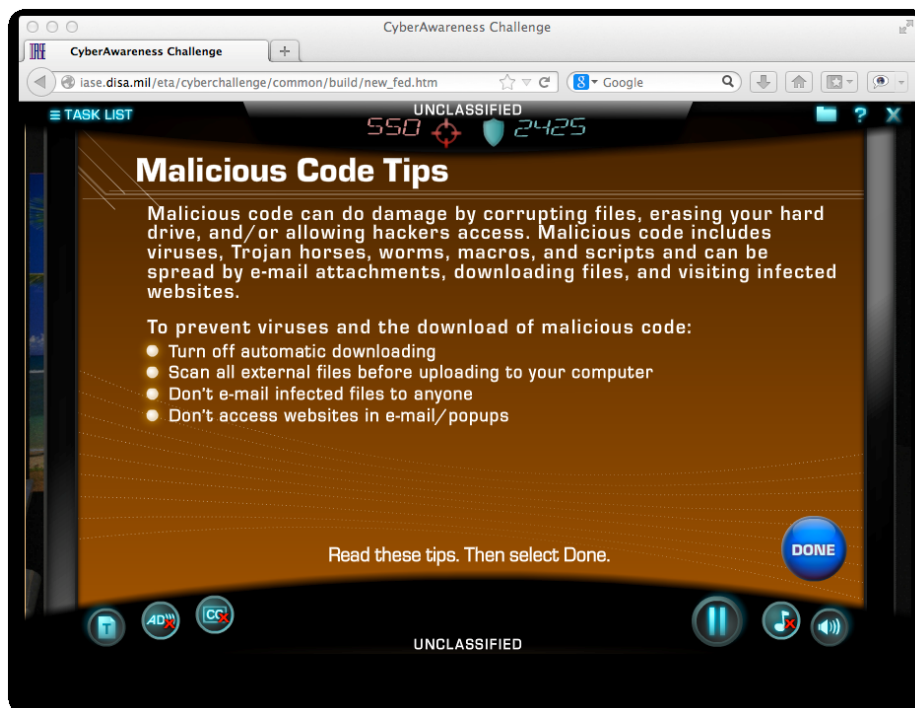


Figure A37. Malicious code tips.

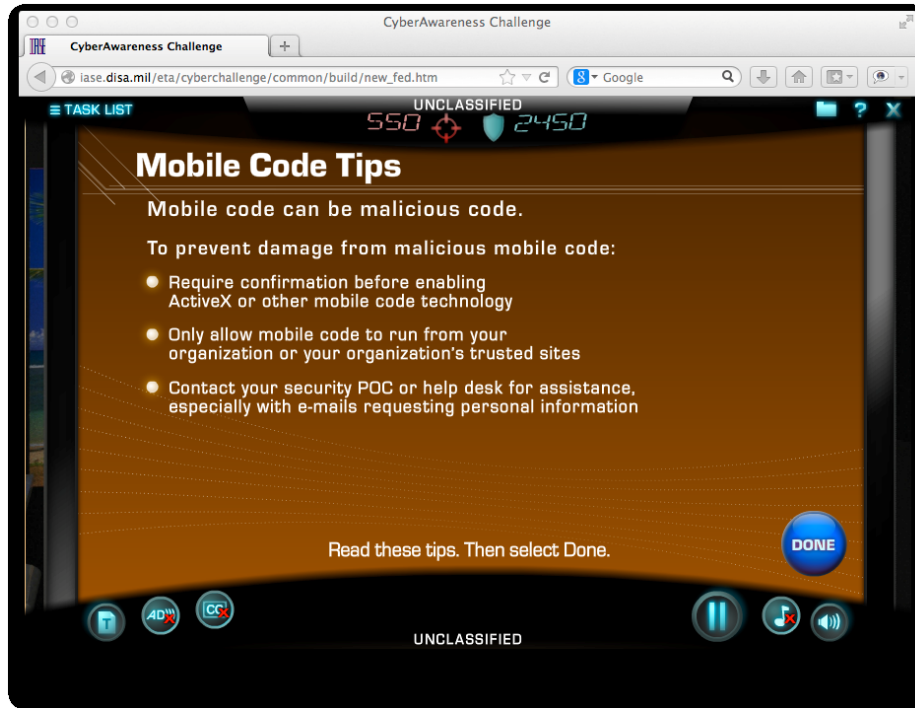


Figure A38. Mobile code tips.

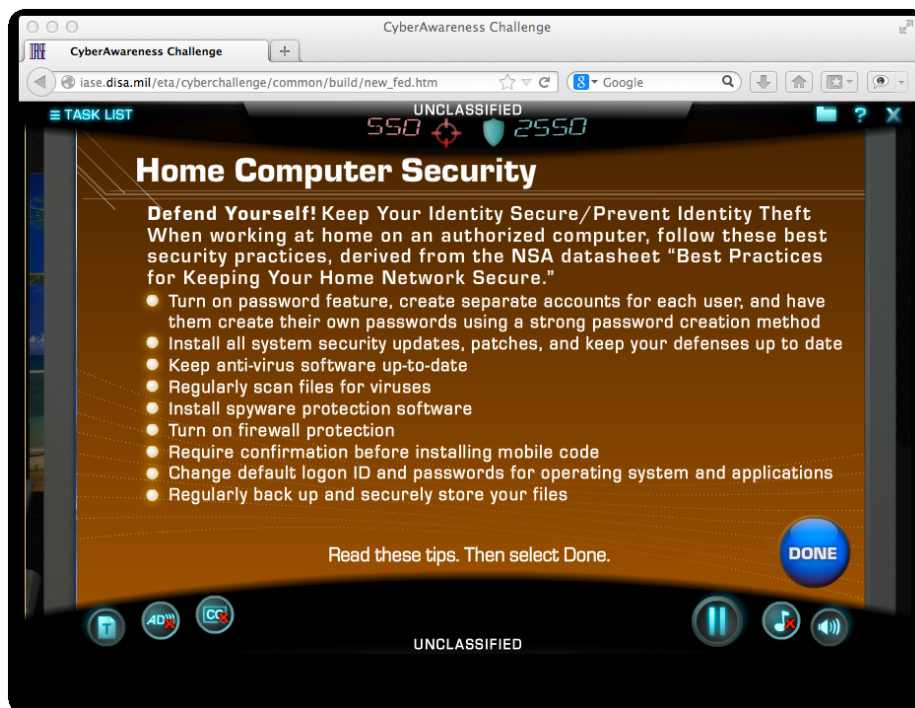


Figure A39. Home computer security.

