2-4-2015

Motivating Information Security Awareness (isa): An Action Research Study

Grace Giraldo
Syracuse University

Recommended Citation

Giraldo, Grace, "Motivating Information Security Awareness (isa): An Action Research Study" (2015). *Dissertations - ALL*. 1802.
https://surface.syr.edu/etd/1802

Abstract

The goal of the study was to identify and analyze specific environmental and social conditions that motivate middle management to advocate for Information Security Awareness (ISA), as well as to see if exposure to new information security knowledge would change their behavior. Using a mixed-method action research approach, a group of managers shared their *awareness knowledge, advocacy behaviors,* and *challenges* influencing their engagement in information security awareness advocacy. Post workshop feedback confirmed the effectiveness of the Action Research workshops in increasing ISA advocacy behaviors.

The action research workshops provided an opportunity for the participants to increase their security knowledge and recommend improvements in ISA advocacy practices. Thirty-eight (38) managers, divided among four workshops, participated in the study. Within the research activities, I presented the group with an *awareness knowledge* self-assessment survey, which captured the managers' view of their own information security knowledge, a sample information security awareness presentation brought context to the workshop, and a group discussion similar to a focus group provided the environment for discussions. During these activities, the managers expressed recommended changes they could drive to improve ISA advocacy. The workshop activities concluded with a closing discussion seeking *commitment* from the managers to act on the recommendations to improve ISA advocacy. These engagements of learning, and sharing their awareness, supported the main goal of leveraging action research. The findings support the Action Research workshops were an effective tool to increase the participants learning, to improve the practice of ISA advocacy, and to socialize the topic of information security.

The key lessons learned from the research contribute to the overall body of knowledge in the information security awareness discipline as follows. Key finding 1: the feedback on self-reflective levels of knowledge in information security awareness indicated managers are not sufficiently exposed to ISA content. Key finding 2: the self-reflection on *advocacy behaviors* projected positive attitudes and increased motivation to propose and take actions toward sharing ISA with employees and peers. Key finding 3: the main *challenges* discovered show that managers need more guidance, increased *awareness knowledge*, more organizational support, and the creation of a climate that supports *advocacy behaviors*. Key finding 4: the Action Research workshop contributed to participants learning, and to improvements to information security practices through participants' new behaviors to increase ISA advocacy. Participants reported they learned and used the ISA topics discussed during the workshop with their friends, family, peers, and employees after the workshop. The key thesis findings led to the following recommendations to help organizations foster a climate that supports ongoing *advocacy behaviors*. The recommended activities include: helping managers understand the importance of their engagement in advocacy behavior; obtaining resources that increase information security awareness and knowledge; planning and sharing activities that promote ISA sharing; and, communication the expectation for advocacy behaviors and the resources available to support sharing information security awareness.

MOTIVATING INFORMATION SECURITY AWARENESS (ISA): AN ACTION RESEARCH STUDY

By
Grace Giraldo
B.S., Interamerican University of Puerto Rico, 1987
M.S., Marshall University, 1999

Thesis
Submitted in partial fulfillment of the requirements for the degree of

Doctorate of Professional Studies in Information Management

Syracuse University
December 2014

Acknowledgements

Thesis Examination Committee:

Dr. Michelle L. Kaarst-Brown (Advisor)

Dr. Art Thomas

Dr. Lee McKnight

Dr. Yang Wang (Reader)

Dr. Stuart Thorson (Examination Chair)

This is a great accomplishment, one that did not come without great challenges, discipline and sacrifice on my end, but an accomplishment that without support, I would have not reached on my own.

I would like to express my sincere appreciation to my committee chair Dr. Michelle Kaarst-Brown, who persuasively guided me during this multi-year journey. Without her supervision and direction, this thesis would not have been possible. I would like to thank my committee members, Dr. Lee McKnight and Dr. Arthur Thomas, for their support, inspiration, and insights through every step of the process. Moreover, to Dr. Yang Wang and Dr. Stuart Thorson for being part of my defense committee that saw me to the finish line.

A special appreciation goes to my peer, friend, study-buddy, and Syracuse brother Dr. Keith Brand, thank you for being there from the beginning to the end. Thank you for always having time discuss ideas, the weekly calls and for being my sounding board. I am especially grateful for the encouragement, for believing in me, and for the strength you gave me when I ran out. I am proud of you!

To my mentor, and forever friend, Richard F. Conti, for encouraging me to stay focused, gracefully listening to my challenges, and reminding me there was light at the end of the tunnel. To the companies who opened their doors to make the research workshops possible. To my Information Security colleagues Jon Lucenius and Chris Emerson for taking time to peer review my ISA presentation.

To my dear son Omar Rivera, for taking care of me with every meal and errand you did so I could make time for my studies.

To my adorable Mom, the kindest person I have ever known, who sent me on this path many years ago and inspired me to reach higher.

To my sisters, family, and friends, my gratitude and thanks for their goodwill, love, constant encouragement, and for understanding the demands of this program. I am looking forward to reconnecting and celebrating our friendships again.

Contents

List of Tables

Table of Figures

MOTIVATINGING INFORMATION SECURITY AWARENESS (ISA): AN ACTION RESEARCH STUDY

Chapter 1: Introduction of the Study

> *Role models are the major determinant of the level of ethical or unethical behaviours in an organization (Falkenberg & Herremans, 1995, p. 139).*

Information security awareness dissemination helps educate end users in the topic of activities that lessen information security risk. "Awareness is taken to mean only the imparting of information, and awareness alone is unlikely to achieve any significant change in behavior" (McLean, 1992, p. 180). While Information Security (IS) specialists' model and advocate security behaviors as part of their job roles, non-IT Managers serve as important role models throughout the organization. Information security is a technical discipline that needs to be socialized. Creating security awareness that has an influence on people's lives can arise from drawing their attention to specific situations what are often intangible threats. The intentions of this study to discover and define factors that help inspire or influence the non-IT middle management of an organization to become advocates for information security awareness (ISA). In particular, the research explores how Action Research ISA Advocacy Workshops offer a viable approach to positively influence non-IT managers, (non- IT and non-security), to advocate IT security even though it is not part of their formal job responsibilities.