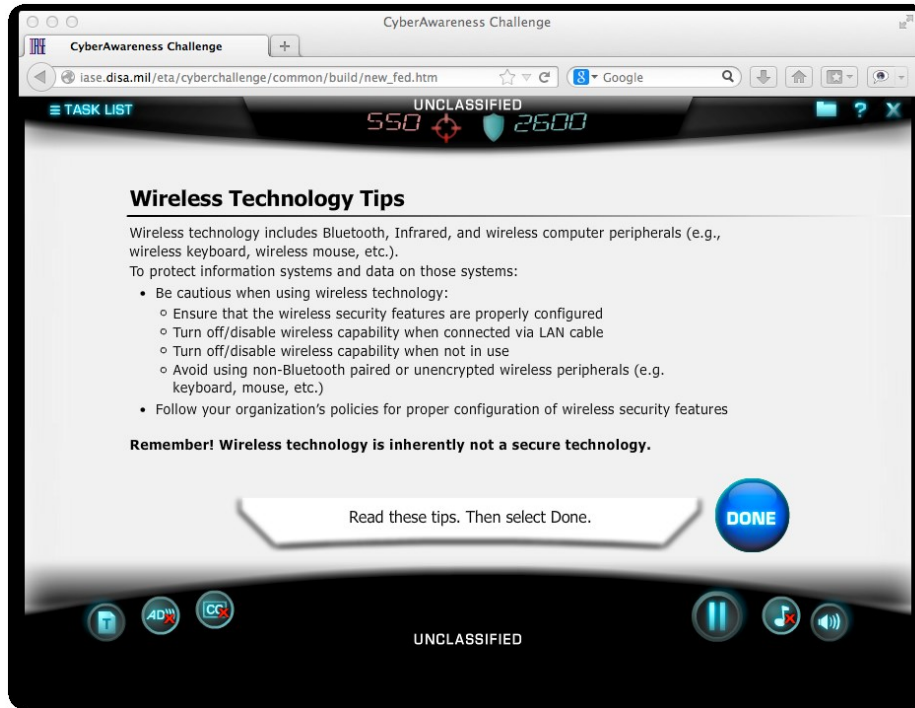


Figure A40. Wireless technology tips.

APPENDIX B: SURVEY INSTRUMENT

The survey instrument was administered on a publicly accessible web site, SurveyMonkey.com. The complete instrument comprised the introduction and instructions, a statement of informed consent, qualifying questions, and the set of questions on IA practices. The introduction section included all information necessary for participants to give informed consent. The survey questions included confirmation of voluntary informed consent, demographic information about the participant, and questions on compliance with IA policies. Prior to conducting the survey, the IA content was first validated by professionals in the field, followed by a pilot study to validate the overall survey. For the pilot survey, an additional section included questions providing feedback about the survey itself. Details on the content validation process and pilot study are at the end of this appendix.

Introduction and Instructions

[Exit this survey](#)

IA Compliance Study

1. Welcome to the Survey on CyberSecurity Policies

Thank you for participating in this survey. This survey is part of a research study to learn how well users of federal government information follow cyber security or information assurance (IA) rules on the job. Rules covered came directly from official training. The study is also to learn reasons workers do not always follow those rules.

The survey is for any adult (18 or older) who is a U. S. federal government employee, or a member of a uniformed service, or working as a federal contractor.

Participation is completely voluntary. No one is required to take the survey.

There is no payment or reward for taking the survey. There is no penalty for not taking or not finishing the survey. It should take you less than 20 minutes to complete the survey. You can take the survey by answering 26 questions.

Please read the entire introduction so you understand the purposes and use of your answers. When ready to see the survey questions, click the NEXT button at the bottom of the page. You can submit your answers at any time, today or later, but you have to do so in a single session. The web site will not remember you, so you cannot start answering, leave the site, and return later to finish. Please take the complete survey only one time.

Confidentiality and Protecting Your Privacy

The researcher will keep all completed survey answers confidential. After downloading the surveys from the web site, he will store all the data offline from the Internet. The researcher will only release summaries and analysis from the collected surveys. The researcher may allow future researchers to analyze the survey data, but only for fully approved research studies and with the same confidentiality and privacy as for in this study.

The survey is anonymous. While it is not possible to guarantee total anonymity on the Internet, the researcher has taken steps to protect your identity when taking part in the survey. You will not log in or identify yourself. The survey begins with a few questions to confirm you understand and agree to the survey, make sure you are in the right group for the study, and find out if you have any IA duties in your job. When the survey period has ended, the researcher will save all completed survey responses offline. However, the researcher will not save any information, such as your Internet (IP) address, that might be used to identify you. No one can contact you later for follow-up questions or more information. The researcher designed the survey to tell the web site not to collect the IP address of your computer. The researcher will have no record of who took the survey.

IA Compliance Study

2. Introduction Page 2

Voluntary Participation

You do not have to take this survey, and you do not have to finish taking it once you begin. You can withdraw from the study at any time while answering the survey questions by closing the web page, or by clicking *Exit this survey* in the upper right corner. The site will only save and record your answers when you click on the **Done** button on the last page. If you close the survey page without clicking **Done**, or if you click the *Exit* button, the site will discard all your answers. Because the site is not saving any identifying information about you, once you click **Done** to submit your answers, it is not possible for you to withdraw your survey answers from the study.

You do not have to take the survey immediately. You can return to the web site at any time later, until the survey period ends, to answer all the questions. You cannot save an unfinished survey and come back later to finish. If you choose to take part, you must complete the survey and submit it in a single session. You can change any answer on the survey as often as you like, until you click **Done** on the last page. You do not have to answer every question, but the more complete and honest your answers, greater your contribution to the study. Please complete the survey only one time.

Risks and Benefits of Participating

You will have no significant risk by taking the survey. No one can share your answers with any employers, supervisors or managers. No one, including the researcher, will know who you are, where you are, what your job is, or where you work. However, you may feel embarrassed if the questions remind you of times you did not follow work rules.

By taking the survey, you may benefit personally by being reminded of cyber security rules you are supposed to follow on the job. You can consider the survey as refresher training in cyber security. More broadly, results from this study may benefit everyone who works with government information. The study may be used to improve how cyber security rules are developed, trained, and enforced.

IA Compliance Study

3. Who to Contact

Questions about the Study

To verify that the study is an approved research activity of Capitol College, you may contact

Office of the Dean, School of Business and Information Sciences

Administrative Assistant Ms. Joy Exner

jexner@capitol-college.edu

(301) 369-2800 x2485

If you have any questions about the survey or study, please contact the researcher,

D. Cragin Shelton

dcshelton@capitol-college.edu

You are welcome to contact him before or after completing the survey.

You can see the cyber security awareness training used to develop the questions by going to the web site at <http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>

The next two pages give a preview of all the survey questions

Survey Preview

IA Compliance Study

4. Preview the Questions

This page and the next have all the questions so you can see them before you begin answering any.

1. Have you read the introduction page information for this survey explaining the purpose, use, and privacy protections involved?
2. Do you agree that you are taking part in this survey voluntarily, with no expectation of reward or payment, and no penalty for not participating?
3. Are you at least 18 years old?
4. Do you work as a U.S. federal government employee, uniformed service member, or U.S. federal government contractor?
5. Have you completed required annual training in information assurance awareness or cyber security awareness within the past two years?
6. Do your assigned work duties include responsibility in any area of computer security, network security, information security, information assurance, or cyber security (whether or not in your job title)?

IA Compliance Study

5. Preview the Questions (2)

After each of the following questions, you will see the same options:

Never Rarely Sometimes Very often Always

Below the selections a follow-up question will ask

If you selected *Rarely*, *Sometimes*, *Very often*, or *Always*, please briefly explain any reason(s) for your actions.

[There will be an open text box for your answer. You can type as much as you wish; all of your answer will fit.
Remember that this survey is completely anonymous.]

7. As best you recall, within the past two years how often have you created any computer system or account passwords using personal information?
9. As best you recall, within the past two years how often have you written down any computer system or account passwords?
11. As best you recall, within the past two years how often have you used your work-provided computer e-mail account to send any chain letters, jokes, mass e-mails, or inspirational stories?
13. As best you recall, within the past two years how often have you used your work-provided computer to click on a link in an e-mail from an unknown sender, instead of manually typing the web address (URL), or using a bookmark you had already saved?
15. As best you recall, within the past two years how often have you used your work-provided computer with a personally owned thumb drive, flash memory, or portable hard drive not provided by or approved by your employer?
17. As best you recall, within the past two years how often have you used your work-provided computer to transfer sensitive information, such as For Official Use Only (FOUO), Controlled Unclassified Information (CUI), personal identification information (PII) or protected health information (PHI), other than your own, or classified information to a personally-owned computer?
19. As best you recall, within the past two years how often have you used your work-provided computer to view or download pornography?
21. As best you recall, within the past two years, how often have you used your work-provided computer to gamble on the internet?
23. As best you recall, within the past two years how often have you used your work-provided computer to conduct private money-making business?
25. As best you recall, within the past two years how often have you used your work-provided computer to illegally download copyrighted programs or material?

Informed Consent Agreement

IA Compliance Study

6. Agreeing to Participate

1. Have you read the introduction explaining the purpose, use, and privacy protections involved?

- Yes
 No

2. Do you agree that you are taking part in this survey voluntarily, with no expectation of reward or payment, and no penalty for not participating?

- Yes
 No

Confirmation of Eligibility to Participate

IA Compliance Study

7. Eligible to Participate

3. Are you at least 18 years old?

- Yes
 No

4. Do you work as a U.S. federal government employee, uniformed service member, or U.S. federal government contractor?

- Yes
 No

5. Have you completed required annual training in information assurance awareness or cyber security awareness within the past two years?

- Yes
 No

The survey site design enforced the requirements for informed consent (CITI, 2012) and eligibility to participate. An answer of *No* to any of questions 1 to 5 caused a jump to the final thank you page, ending the survey without giving the volunteer an opportunity to answer the remaining questions. The thank you page included instructions to return to the initial page to change the answer.

IA Job Duties

IA Compliance Study

8. Job duties

6. Do your assigned work duties include responsibility in any area of computer security, network security, information security, information assurance, or cyber security (whether or not in your job title)?

- Yes
 No

Questions Supporting the Research Questions

The survey presented separate screens for questions related to several areas of IA guidance. As discussed in Chapter 3 the current study presents analysis of only the responses related to password usage. Additional data collected will be available for future studies. Data collection questions follow, grouped for passwords, e-mail, data protection, and computer use ethics.

Password Policies

IA Compliance Study

9. Password policies

7. As best you recall, within the past two years how often have you created any computer system or account passwords using personal information?

- Never Rarely Sometimes Very often Always

8. If you selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #7 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

9. As best you recall, within the past two years how often have you written down any computer system or account passwords?

- Never Rarely Sometimes Very often Always

10. If you selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #9 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

The content of questions 7 and 9 derived directly from the *Cyber Awareness Challenge* as shown in Figure A6, p. 171 (DISA, 2013, Th3_P@\$W0rd_Ch@lL3ng3).