In this study, the term *advocacy* designates the willingness to raise consciousness of information security awareness by participating in the act of sharing information (good practices, risks, etc.) received from the organization with peers and employees. Influencing individuals to share, and the action of sharing advocacy, are the behaviors explored, including accounting for the reasons (motivating factors) participants identify as influenced their decision toward or against advocacy.

The key thesis findings led to the following recommendations to help organizations foster a climate that supports ongoing *advocacy behaviors*. The recommended activities include helping managers understand the importance of their engagement in advocacy behavior; obtaining resources that increase information security awareness and knowledge; plan and share activities that promote ISA sharing; and, communicating the expectation of advocacy behaviors and the resources available to help managers share information security awareness.

The Research Problem

"The concept of information security awareness is taken in the literature to mean that users should be made aware of security objectives (and further committed to them)" (Siponen, 2000, p. 24). An organizational information security awareness (ISA) program alone will not motivate dissemination, but it is part of the bigger picture. If we can develop an understanding of how to influence middle managers' *advocacy behaviors*, these results may serve as a guideline for organizations to self-assess their ISA advocacy posture and or identify gaps for those looking to improve in this area.

The research questions pursued here are what do members of middle management know about information security risk awareness? What are members of middle management currently doing about advocacy of information security awareness? Have members of middle management identified any factors that affect their or peer managers' ISA *advocacy behavior*? Do Action Research workshops have a measurable impact on positive ISA behaviors among Middle Managers who participate?

Security breaches (monetary loss or information disclosure) and violation of privacy concerns are just two of the most common threats we face on a daily basis as part of a culture that actively uses the Internet and online services for many of our business and personal activities. These problems cannot be addressed only after threats have happened, nor is the solution to these problems isolated to those who work in the IT function. Organizations providing services that process, transmit, or store information ideally should take action to prevent such threats. They also should educate everyone in the company about behaviors that are consistent with better protection of company information and other assets, for instance, “telling people what to do through standards, guidelines and other instructions and motivating them to perform in the interest of good security” (McLean, 1992, p. 180).

Although ISA programs may exist today, it is unclear at this time which dissemination methods best motivate members of middle management toward advocacy. The middle managers’ exposure and appreciation of the existing ISA program and their preferences for the different formats of ISA information help determine their willingness to adopt and practice *advocacy behavior*. These factors also help the ISA program leaders target topics and formats to improve the non-security audience’s content absorption.

Middle managers, specifically, those outside the IT function, are critical information security resources that need to be leveraged. The middle management of an organization has the most direct influence over the employees. “An individual’s direct supervisor, particularly in a large organization, may be the dominant role model” (Falkenberg and Herremans, 1995, p. 139). Further, “anyone who regards information in any form as an important asset (e.g., starting from information that is regarded as private) should be aware of the possible threats to it” (Siponen, 2000, p. 24). The study explores the individual attitudes, organizational social norms, and value alignment among members of middle management as motivating factors enabling their *advocacy behavior*. “The exact nature of behavioral and attitudinal change we require depends on the role and seniority of each individual” (McLean, 1992, p. 180). According to a 2001 study by Zaccaro and Klimoski, the study participants have the ability to “facilitate the processes that enable organizations to achieve their goals and objectives” (as cited in Grojean, Resick, Dickson, & Smith, 2004, p. 224). On order to increase information security awareness as a part of organizations and culture, more than rules or ISA artifacts are needed. “Leaders not only directly influence the behavior of members, but their actions also influence perceptions of members, which lead to norms and expectations of appropriate conduct that become ingrained in the organizational climate” (Grojean et al., 2004, p. 224).

My study explores constructs drawn from the literature: *awareness, advocacy, constraints or challenges, and commitment.* Within these constructs, the organizational environment and personal perspectives are potential factors affecting the motivation of *advocacy behavior*. This limits the scope of prescribed variables, but creates an opportunity for discovery used semi-guided questions and discussions to enable study participants to express in their own words their understanding of organizational and personal factors (influential or detrimental), to their *advocacy behavior*. Literature-based variables drove discussion, while industry trends and incidents drive the presentation of the problem statement. The discussions and feedback from members of middle management uncover factors motivating ISA advocacy. The combination of literature-derived constructs, industry incidents, and practical experience triangulate through accumulated experience of the participatory action research, and test a practical approach to increasing of ISA *advocacy behavior*. While the researcher is both participant and contributor to the study, it was imperative to capture the middle managers’ perspective objectively and without bias. In the Action Research workshop, the researcher introduced the subjects of discussion to the group, but ensured participants engaged in a group dialogue freely and recorded their responses. During the data analysis, it was important to take a holistic approach to the responses, rather than only considering those responses that directly affect the working propositions.

The action research approach created a baseline measure of the present state of ISA advocacy by middle managers in the small sample of companies, but also allowed participants to learn and identify potential changes to their own ISA behavior. By companies, I am referring to corporations, institutions, or businesses of various sizes that have multiple layers in their organizational structure. Within these organizations, the layers of managerial structure have a distinct executive level, one or more middle levels, and their lower level employees that do not manage other individuals. This existence of multiple layers of management in the structure allows me to separate the middle management layer, which is the leadership layer of interest for this study.

The purpose of this research was to discover factors (reasons) affecting ISA advocacy of middle managers in various organizations. ISA advocacy was defined as an individual's decision to share information security awareness information with peers and those they supervise.

The study design is participatory action research used a mixed-method approach in order to explore participants' views, and examine the various influences from the surrounding environment that affect *advocacy behavior*. The intent was to use the information discovered from the participant discussions to explain the ISA advocacy influences. "Security activities, whether in terms of science or practice, are mainly stimulated by a concern to prevent certain activities that are interpreted as abuses" (Siponen, 2001, p. 27). The boundaries of ISA advocacy influences are not clear. This action research study had a broader view, permitting the consideration of factors affecting *advocacy behavior* by middle management and the possibility that the discovered factors were outside of the individual participant's control.

Definition and Scope of the Problem Space

The research focuses on understanding the *awareness knowledge*, *advocacy behavior*, *perceived constraints* and *challenges* and *advocacy commitments* expressed by middle managers toward ISA advocacy. The middle manager's perspective and comments about the ISA content were all legitimate sources of data, since they proposed ideas to increase ISA advocacy and behavior.