E-Mail Policies

| IA Compliance Study |
|---|
| 10. E-mail policies |
| <p>11. As best you recall, within the past two years how often have you used your work-provided computer e-mail account to send any chain letters, jokes, mass e-mails, or inspirational stories?</p> <p> <input type="radio"/> Never <input type="radio"/> Rarely <input type="radio"/> Sometimes <input type="radio"/> Very often <input type="radio"/> Always </p> <p>12. If you selected <i>Rarely, Sometimes, Very often, or Always</i> for #11 please briefly explain any reason(s) for your actions. [Type as much as you wish. All of your answer will fit.]</p> <div style="border: 1px solid black; height: 60px; width: 100%;"></div> |
| <p>13. As best you recall, within the past two years how often have you used your work-provided computer to click on a link in an e-mail from an unknown sender, instead of manually typing the web address (URL), or using a bookmark you had already saved?</p> <p> <input type="radio"/> Never <input type="radio"/> Rarely <input type="radio"/> Sometimes <input type="radio"/> Very often <input type="radio"/> Always </p> <p>14. If you selected <i>Rarely, Sometimes, Very often, or Always</i> for #13 please briefly explain any reason(s) for your actions. [Type as much as you wish. All of your answer will fit.]</p> <div style="border: 1px solid black; height: 60px; width: 100%;"></div> |

The content of question 11 derived directly from the *Cyber Awareness Challenge* as shown in Figure A7, p. 171 (DISA, 2013, Ethical E-mail User Agreement) and Figure A14, p. 175 (DISA, 2013, InBoxing Challenge Summary). The content of question 13 derived directly from the *Cyber Awareness Challenge* as shown in Figure A8, p. 172 (DISA, 2013, Tips About Phishing).

Data Protection Policies

IA Compliance Study

11. Data protection policies

15. As best you recall, within the past two years how often have you used your work-provided computer with a personally owned thumb drive, flash memory, or portable hard drive not provided by or approved by your employer?

- Never
 Rarely
 Sometimes
 Very often
 Always

16. If you selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #15 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

17. As best you recall, within the past two years how often have you used your work-provided computer to transfer sensitive information, such as For Official Use Only (FOUO), Controlled Unclassified Information (CUI), personal identification information (PII) or protected health information (PHI), other than your own, or classified information to a personally-owned computer?

- Never
 Rarely
 Sometimes
 Very often
 Always

18. If you selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #17 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

The content of question 15 derived directly from the *Cyber Awareness Challenge* as shown in Figure A16, p. 176 (DISA, 2013, Tips for Removable Media Use). The content of question 17 derived directly from the *Cyber Awareness Challenge* as shown in Figure A26, P. 181 (DISA, 2013, Protecting Sensitive Information Tips).

Ethical Computer Use Policies

| IA Compliance Study |
|---|
| 12. Ethical computer use policies |
| <p>19. As best you recall, within the past two years how often have you used your work-provided computer to view or download pornography?</p> <p><input type="radio"/> Never <input type="radio"/> Rarely <input type="radio"/> Sometimes <input type="radio"/> Very often <input type="radio"/> Always</p> |
| <p>20. If you selected <i>Rarely, Sometimes, Very often, or Always</i> for #19 please briefly explain any reason(s) for your actions. [Type as much as you wish. All of your answer will fit.]</p> <div style="border: 1px solid black; height: 60px; width: 100%;"></div> |
| <p>21. As best you recall, within the past two years how often have you used your work-provided computer to gamble on the internet?</p> <p><input type="radio"/> Never <input type="radio"/> Rarely <input type="radio"/> Sometimes <input type="radio"/> Very often <input type="radio"/> Always</p> |
| <p>22. If you selected <i>Rarely, Sometimes, Very often, or Always</i> for #21 please briefly explain any reason(s) for your actions. [Type as much as you wish. All of your answer will fit.]</p> <div style="border: 1px solid black; height: 60px; width: 100%;"></div> |

The content of questions 19 and 21 derived directly from the *Cyber Awareness Challenge* as shown in Figure A2, p. 169. (DISA, 2013, Use Your Government Computer Ethically).

IA Compliance Study

13. Ethical computer use policies (2)

23. As best you recall, within the past two years how often have you used your work-provided computer to conduct private money-making business?

- Never Rarely Sometimes Very often Always

24. If you selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #23 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

25. As best you recall, within the past two years how often have you used your work-provided computer to illegally download copyrighted programs or material?

- Never Rarely Sometimes Very often Always

26. If you did not selected *Rarely*, *Sometimes*, *Very often*, or *Always* for #25 please briefly explain any reason(s) for your actions.

[Type as much as you wish. All of your answer will fit.]

The content of question 23 derived directly from the *Cyber Awareness Challenge* as shown in Figure A2, p. 169 (DISA, 2013, Use Your Government Computer Ethically). The content of question 25 derived directly from the *Cyber Awareness Challenge* as shown in Figure A3, p. 169 (DISA, 2013, Tips for Peer-to-Peer (P2P) and Unauthorized Software).

Conclusion and Thanks

[Exit this survey](#)

IA Compliance Study

14. Thank you for checking out the survey.

Thank you for taking time to help out with this research study.

If SurveyMonkey jumped you to this page before you could answer all of the questions you may have answered a question indicating you are not in the right group for this study. To be counted in this study you must be a federal government worker or contractor, over 18, who completed cyber security training within the past two years. If you clicked a NO on one of those three questions by mistake just go back to the beginning page and start over.

Please share the web address for this survey with coworkers and friends who may also be eligible to take part.

You can reach me with any questions you have about the survey or the research study at

dcshelton@capitol-college.edu

Thanks!

D. Cragin Shelton
Student, Capitol College

Pilot Survey Questions

The following questions, as suggested by Pittman (2014a), appeared as a final section of the pilot survey, only. Responses by pilot participants resulted in several improvements to the survey used for data collection. See the discussion in Chapter 4. The response field for each question was an open narrative text entry area.

IACompliance-Pilot

14. Pilot Test questions

Thank you for helping out with this pilot run of the survey. Your answers to the following questions will help the researcher ensure the survey is a valid and reliable data collection tool for the study.

27. About how long did it take to complete the survey?

28. Does the survey take too long to finish? If so, how would you suggest making it shorter?

29. Were the questions clearly worded and easy to understand? If not, what changes do you suggest?

30. Do you have any suggestions for improving the survey? If so, please provide them here.

APPENDIX C: SURVEY PARTICIPANT SOLICITATION

The validity of the results of the described research will depend on the validity of the survey as the data collection instrument (Creswell, 2012; Salkind, 2012). The process of validating the content and structure of the survey instrument requires recruiting content experts to review the information in the instrument, as well as pilot study participants representative of the target population for feedback on the overall survey (Creswell, 2012; Fink, 2009). Final results also depend on recruiting sufficient volunteers to complete the survey during the data collection phase. This appendix contains the text of e-mails used to solicit the three groups of content experts, pilot study participants, and survey participants.

Content Validity Review

In order to confirm the content validity of the data collection questions, the following request was sent by e-mail to four colleagues, all experienced professionals in information assurance or cyber security. Significant comments in response would have resulted in modification of the survey questions prior to conducting the pilot study.

Dear --,

I'm writing to ask your help in part of my research for a doctorate in information assurance (IA) at Capitol College. Capitol has approved the research proposal, but I need to validate the content of the data collection survey questions before seeking survey participants. The survey has ten questions about compliance with specific IA guidelines, each extracted from the DoD Cyber Awareness Challenge training program released by the Department of Defense, and used by other federal departments.

Would you please review those ten questions, and confirm, based on your experience in the IA field, that they represent relevant and accurate content in the field of IA? Let me

know within the week if the questions are acceptable as written, or, if you believe any of the questions needs modification, the reasons for changing them. For your convenience, I've attached to this e-mail portions of the research proposal, consisting of the survey design with the ten questions, and screenshots of all of the IA guideline screens from the Cyber Awareness Challenge. You can compare each question to the training program content.

To verify that the study is an approved research activity of Capitol College, you may contact the Office of the Dean, School of Business and Information Sciences, Administrative Assistant Ms. Joy Exner, jexner@capitol-college.edu, (301) 369-2800 x2485.

You are welcome to a copy of the complete proposal if you wish. Just let me know.

Thank you for helping.

Cragin Shelton

dcshelton@capitol-college.edu

Attached: Survey description with questions

Cyber Awareness Challenge training screenshots.

Pilot Participant Solicitation

The following invitation was sent by e-mail to colleagues of the researcher, requesting participation in the pilot stage of the survey. The invited pilot group consisted of six participants without IA duties and six participants with IA duties.

Dear --,

I'm writing to ask your help in my graduate school research. Capitol College approved the proposal for research for a doctoral dissertation in information assurance. In the initial stage I need to validate that the data collection survey is adequately designed. Would you please complete the pilot study version of the online survey within the next week? The pilot survey is online at https://www.surveymonkey.com/s/IA_Comply_pilot

I'm estimating you will need about a half hour to complete the pilot survey.

The final survey will be completely anonymous. However, for this pilot study with participants like yourself, I will know who I have invited to take part. Even so, I will not know who answered any specific instance of the pilot. The introduction and data collection pages will be as planned for the full survey. Following the ten two-part data collection questions, you will see four questions about the survey, including an estimate of how long the survey took. Your responses will help me confirm the survey design, and may guide me in re-working the survey if necessary before beginning the full survey period. I will maintain the records of your comments in those four pilot survey questions, but will not keep any records of your responses to the main part of the survey, itself.

If you cannot take part, please let me know so I can invite another pilot participant.

Please do not pass this pilot study request on to anyone else; I need to limit the number of pilot participants. When I announce the full survey, please do not complete that version, since you will have been part of this pilot study. If you are a member of one of the groups who receives the invitation I will ask you, however, to pass on to others the invitation for the full survey.

To verify that the study is an approved research activity of Capitol College, you may contact the Office of the Dean, School of Business and Information Sciences, Administrative Assistant Ms. Joy Exner, jexner@capitol-college.edu, (301) 369-2800 x2485.

Thank you for helping with this pilot study.

Best regards,

Cragin Shelton

Research Survey Request for Volunteers

Capitol College has approved my proposal for research for a doctoral dissertation in information assurance. If you work for or with the U.S. government I invite you to take part in a short anonymous survey about cyber security and information assurance on the job. The survey is open to all adult (over 18) U.S. government civilian employees, members of the uniformed services, and government contractors, in all job categories, not just information assurance or cyber security. The survey is for a study of reasons people do not always follow cyber security guidelines. The study will help my work for an information assurance degree at Capitol College in Laurel, Maryland.

Participation is completely anonymous. You will not be asked to identify yourself, where you work, or who you work for. No records will be kept that could be used to identify who completed the survey. I will not know who takes the survey, or whether any member of any invited group does so. There will be no negative consequences for not taking the survey. More details are on the survey site, including a view of all the questions before you decide to take part.

Please go to

https://www.surveymonkey.com/s/IA_Comply

It is important that workers from many job categories take part in this survey. Please share this survey invitation as broadly as possible with colleagues who may be eligible to take part.

To verify that the study is an approved research activity of Capitol College, you may contact the Office of the Dean, School of Business and Information Sciences, Administrative Assistant Ms. Joy Exner, jexner@capitol-college.edu, (301) 369-2800 x2485. If you have any questions or comments about the survey or research, please contact me at

dcshelton@capitol-college.edu

Thank you,

D. Cragin Shelton

Doctoral Candidate, Capitol College

First Reminder, September 28, 2014

I need help from group members for a short anonymous survey for my grad school research. The survey has 26 questions and takes 10 to 20 minutes to complete.

https://www.surveymonkey.com/s/IA_Comply

Please check the survey at that link, and pass the link on to friends and colleagues.

I'd like to answer questions about the research here in the discussion area. The full invitation is in the group promotion area. I'm happy to answer questions about the survey, the research study, the program (information assurance), and the school (Capitol College). Ask anything you like here in this discussion thread.

Thank you.

Cragin Shelton

Capitol College (Capitol Technology University) Grad Student

Second reminder October 6, 2014

Y'all have really been helping. On September 29 there were 11 completed surveys; today, October 5, there are 59. Thanks to you that is an over 500% increase in only a week!

Please continue to share the survey link with individuals and groups who might be eligible.

https://www.surveymonkey.com/s/IA_Comply

If you have not checked the survey yourself, please take a few minutes and do so, and complete it if you can.

For a solid statistical result, I need over 200 surveys completed. With your help spreading the word, and asking colleagues to do the same, that could happen quickly. As before, I'd love to answer questions about the survey, the research, the program, and the school here in this forum.

Related news item: On October 1st Capitol College announced it is now a university, Capitol Technology University. Cool, eh?

A very special thanks to each of you who already completed the survey. Your feedback is truly appreciated.