The middle management knowledge level regarding ISA was expected to differ, especially across several different companies, and was included in the study as a potential factor that affected *advocacy behavior*. "It constitutes an integral part of the general knowledge of citizens in the information society" (Siponen, 2001, p. 24). In a related health care study, Katsikas (2000, p. 135) defines a complete body of knowledge, but differentiates it by subsets of "knowledge necessary for HCE managers" according to the manager's functional role, HCE being the organization in the researcher's study. Consistencies or inconsistencies in the level of *awareness knowledge* that middle managers was expected to affect their individual decisions to share ISA with their employees. Asking middle managers about their present understanding of ISA helped address this research sub-question: What do members of middle management know about information security risk awareness? Their ISA knowledge level was found to be a direct contributing factor to *advocacy behavior*. The exploration results helped identify ISA learning opportunities for the study participants. The results further help contribute to the organizations identifying the need for training resources for middle management.

Therefore, a questionnaire and dialogue on the subject of level of *awareness knowledge* was required in order to baseline the need for increased ISA exposure. An understanding of their exposure to content and its longer-term impact on learning benefited everyone, since it helped fine-tune ISA content into the right size, the right topic, and the right level of technical content. “While there are numerous resources available to provide security advice and guidance without incurring significant expense (e.g., books, websites, newsgroups and e-mail lists), these do not offer the ability to test one’s understanding in practice. It is desirable to be able to perform such testing before being faced with the task of applying security for real within an organisation” (Furnell, et al., 2002, p. 354).

Advocacy behaviors are activities mid-level managers, or supervisors, engage in to promote, share, and communicate information security awareness learning among peers and those they manage. These behaviors are observed in their daily routines, like forwarding emails with security notifications or sharing industry related security incidents.

Perceived *constraints* and *challenges* are reasons that hinder a manager from performing *advocacy behaviors*. Some reasons may include lack of time, resources, reliance on other staff members, or the belief that it is not a responsibility within their job function to share security awareness.

This study presented a unique opportunity for middle managers to contribute to their organizations (program recommendations), to themselves (increased development), and to their employees (improve best practices). During the Action Research workshop, an understanding of factors that motivate managers’ was the driver for recommended solutions to increase their *commitment* to ISA advocacy.

The differences in the characteristics of the existing environment are potential motivators of ISA advocacy. Some but not all industries are regulated by the government or industry standards. Organizations may have different levels of security and privacy expectations for information including intellectual property, employee data, and company data considered sensitive or confidential. As such, exploring these factors across participants from different industries adds to the richness of our understanding of outside influences in middle managers.

Outside Scope of Study

This study only represents the corporate culture and present state of a small set of organizations; the findings for other organizations within the same industry may not be the same. The study represents the perspectives of a particular group of people, that is, non- IT middle managers. This study does not include attitudes and perspectives of employees with no direct reports, and excludes top-level personnel such as senior managers or members of the board of directors.

Assumptions and Requirements

It is important to acknowledge any assumptions that the researcher is making. This is especially important when the researcher is not internal to the organization studied. Regarding the organizations, one assumption is that the organization approves the use of needed resources, including information security and legal departments. A second assumption and requirement is that all organizational documentation and artifacts used for the research study will be scrubbed of branding for all research publications. This ensures confidentiality for the participants and their firms.

Regarding the target participants, a third assumption is that they are either currently exposed to ISA content through organizational efforts, or have been exposed in the past. For example, security policies exist for most organizations. A fourth assumption regarding target participants is that they either have a sense of awareness that they should, to some level, support or champion the need for information security awareness through their own acts of dissemination or mentorship.

The final assumption is that there is at least one or more middle layer of management in the participating firms. Even so, organization's management structure may change between the time the participant selection process occurs and the completion of the study. This is important to consider because a participant's functional job may change between the time the research study takes place and the time the results of the research are published.

Practical Motivation for the Study: Why Is This Topic of Interest?

As will be highlighted in chapter two, there are gaps in our understanding of ISA *advocacy behavior*, specifically related to the role of the middle manager. From a practical perspective, practitioners in the information security field, protection of information and other assets are a central point of focus. In practice, it is common to conduct a deep analysis to follow the data path as a way to discover points that are vulnerable to threats. Looking for threats is a multidimensional endeavor; as vulnerabilities are often a result of several contributing opportunities and weaknesses. When combined, they expose information assets to risk and misuse. This research intends to gain the perspective of managers, from which one can leverage and recommend changes to improve the organization's security posture. "If the appropriate cognitive strategy is present in the minds of the management of the organization, the organization can succeed in implementing the approach effectively" (Thomas, 1990, p. 63).

By exploring, learning, and understanding the organizational and individual factors motivating middle managers in favor of ISA advocacy, we can develop a better understanding of how to better promote information dissemination. This research is a discovery process to explore the middle manager's personal point of view of advocacy and the organizational environment influences that shape this view. Increasing *advocacy behavior* evokes a ripple effect, creating momentum of information dissemination about security practices that has potential to reach a greater number of individuals.

Awareness may also influence individual decisions regarding information assets. "The dimensions of security awareness are based on the belief that awareness is an issue that everyone using any form of IT services, either directly or indirectly, particularly in an Internet environment, should bear in mind" (Siponen, 2001, p. 25). Details of information security incidents often contain organizational proprietary information that is technical and complex, creating a challenge that would result in revealing organizational and trade secrets if the issues were to be disclosed. However, information security awareness takes lessons learned from true incidents and socializes them to a state of disclosure that is shareable with all employees in an organization. By providing middle managers with a "call-to-action message", they can apply this in their future actions. Choi, Kim, Goo, and Whitmore (2008) note, "by staying aware of the current state of activities and threats related to environments, people are able to adjust their own work toward a common goal" (p. 486).

How We Know There is a Problem

Several work-related observations drove my interest to explore this topic as an opportunity for research. My job function in the Information Security Department includes selecting and organizing the delivery of informational sessions for the business community. The usual audience includes technical and non-technical organizational members, regardless of their seniority and job function or location. In other words, the informational sessions are for the general community; all are welcome to attend.

Information security incidents are often a topic of security awareness informational sessions. Typically, Information Security Awareness sessions show examples of situations where information is affected in a manner that causes harm to a person or organization. Although many types of incidents exist, my perspective focuses on the threats against information that lead to violations of privacy, information breaches, or fraudulent activity. In these cases, information is disclosed, lost, used for fraudulent activity, or made unreachable.