My best to all,

Cragin Shelton

Third reminder, October 13, 2014

Please keep sharing the link to my grad school study to friends, colleagues, and other groups that might have U.S. government workers in them.

https://www.surveymonkey.com/s/IA_Comply

Your support makes a difference. With your sharing, the number of surveys jumped from 59 to 112, nearly doubling in the past week. The survey is anonymous, and takes only a few

minutes. The intro pages explain what it is about, and who can take it. (Sorry about how long the intro is - that's required by the university ethics program for informed consent.)

As always, feel free to ask questions here about the study or program.

Thank you.

Cragin Shelton

Capitol Technology University grad student

Fourth reminder, October 19, 2014

The numbers are up, but please send out another round of reminders. Over the past week the survey count grew to almost 150. Please keep sharing the link with friends, colleagues, and any groups that might have U.S. government workers or military in them. Go back to those you already told, in case folks intended to check the survey, and just had not yet gotten around to it. Remind them the survey takes only a few minutes, and it will really help for them to complete it if they are eligible

https://www.surveymonkey.com/s/IA_Comply

Thank you, all, for great help in this study.

Cragin Shelton

Capitol Technology University

Fifth Reminder, October 26, 2014

My Weekly Status - Research Study Survey

Keeping you all up to date on the research study. Over 160 started the survey, but fewer than 90 are in the target group of U.S. federal government workers, contractors, or military.

Please keep sharing the survey link with individuals and groups that may include such workers.

Include any you have told before, in case some had forgotten to go to the link. Most have needed less than 10 minutes to finish.

https://www.surveymonkey.com/s/IA_Comply

Thank you all, again. I really do appreciate your help.

Cragin Shelton

Capitol Technology University

dcshelton(AT)CapTechU(DOT)edu

Final Notice, Closing the Survey, October 31, 2014

As of October 31 after six weeks the survey is now closed. 178 people took it. 105 of the 178 provided data for the study. A great big thank you to each member of the group who took the survey, passed on the link, or helped accumulate the numbers.

It will take a number of months to analyze the results and prepare them for release through academic sources. Feel free to drop me a note if you are curious about early, preliminary findings.

My best to all,

D. Cragin Shelton

DCShelton(AT)CapTechU.edu

APPENDIX D: LITERATURE SEARCH

Table D1.
Literature Search Categorization

| Topical Focus | Peer Reviewed Works Reviewed | Geminal Works Reviewed | Books Reviewed |
|------------------------------------|------------------------------|------------------------|----------------|
| Frameworks | | | |
| Systems engineering | 2 | 2 | 5 |
| Information assurance | 175 | 4 | 10 |
| Human behavioral theory | 24 | 1 | 2 |
| Measures of Training Effectiveness | | | |
| General training effectiveness | 24 | 0 | 1 |
| Security compliance | 116 | 2 | 8 |
| Security Usability | 9 | 0 | 4 |
| Safety compliance | 9 | 0 | 0 |
| Medical compliance | 10 | 0 | 0 |
| Research Methodology | | | |
| Qualitative Analysis | 88 | 0 | 12 |
| Quantitative Analysis | 57 | 0 | 12 |
| Mixed Methods | 45 | 1 | 9 |
| Total Documents Reviewed 275 | | | |

Note: numbers are not additive due to multiple topics identified in individual documents.

APPENDIX E: MEASURES OF TRAINING EFFECTIVENESS IN PRIOR STUDIES

Table E1.

Measures of Training Effectiveness

| Assessment Method | Immediately after training | Post-training after delay |
|---|--|---|
| Task knowledge | | |
| Quiz questions | Shaw et al., 2009 Kim, 2010 | Kim, 2010 |
| Interview or survey | | Abraham, 2012 Al-Omari et al., 2012 Aytes & Connolly, 2004 Heckle & Lutters, 2011 Kolskowska & Dhillon, 2013 Koppel et al., 2008 Kruck & Teer, 2010 Mylonas et al., 2013 Puhakainen & Siponen, 2010 Rhee et al., 2012 Sim et al., 2012 Yang et al., 2012 Workman et al., 2009 |
| Task application | | |
| Self-reported compliance (survey or interview) | | Jones & Heinrichs, 2012 Kruck & Teer, 2008, 2010 Lomo-David & Shannon, 2009 Mensch & Wilkie, 2011 Mylonas et al., 2013 Stanton et al., 2005 Teer et al., 2007 |
| Training exercise (overt) | Kumaraguru et al., 2010 Shaw et al., 2009 | Jenkins et al., 2012 |
| Survey exercise | Kim, 2010 | Abraham, 2012 Kim, 2010 Sim et al., 2012 |
| Real-world (covert) exercise | | Caputo et al., 2014 Dodge et al., 2007 Eminağaoğlu et al. 2009 |

| Assessment Method | Immediately after training | Post-training after delay |
|---|--|---|
| 3 rd party observation | | Puhakainen & Siponen, 2010 Rhee et al., 2012 Shropshire, 2008 Stanton et al., 2005 |
| Researcher observation | | Heckle & Lutters, 2011 Koppel et al., 2008 Yang et al., 2012 |
| Attitude: Intention, motivation, satisfaction with training, self-efficacy | Johnston & Warkentin, 2010a, 2010b Kim, P., 2010 | Abraham, 2012 Al-Omari et al., 2012 Bulgurcu et al., 2009 Godlove, 2012 Goo, Yim, & Kim, 2013 Herath & Rao, 2009a, 2009b Jaafar & Ajis, 2013 Johnston & Warkentin, 2010b Kolskowska & Dhillon, 2013 Mensch & Wilkie, 2011 Mylonas et al., 2013 Shropshire, 2008 Siponen et al., 2010 Stanton et al., 2005 Uffen & Breitner, 2013 Warkentin et al., 2011 |
| Event analysis of operating environment | | Eminağaoğlu et al., 2009 Heckle and Lutters, 2011 LaRosa et al., 2007 Workman et al., 2008, 2009 |

APPENDIX F: POPULATIONS, IA FOCUS AREAS, & RELATED TRAINING IN PRIOR
STUDIES

Table F1.
Prior Research Study Populations, Focus, & Training

| Study | Population Studied | IA Focus area | Correlation to Type of Training |
|--------------------------|---|---|--|
| Abraham, 2012 | Students in a university in the U.S. | Web sites & URLs | Specific training integral to the study |
| Aytes & Connolly, 2004 | Undergraduate business class students | Passwords, e-mail, data back-up. | No specific training identified; assumed cultural or environmental awareness |
| Bulgurcu et al., 2009 | Employees of multiple diverse organizations in the U.S. | General information security practices | General information security policies |
| Bulgurcu et al., 2010 | Employees of multiple diverse organizations in the U.S. | General information security practices | General information security policies |
| Caputo et al., 2014 | Employees of a medium-sized U.S. Company | e-mail spear phishing | Specific mandatory training |
| Dodge et al., 2007 | Students in a university in the U.S. | e-mail Web sites & URLs | Specific mandatory training |
| Eminağaoğlu et al., 2009 | Employees of a large company in the Turkey | Passwords | Specific mandatory training |
| Godlove, 2012 | Teleworkers | General information security policies | General information security policies |
| Goo et al., 2013 | IT Managers in Korea | General information security policies | General information security policies |
| Heckle & Lutters, 2011 | Employees of a large hospital in the U.S. | Passwords General Internet or computer use | Specific mandatory training |
| Herath & Rao, 2009a | Employees of multiple | General information security policies | No specific training identified; |

| | | | |
|-----------------------------|--|--|--|
| | organizations in U.S. | | assumed cultural or environmental awareness |
| Herath & Rao, 2009b | Employees of multiple organizations in U.S. | General information security policies | No specific training identified; assumed cultural or environmental awareness |
| Jaafar & Afis, 2013 | Malaysian Army | General security practices | No specific training identified |
| Jenkins et al., 2012 | Students in a university in the U.S. | Passwords | Specific training integral to the study |
| Johnston & Warkentin, 2010a | Students, faculty, and staff in a large university in the U.S. | General Internet or computer use | Specific training integral to the study |
| Johnston & Warkentin, 2010b | Students, faculty, and staff in a large university in the U.S. | General information protection | Specific training integral to the study |
| Jones & Heinrichs, 2012 | Students in a public university in the U.S. | Smartphone security | No specific training identified; assumed cultural or environmental awareness |
| Kim, 2010 | Employees of a bank in the U.S. | General information protection | Specific training integral to the study |
| Kolkowska & Dhillon, 2013 | Employees of a Social Services Division office in Sweden | General information security | Incidental system-usage training |
| Kruck & Teer, 2008, 2010 | Undergraduate university students in 42 majors | Passwords Patches Attitudes (p. 256) | Mandatory online training on general computer security and password confidentiality. |
| Kumaraguru et al., 2010 | General population recruited by advertising in U.S. | e-mail phishing | Specific training integral to the study |
| Lomo-David & Shannon, 2009 | Students in Turkey, Republic of | Passwords, daily system scan, email attachments scans, | No specific training identified |

| | | | |
|----------------------------|---|---|---|
| Mensch & Wilkie, 2011 | China, and Nigeria Graduate and undergraduate students at a mid-sized university in the U.S. | anti-virus software, and firewalls Basic computer security | No specific training identified |
| Mylonas et al., 2013 | Random people in public areas in Athens, Greece | Smartphone security | No specific training identified; assumed cultural or environmental awareness |
| Novakovic et al., 2009 | All computer users, in home and work environments | Password use | No specific training identified |
| Puhakainen & Siponen, 2010 | Employees of a technology company in Finland | e-mail General Internet or computer use | Specific training integral to the study |
| Rhee et al., 2012 | Management information systems executives in multiple companies in the U. S. | General information security | No specific training identified |
| Shaw et al., 2009 | Freshman information systems students in a private university in Taiwan | e-mail | Specific training integral to the study |
| Shropshire, 2008 | Employees of a bank in the U.S. | General information protection | Limited correlation with established training content |
| Sim et al., 2012 | Active Facebook users 18 and older in the U.S. | Privacy protection | Specific training integral to the study |
| Siponen et al., 2010 | Employees of companies in Finland in four diverse business sectors | General information protection | No specific training identified |
| Stanton et al., 2005 | Employees of multiple organizations across U.S. | Passwords | Specific training integral to the study |
| Teer et al., 2007 | University students | Security perceptions and practices | Mandatory online training on general computer security and |

| | | | |
|-------------------------------|--|---|--|
| Uffen & Breitner, 2013 | Business executives in Germany | General security practices | password confidentiality. No specific training identified |
| Warkentin et al. 2011 | Employees of multiple healthcare organizations in the U.S. | Privacy protections | Regulatory guidelines (HIPAA) as training proxy |
| Workman et al., 2008, 2009 | Employees of a U.S. technology company | Password maintenance, system patching, data backup practice | Specific mandatory training |

APPENDIX G: LITERATURE SUMMARY FROM ABRAHAM (2012)

Table G1.

Summary of Behavioral Theories in Information Security Studies

| Discipline | Theory | Attributes | Studies |
|---------------------|---|--|--|
| Social Psychology | Theory of Reasoned Action and Theory of Planned Behavior Social Cognitive Theory | Attitudes Subjective norms Perceived behavioral control Self-efficacy | Loch and Conger (1996) Chang (1998) Leonard et al. (2004) Rhee et al. (2009) Bulgurcu et al. (2010) Siponen et al. (2010) |
| Information Systems | Technology Acceptance model | Perceived usefulness Perceived ease of use | Cannoy and Salam (2010) |
| Criminology | Deterrence Theory Neutralization Theory | Certainty of sanctions and severity of sanctions Security policy violations | Straub (1990) Siponen and Vance (2010) |
| Health Sciences | Protection Motivation Theory Health Belief Model | Severity of risks; vulnerability to the risk; self-efficacy in performing the risk-mitigating behavior; and response-efficacy of the risk-reduction behavior. Attitudes and beliefs | Workman et al. (2008) Siponen at al. (2010) Anderson and Agarwal (2010) Johnston and Warkentin (2010) Ng et al. (2009) |
| Philosophy | Value Focused Thinking | Values | Dhillon and Torkzadeh (2006) |
| Economics | Agency Theory | Intrinsic and extrinsic motivation | Herath and Rao (2009) |

| Discipline | Theory | Attributes | Studies |
|-------------------------|------------------------|--|------------------------|
| Neo-classical economics | Rational Choice Theory | Attitudes and beliefs towards compliance | Bulgurcu at al. (2010) |

Note. From Table 2.1, Exploring the effectiveness of information security training and persuasive messages (p. 10), by S. Abraham, 2012, University at Albany, State University of New York. Copyright 2012 by the author. Reproduced with permission.