Table 1.1: Examples of Information Security Incidents

Type of Breach	Article Title (Author and Year)	Publication Date
Account breaches	*Twitter User Passwords Reset After Accounts Breached* (Whittaker, 2012)	11/08/2012
Account breaches	*Pinterest Locks Out Hacked Accounts, Investigates Security Breach* (Racoma, 2012)	06/20/2012
Account breaches	*Another Hack? Last.fm Warns Users to Change Their Passwords* (Mattise, 2012)	06/07/2012
Account breaches	*LinkedIn Member Passwords Compromised* (Silveira, 2012)	06/07/2012
Phishing	*Bogus Twitter Direct Messages Lead to iPad Scam, Survey and Phishing* (Zorz, 2012c)	10/24/2012
Phishing	*Beware Remove your Facebook Timeline Scams* (Cluley, 2012)	05/29/2012

Type of Breach	**Article Title (Author and Year)**	**Publication Date**
Phishing	*Beware of Fake Facebook Account Cancellation Emails* (Zorz, 2012b)	05/22/2012
Phishing	*Worm Targets Facebook via PMs* (Zorz, 2012a)	05/18/2012
Vulnerabilities	*Facebook's Phone Search Can Be Abused to Find People's Numbers, Researchers Say* (Constantin, 2012)	10/08/2012
Vulnerabilities	*Facebook Takes Aim at Cross-Browser "LilyJade" Worm* (Krebs, 2012)	05/17/2012

My informational sessions typically include a "call to action", which intends to help the audience understand what they can do to prevent a security incident. However, these are not 'action research' sessions as they are one-way presentations where I disseminate information. In the past, I was unable to capture data on whether participants' advocacy or other security behaviors actually changed. The sessions also highlight the organizational policies and guidelines that serve as best practices in an attempt to help the audience understand why the guidelines exist. Some examples of information security industry incidents publicly available through the Internet are included in Table 1.1.

Industry incidents continually occur, creating a constant need for consciousness and awareness. Through my experiences managing information security awareness (ISA) sessions, I have observed some behaviors that have support that practical problems still exists. For example, some employees who received an invitation to the information sessions did not think they should attend. Not fully understanding the reasons why employees would think this, I began an informal dialogue with the corporate ISA department to learn about new and existing initiatives and about some of the challenges of having a broad and extensive audience. This dialogue made me aware of opportunities where research could benefit the organization.

One example of work-related observations included the following scenario. An invitation for an awareness event titled "Information Security Industry Trends Presentation" was sent to about a thousand employees. The following text was included as part of the description of the event:

> *"This information security awareness session provides business and IT professionals with a general understanding of current trends in information protection. By familiarizing the audience with common concepts and real-world examples, we'll provide a basic understanding and practical ways to protect against various risks like social engineering, phishing attempts, and virus transmission."*

The boundaries of the influences of ISA advocacy are not clear. The following are responses from members of the general audience, three of whom have a functional title of manager. The responses below led me to believe that there may be a gap or potential problem to research:

> *"I'm not sure, but this may have been sent in error to me; please advise… thank you!"*
>
> *"I don't believe this was intended for me."*
>
> *"I think you have the wrong Dxxx Mxxxxx. I am in the XXXX Dept. in XXXXX."*
>
> *"I think this was sent to me in error."*
>
> *"I believe I am on this list in error. Can you please remove me?"*

Between this workplace observation, the industry incidents, and several informal conversations with IT security management, I was highly motivated to pursue this research inquiry as having both research and practitioner value.

Research Questions

The larger problem statement for this study is as follows: How can we motivate management in advocating for IT security behavior among their direct reports and peers? The research keeps the focus of understanding the attitudes, perceptions, and values expressed by the middle managers about ISA advocacy. This larger problem statement is broken down into several specific research questions that are explored the literature and then through Action Research Design described in chapter 3.

Research Question 1: What do members of middle management know about information security risk awareness?

The individual's level of *awareness knowledge* could be an instrumental contributing motivator for practicing advocacy. The middle managers can only advocate what they know. The purpose of an ISA knowledge assessment is to "give corporate security officers a benchmark measure of their own success or failures" (Deyhle, 2002, p. 2). Desman notes the source of awareness content as "Baseline policies, standards and procedures are the foundation of this concept" (2003, p. 2). Individuals with more ISA knowledge about security practices have a greater base of ISA knowledge to share should they choose to advocate to others about good information security behaviors. Unfortunately, we still do not know if ISA knowledge is simply a necessary characteristic or a sufficient one to explain *advocacy behavior* on the part of middle managers. Rich feedback on self-reflective levels of knowledge in information security awareness could indicate positive attitudes toward ISA advocacy.

> *Working proposition 1: Feedback on self-reflective levels of knowledge in information security awareness indicates managers are sufficiently exposed to ISA content.*

Research Question 2: What are members of middle management currently doing about advocacy of information security awareness?

Discovering the present *advocacy behavior* helps researchers strengthen the validity of the action research findings and helps the organization reach the goal of increasing information security awareness by spreading the word. Discovering present practical organizational activities could also help define roadblocks or identify opportunities to propose recommendations for awareness program improvements. Members of middle management alone will not drive dissemination; however, they can be great contributors, since “role models are the major determinant of the level of ethical or unethical behaviors in an organization” (Falkenberg & Herremans, 1995, p. 139).

> *Working proposition 2: Self-reflection on present advocacy behavior projects positive attitudes and increases motivation to propose and take action toward sharing ISA with employees and peers.*

Research question 3: Have members of middle management identified any factors that affect their or peer managers’ ISA *advocacy behavior*?

Members of middle management have a unique point of view. Understanding the attitudes, perceptions, and values may lead to recommendations for the organizational ISA practices. The managers’ influencing factors for engaging is ISA may include the media and delivery methods used to disseminate the information. McLean (1992) notes “despite the popularity of brochures and newsletters articles, the respondents felt they were not effective in selling the message” (1992, p. 186). The media is only one of the potential challenges to advocacy behavior. We need more data on other inhibitors.

> *Working proposition 3: Discovery of organizational and personal attitudes and motivations enabling or hindering ISA advocacy, including the media used to communicate about security practices, provides the organization with recommendations for changes to increase the ability to practice advocacy behavior.*

Research Question 4: Do Action Research workshops have a measurable impact on positive ISA behaviors among Middle Managers who participate?

Using action research design has the goal of increasing the participants’ knowledge and motivating change through practice. In their 2006 book, McNiff and Whitehead presented the main reasons for doing action research as: *"*You can improve learning in order to improve educational practice. Second, you can advance knowledge and theory, that is, new ideas about how things can be done and why" (Introduction section, para. 2).

> *Working Proposition 4: An Action Research workshop contributes to participants learning, and to improvements to practice through participants contributions to increase ISA advocacy.*

Overview of Theory

Action Research is both a theory and a design. The theory of Action Research argues that through the process of the research, both participants and researcher are "increas[ing] opportunities for learning" and "producing ideas which can influence the learning of others" (McNiff & Whitehead, 2006, introduction, para. 4). In addition to increased learning, "*as a practitioner-researcher, you are aiming to generate theories about learning and practice, your own and [those of] other people* (McNiff & Whitehead, 2006, introduction, para. 2). An Action Research approach is valuable in terms of increasing the security posture of the employees and the organization by discovering improvements to practice or new methods for sharing security-related information. It takes the ISA lessons learned from the known reality, as it is perceived by the research participants and through the Action Research workshop, and transforms these lessons into a path toward developing organizational best practices that include information security awareness as a routine, living cycle of sharing information. This dissemination cycle starts with the use of ISA as a tool for delivering information that is learned, and when understood, is shared, and through sharing retaught again using the same tool.

However, advocacy researches draws upon other theories of change and self-change. As my research attempted to evoke action-driven change by middle management, I looked for a theoretical proposition to guide the fact-finding focus. My thinking shifted to evaluate whom or what is driving change, the organization or the middle managers. Kritsonis (2005) introduces a change theory developed by Lippitts, where the focus is on "the change agent rather than on the change itself (as cited in Kritsonis, 2005). The phases of change in Lippitts change theory include "diagnosing a problem, assessing motivation and capacity for change" (as cited in Kritsonis, 2005), which take in consideration the resources that could affect motivation, and setting an expectation toward a path of desired change. Throughout the research, I sought to diagnose reasons a manager would behave in favor of increasing ISA advocacy, including personal attitudes, gaps in ISA knowledge, or perceived *challenges* affecting a manager's *commitment* toward sharing ISA. I also sought to understand if an Action Research intervention, in the form of an ISA Advocacy Workshop, changes ISA *advocacy behavior* among the participants.

Overview of Research Design and Action Research Methods

The study approach is participatory action research. The nature of action research includes the investigative portion of the study, as well as the intent to introduce change. *Awareness knowledge, advocacy behavior* management or*, commitments, constraints, were* proposed to influence *advocacy behavior* of the study participants, (members of middle management). *Advocacy behavior* may be desirable, but not feasible due to lack of resources or other individual limitations. A participatory action research approach expands our understanding by considering middle management's perspective and potential ideas that could contribute to future *advocacy behavior*.

The researcher in the study maintained a subjective approach as the intent of the study was to discover and understand reasons influencing ISA advocacy. The initial aim was to create awareness of ISA *advocacy behavior* in order to gather ideas from the participants to motivate ISA advocacy. Leveraging participatory action research enabled the interaction between the researcher and the participants to contribute ideas and recommendations that would lead to improvements in practice.

There are several important components of action research design. The literature highlights significant constructs to explore through the participatory action research activities to help explain the influences toward ISA *advocacy behavior*. The participants in the corporate environment contributed solutions toward increasing the desired behavior based on their experience in the current business practices. The researcher contributed clarity and understanding of middle management's ability and motivation to increase ISA *advocacy behavior* by continually making "sense of the accumulating experience" (Iversen, Mathiassen, & Nielsen, 2004, p. 405). The study findings of ISA motivating factors became an opportunity to apply to practice the study's lessons learned. In summary, the action research outcome can introduce organizational changes that target the desired behavior by increasing the ISA knowledge, reinforcing management values, or enhancing the dissemination program. The study intended to have immediate relevance toward contributing change by looking at the participants' responses in order to tell the story of what triggers their motivation to practice ISA *advocacy behavior,* as well as to listen to which potential changes should be considered.

Action research (AR) seeks to solve an issue or bring change to the issue at hand, unlike other research methods that investigate an inquiry only. The researcher's role is not limited to the study of the phenomena; there is a practical application to the findings, often leading to recommended changes. Often, this method is a collaborative effort between the researcher and the entity that is experiencing the issue: "Theorizing is shared between the researchers and client participants because each brings their distinctive set of knowledge into the action research process. Action researchers bring knowledge of the action research and general theories, while clients bring situated practical knowledge" (Baskerville & Myers, 2004, p. 330).

The Action Research workshop was the tool used to achieve the inquiry. The workshop was an event where the managers were invited to discuss topics related to information security, assess, and develop, from their point of view some potential action-driven changes to increase ISA advocacy. At a glance, the workshop design included a security awareness presentation to set the tone of the activities. The inquiry exercises included an individual ISA knowledge self-assessment about security awareness. A group discussion explored *constraints* and *challenges* toward advocacy, recommendations, and *commitments* leading toward future ISA advocacy behaviors.

Exploring motivating factors resulted in a multidimensional perspective that included learning, self-reflection, creating awareness, and asking for information. Through group dialogue with members of middle management, the researcher learned their perceptions and attitudes, as well as detailed information contributing to ISA advocacy. "The pedagogic function basically involves collective engagement designed to promote dialogue and to achieve higher levels of understanding" (Denzin & Lincoln, 2011, *Multifunctionality and Focus Groups*, para. 3).

The action research design created a mutually beneficial growth in ISA knowledge and practice for the organization and the research since it contributed to practical solutions toward the problem statement investigated. It affects growth for the body of knowledge (research approach, data, and theories) and the participatory practice (results, recommendations to action).

Contributions

The study contributed a description of potential organizational and individual factors influencing ISA advocacy. The main research topic revolved around the role members of middle management, (from several organizations), played in information security awareness and risk avoidance by identifying attitudes, perceptions, and values enabling or preventing ISA advocacy. In 2008, Choi and colleagues reported through a study published in *Information Management & Computer Security* "an absence of empirical studies examining the relationship between managerial information security awareness and managerial actions toward information security in an organization" (2008, p. 485).