APPENDIX H: METHODOLOGY MAP

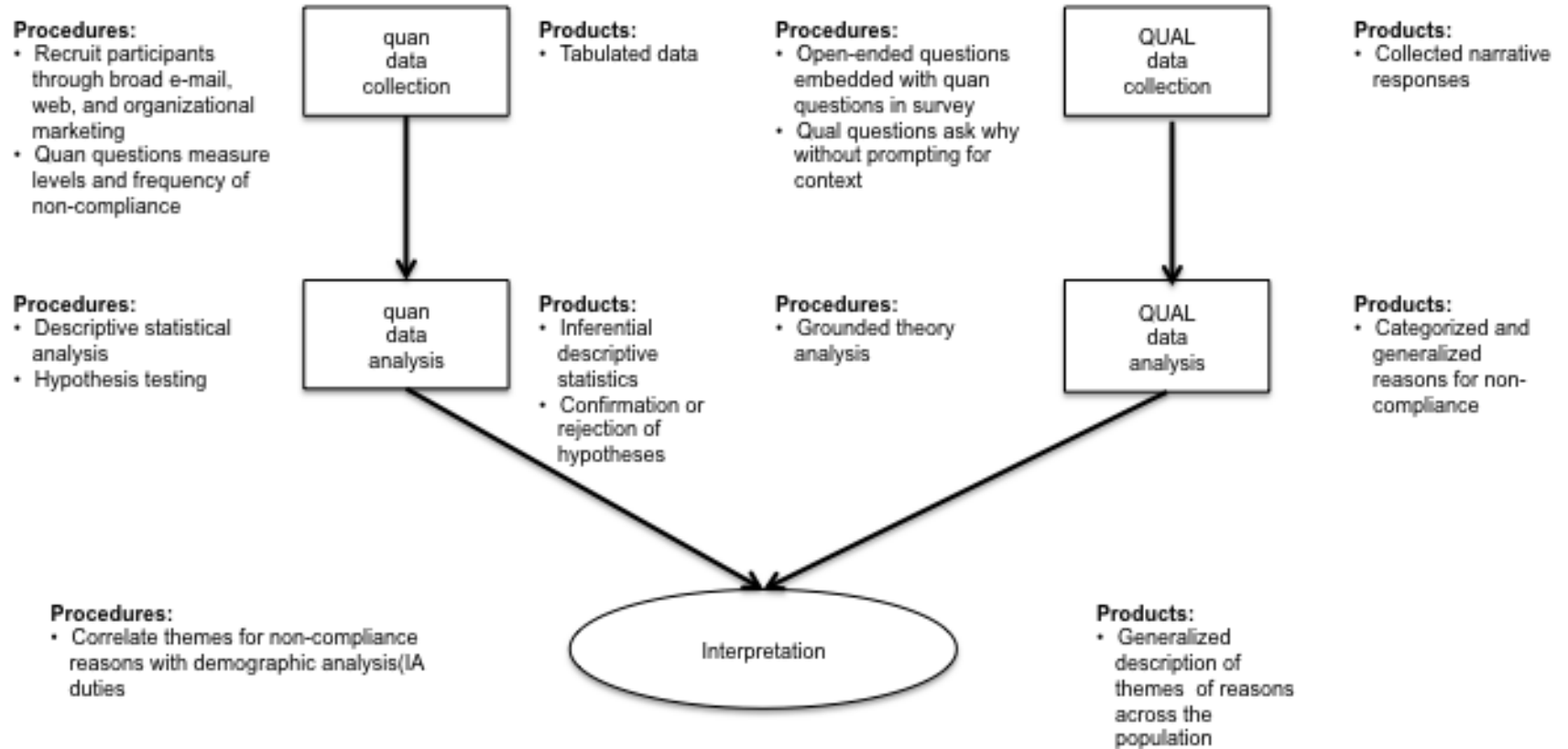


Figure H1. Mixed method procedures diagram for concurrent, embedded design research, in the format recommended by Creswell and Plano Clark (2011).

APPENDIX I. ACRONYMS

| | |
|--------------------|---|
| (ISC) ² | International Information Systems Security Certification Consortium |
| ACM | Association for Computing Machinery |
| CBK | Common Body of Knowledge |
| CEO | Chief Executive Officer |
| CIA | confidentiality, integrity, availability |
| CNSS | Committee on National Security Systems |
| COBIT | Control Objectives for Information and Related Technology |
| CUI | controlled unclassified information |
| DHS | Department of Homeland Security |
| DISA | Defense Information Systems Agency |
| DoD | Department of Defense |
| EBK | Essential Body of Knowledge |
| EMAS | electronic medication administration system |
| ENISA | European Network and Information Security Agency |
| EU | European Union |
| FOUO | for official use only |
| GDT | General Deterrence Theory |
| HIPAA | Healthcare Insurance Portability and Accountability Act |
| IA | information assurance |
| IEEE | Institute of Electrical and Electronics Engineers |
| INCOSE | International Council on Systems Engineering |
| IP | Internet Protocol |

| | |
|---------|--|
| IS | Information system |
| ISACA | Information Systems Audit and Control Association |
| ISO/IEC | International Organization for Standardization (ISO) and the International Electrotechnical Commission |
| ISPC | information security protocol compliance |
| NICCS | National Initiative for Cybersecurity Careers and Studies |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| OMB | Office of Management and Budget |
| PGP | Pretty Good Privacy |
| PHI | protected health information |
| PII | personal identification information |
| PMT | Protection-Motivation Theory |
| RCT | Rational Choice Theory |
| SAM | Security Acceptance Model |
| SE | systems engineering |
| SEBoK | Systems Engineering Body of Knowledge |
| SEI | Software Engineering Institute, Carnegie Mellon University |
| SSO | single sign-on |
| TAM | Technology Acceptance Model |
| TCM | Threat Control Model |
| URL | universal resource locator |