Several perspectives should be considered when questioning the importance of learning how to motivate managers. Exploring motivations that lead toward *advocacy behavior* can provide a way of extending the ISA message beyond a single presentation of information, "ensuring that security awareness occurs both in the first instance and as an ongoing factor of an organisation's operation" (Furnell et al., 2002, p. 352). Most perspectives are explained by asking the question "What is in it for _____?"

- *What is in it for the researcher practitioner?* The researcher benefited by creating alignment between a job-related topic and an action research approach. This alignment of interests allowed the researcher to maximize the knowledge based on practical experience with the knowledge acquired from the literature.
- *What is in it for the participants?* The participants had the opportunity to contribute their perspective on motivating factors to practice *advocacy behavior*. These opinions and recommendations provided insights needed to better disseminate information security awareness. This experience also gave the participants a voice that could influence the flow

of organizational practices. The group discussion was an ISA opportunity itself, as "awareness activities aim merely at attracting the attention of individuals to the subject, in our case security, and at allowing them to recognize the concern for information systems security and to respond accordingly" (Katsikas, 2000, p. 130).

- *What is in it for the organization?* The participating organizations benefited from a data set collection, manager's feedback, and recommendations for information sharing improvements. This information aimed to increase the reach of the awareness message and to raise the effectiveness of ISA. The research contributed a perspective to the overall risk posture of the organization. An inherent benefit is gained when employees have a better understanding of security; consequently, they are less tolerant of risk.
- *What is in it for society?* By managing information in a reasonable, secure way, society benefited from increased confidentiality and integrity of their private information, as well as the applicable lessons learned for personal information security.
- *What is in it for the industry?* Given that organizations have similar *challenges*, it is beneficial to other companies to gain a perspective that could contribute to their own ISA security best practices. In other words, the lessons learned from this are generalizable to others.

It is also important to ask, *what is in it for the existing research?* This study contributes to the body of literature on action research design, as well as to research on information security awareness and the role of the middle manager. It adds to our understanding of how to influence positive change in the Information Security discipline.

Summary

This chapter introduced the study's research setting as information security awareness in various companies. This research focuses on whether Action Research workshops offer a viable approach to influencing non-IT managers to advocate IT security, even though it is not part of their formal job responsibilities. The inquiry focuses on the middle manager as the driving force to contribute action-driven change to increase the spread of awareness education.

This research studied the middle manager's level of ISA *knowledge*, existing ISA *advocacy practices*, *challenges*, and *commitments* to contributing to information security awareness and advocacy. Through Action Research workshops, the researcher solicited feedback and recommendations that may improve the spread of ISA by engaging middle managers as change agents. Chapter 1 also emphasized the practical, research motivation for the study and summarized the findings and contributions.

In chapter two, I review the literature supporting my epistemology (action research methods) and ontology (pragmatism) position, and alignment within the study. I also explore the constructs of *awareness knowledge, advocacy behavior, challenges and commitments* that were introduced in chapter one, and which are the focus of my data gathering inquiry. Literature is presented on current knowledge, gaps in information security awareness, and contributions from other disciplines as it relates to my research topic. Chapter 3 details the action research design, process, and instrumentation. Chapter 4 presents the analysis and interpretation. Chapter 5 concludes with a comparison back to the literature, implications, and recommendations for future research and practice.

Chapter 2: Literature Review

Introduction

Chapter 1 introduces the context of the research and the research problem. The subject matter of the study is information security awareness (ISA) and advocacy. The research attempts to identify organizational and personal factors motivating middle managers in favor of information security awareness advocacy and to evaluate the impact of an Action Research ISA Workshop as an influence on such behaviors. The results are lessons learned for action driven changes that influences middle managers' ISA advocacy as a best practice. The setting for the study represented here was three businesses willing to participate and benefit from the awareness exposure to improve their security positions.

My worldview approach for the study is pragmatic. Since the research is an empirical study and uses a real-world scenario, it seemed fitting to evaluate factors such as *awareness knowledge*, behavior changes, and attitudes experienced by middle managers towards information security awareness advocacy. These factors are issues influencing middle managers in favor of ISA advocacy, which is also the "*known reality"* from the manager's perspective. Accounting for the known reality sets the stage for eliciting participants' recommendations and clears a path for action-driven change that increases ISA advocacy by middle managers, which is the "desired reality*"* (Goldkuhl, 2004) of this study.

The recommendations for change come from the study participants, a group of middle managers from the participating organizations. The middle managers become the change agents according to Lippitt's phases of change theory. See Kritsonis (2005) change centric study.

Information Security and Awareness

My literature review was initially driven by my work experience and prior knowledge. My work background is technical, and my work experience has been focused on risk management of information security. The majority of my job-related tasks and interactions are concentrated on the security of data, applications, and infrastructures. As mentioned earlier, it was through my work involvement in information security awareness (ISA) presentations that I began to see potential research opportunities. Specifically, when managing an ISA event, I noticed missed opportunities for audience engagement and began to question what was keeping more employees from taking advantage of learning about information security awareness. Since the setting of this study takes place in the participants' organizations, which are not my place of employment, it increased the value of focusing in members of middle management with the idea that this group would be able to influence their own employees and peers through later advocacy activities. It also decreased my direct influence, reducing bias and allowing me to explore the variables from the literature.

The topics for the organization's informational sessions were related to information security. Participants were presented with the intent to create awareness on the topic and its potential impact on their personal and organizational environment and to send a call to action for the audience. Several sources serve as contributors for topics of awareness. Examples include changes in the industry as digital environments provide new ways to process information, communicate, or access information and enhance ways of interacting with other people. These changes in technology bring threats often not considered or appreciated by those who use it. Loch, Carr, and Warkentin (1992) describe these threats as "a gap between the use of modern technology and the understanding of the security implications inherent to its use" (p. 173).

Threats are actions taken against organizational or personal assets, which include information, money, and resources. A threat, when executed successfully, whether by mistake or on purpose, is called an incident, a term used in both practice and literature (academic or gray).

In their 1992 study, Loch and colleagues focused on measuring members of executive management's concern for risks and the threats that come with the use of technology. Their study explores executive management's understanding of the existing threats to the working environment and the sources of these threats. It also explores executive management's understanding of risks when using a new technology. Understanding the threats to the working environment is important, since it helps management make investment decisions meant to mitigate threats. "Protecting the corporation's information system and data warrants management's attention" (Loch et al., 1992, p. 173).

New technology developments bring changes in the working environment, particularly the computing environment. Since the writing of Loch's study in 1992, there have been significant changes in computing architecture. For many companies, these include shifting from an isolated to a networked computing environment, hence expanding the points of entry for threats. In addition, the accessibility of the Internet adds another level of threats. Some companies have shifted from mainframe centric to distributed environments that include end-user stations. Every technology end-point contributes to the expandability of the work environment and brings potential threats that must be considered as part of the investment decision. Drawing consciousness to threats should be part of an organization's approach to addressing concerns. Otherwise, how could managers protect corporate assets if they had no awareness of the matter?

In Loch's study, the sources of risk and threats were initially drawn from the literature, and then compiled and shared with a group of executive managers to provide feedback on the threat's validity. I determined this to be important in my own research as organizational or personal factors affecting awareness are identified; however, my target participants are in a different management group and may perceive them differently based on their context, knowledge, and experience.

(Loch et al., 1992, p. 176) contribute a model that serves very well to create awareness of the sources of information systems security. The model explains threat sources from a four-dimensional perspective; they are "sources, perpetrators, intent, and consequences". This threat model is still applicable to present information security practices, and it can serve to help create awareness about information security.

- *Sources*, meaning an employee or another person with ill intent, can be both internal and external to the organization.
- *Perpetrators* include the actors initiating the threats or attacks, which can come from either a person or an automated machine.
- *Intent* speaks to the reason behind the act. Some threats are started by accident or by employee error. Other attacks are meant to cause harm.
- *Consequence* speaks to the motive for the attack, which includes disclosure, modification, destruction, and denial of use.

An increased understanding of security threats contributes an opportunity and motivation for members of middle management to share information security awareness in the organization. With present uses of modern technology such as wireless grids and social media, information security awareness artifacts and programs have become instrumental tools for creating consciousness about the potential threats management should consider when making investment decisions and promoting ISA.

Industry information security incidents are often a topic of security awareness informational sessions. These sessions show examples of situations where information is affected in a manner that causes harm to a person or organization. In these cases, information is disclosed, lost, used for fraudulent activity, or made unreachable. The security informational sessions include a call to action, which intends to help the audience understand what they can do to prevent a security incident. The session also highlights the organizational policies and guidelines that serve as best practices in an attempt to help the audience understand why the guidelines exist.

Wada, Longe, and Danquah (2012) draw several theories from the criminology and social disciplines. Their theories explaining cyber-criminal behavior gave me insights into common criminal behaviors leading to fraud. For example, cyber criminals use public tools such as e-mail to create an anonymous identity, which they often use as part of a fraudulent attempt called “phishing”. Phishing is a topic worthy of an awareness informational session to alert the public and aid to prevent them from becoming victims of cyber-crime. Wada et al.’s 2012 publication highlights the values of perception and behavior in the senior management of corporations. Their study provides examples of how social theories could be applied across discipline of criminology.

Wada and colleagues (2012) cite Denning’s (1999) “defensive information warfare”, which proposes that security policy training and awareness education prevent threats. Social theories provide guidance for protection against security breaches and misuse of information systems that have evolved through increased availability of online services, such as “banking, commerce and other financial services" (Wada et al., 2012, p. 2). That is, understanding events that occurred in the form of breaches or incidents and applying information security awareness is a preventive measure to influence end-user behaviors. Different theoretical perspectives apply depending on the point of view taken.

Wada et al. (2012) discuss perspectives from tree points of view introduced by Beatson (1991), Bray (2002), and Kabay (2002). The situational characteristics theory introduced by Beatson et al. (1991) is applied when examining situational use cases to evaluate end-user ethics. Bray (2002), argues that new users are more vulnerable to security breaches may be more applicable and the hierarchical level of the end-user experience helps predict the potential for breaches. Kabay (2002) introduces the use of psychology as a mechanism to influence end-user behavior.

These theories helped identify the many perspectives taken for my research and led me to consider my own research perspective. Thus far, I have taken an interest in combating the technology-driven concern of data theft by channeling preventive measures through individual advocacy, a social solution. My main interest is to appeal to those in leadership, (people with authority in an organization), to influence professional behavior toward advocacy for information security awareness. There is a need to understand the factors that might prevent managers from sharing security *awareness knowledge* in the subject area (What may be preventing them from sharing?) or their level of *awareness knowledge* (What do they know?). This process of discovery may reveal that leaders are provided a limited amount of information on the subject of ISA or that the expectation of sharing the awareness has not been understood. Is it a matter of influencing the corporate culture or could it be that the most senior leaders must buy into ISA messages first in order to provoke a trickle-down effect in communication? My research does not use the theories mentioned previously to explain behaviors; instead, I approach the participants directly, as the primary change agent, to gain an understanding of their experiences, attitudes, and *awareness knowledge*.

Dutta and Roy (2008) introduce the systems dynamics methodology as a "useful method to study IS problems" (p. 372). This methodology proposes a model to analyze systems loops and the effects among the constructs of perceived risk, investments in information security, and risk threshold. The paper suggests that exposing or sharing security incidents and the risk of vulnerability with the organization increases risk awareness and supports the investments needed to protect organizational assets. It aims to help stakeholders understand the relationships between IT and people's behavior, as well as "technical and behavioral security factors, along with their impact on business value of an organization's IT infrastructure" (Dutta & Roy, 2008, p. 1). The authors also propose that the *knowledge of risks* motivates employees to protect organizational assets, since security technology alone is not enough. Information security "involves a complex interaction between technical, organizational, and behavioral factors" (Dutta & Roy, 2008, p. 1). I draw from this research the suggestion of leveraging security incidents as a way to raise consciousness toward advocacy by helping the ISA audience understand how the security of their organization's technology may be affected by their own behavior.

Security awareness provides a way for employees to understand the potential threats within the organization and to use these insights as a learning tool for prevention of future risks. In their 2006 study, Chen, Shaw, and Yang "point out that lack of security awareness on the part of end users can lead them to miss common attempts to breach security" (as cited in Dutta & Roy, 2008, p. 1). These security lessons also serve as justification for organizational investments by executive leaders and as an educational tool for employees. Dutta and Roy (2008) combine the perspectives of social behavior, business values, and technical factors that affect risk management into a model to help explain motivation for better organizational risk management. “The model is simple in that it takes a high-level, aggregate view of both technology and behavioral factors” (p. 351). In 2002, Gonzalez and Sawicka (as cited in Dutta & Roy, 2008) proposed a framework for human factors in information security, noting that “any security system, no matter how well designed and implemented, will have to rely on people” (p. 351). Ostowan’s 2006 research (as cited in Dutta & Roy, 2008) contributes the construct and understanding of perception of risk as a motivator of security compliance: “A major motivator for end users to comply with [information security] policies is their perception of the risk of information assets being compromised” (p. 9). This strengthens the need to raise middle managers’ consciousness in favor of advocacy.

Will gaining a better understanding of the existing risk motivate managers to practice ISA advocacy? This study has an opportunity to leverage a research methodology that conducts inquiries of the participants’ understanding of risk as a motivation for *advocacy behavior*.

Middle Management

The literature in information security awareness is rich in program recommendations and end-user compliance (McLean, 1992; Katsikas, 2000; Siponen, 2000; Desman, 2003). That does not mean targeted security awareness training exists in any organization. This understanding led me to focus further on members of middle management as advocates of information security awareness. Middle managers have “the most influential role in large organizations” (Falkenberg & Herremans, 1995, p. 141).

The 2004 research from Grojean, Resick, Dickson, and Smith highlights organizational leadership's contribution to a value-based climate that foster ethics in the workplace. The study also discusses the mechanisms used by the different levels of management to channel the priority of ethics. It is about leaders' discipline and ethical conduct.

Grojean et al. (2004) theoretical background is based on social learning theory. It "provides some clues as to why leaders' behavior is influential in facilitating individual ethical behavior" (p. 228). Grojean et al. (2004) start by introducing the role of a leader. Leaders are driven by business goals; they set employee expectations on corporate standards and organizational values. The consistent practice of organizational aligned values, paired with leadership behavior reflecting these values, creates the image of normal corporate behavior. It is this perception of normal behavior that shapes the organizational climate. Zaccaro and Klimoski, (2001) describe the function of leaders as to "provide direction and facilitate the processes that enable organizations to achieve their goals and objectives" (as cited in Grojean et al., 2004, p. 224). "Leaders not only directly influence the behavior of members, but their actions also influence perceptions of members, which lead to norms and expectations of appropriate conduct that become ingrained in the organizational climate" (Grojean et al., 2004, p. 224).

Grojean et al. (2004) further argue that organizational *climate* is a factor to investigate as it relates to ISA advocacy. In other words, climate is composed of the attributes that are likely to influence employee perceptions of normal (normative) ISA *advocacy behavior*. These climates attribute aid in describing the ISA *advocacy behavior*. Grojean et al. also hold that "values of the organization, its leaders, and its members play important roles in shaping the organization's climate regarding ethics" (2004, p. 226). Here, the term *values* holds importance as a potential factor influencing ISA advocacy, since organizational values are shared through exposure or socialization in the workplace and the individual's experience. In the case of ISA advocacy, certain behaviors practiced in the workplace may stem from an organization's need to maintain a level of information security awareness maturity, which is growth that is reached through consistent best practices.

I leverage the approach by Grojean et al. (2004) to define the level of managers I choose to study. Higher-level leadership, which focuses on visions and strategies, is different from direct-level leadership, which directly interacts with a broader range of employees. Direct leaders are the link between organizations and their members (Grojean et al., 2004, p. 223). I equate the role of these direct leaders with members of middle management, who are the target for my research. Specifically, my research examines, by identifying factors that enable or prevent ISA advocacy, the role that members of middle management play in a company's information security awareness and risk avoidance.

Grojean et al. (2004) present seven mechanisms leaders use to send messages to influence employees, which are relevant to ISA advocacy behaviors.

- *Mechanism #1: Use value-based leadership.*

If leaders give attention to what they value, it is worth exploring the direct leaders' value for ISA as a way to discover factors influencing advocacy.

Are the direct leaders' values in alignment with the organizational ISA values?

- *Mechanism #2: Set the example.*

It is of interest to explore whether direct leaders (e.g. middle management) are presently behaving in a way that promotes ISA advocacy.

Do direct leaders consider themselves ISA role models?

- *Mechanism #3: Establish clear expectations of ethical conduct.*

Is the organization providing a set of policies and procedures to establish clear information security expectations?

Is the ISA program providing enough exposure to ISA to set clear expectations promoting advocacy?

- *Mechanism #4: Provide feedback, coaching, and support regarding ethical behavior.*

Are the direct leaders providing employees with coaching and feedback regarding the employees' individual behavior toward information security?

- *Mechanism #5: Recognize and reward behaviors that support organizational values.*

Do direct leaders appreciate ISA advocacy by rewarding behaviors?

Do direct leaders recognize or reward employees reflecting good ISA behavior practices in any way?

- *Mechanism #6: Beware of individual differences among subordinates.*

Do direct leaders customize coaching and feedback to the different personality types within the employee group?

What strategies are direct leaders presently using to manage the ISA climate?

- *Mechanism #7: Establish leader training and mentoring.*

Is the organization providing direct leaders with information security training that prepares them to practice ISA advocacy?

Do direct leaders have enough exposure to ISA knowledge? Is ISA socialized in ways that resonate with direct leaders?

Choi, Kim, Goo, and Whitmore (2008) studied the security awareness levels of management and compared it to managerial actions toward information security. "Information systems have penetrated every aspect of today's business processes, requiring organizations to implement comprehensive solutions encompassing physical, procedural, and logical forms of protection" (Choi et al., 2008, p. 485). They emphasized the importance "of security awareness as a first line of defense against unauthorized security breaches" (Choi et al., 2008, p. 485). Choi's et al. (2008) defines *awareness* and its importance in an organization:

> *Awareness is defined in the literature as the individual's passive involvement and increased interest toward certain issues, and it is considered one of the key components of consciousness-raising, the other being action. By staying aware of the current state of activities and threats related to environments, people are able to adjust their own work toward a common goal. Thus, awareness is about appreciating the needs, impetus, and specificity of issues, events, and processes (Choi et al., 2008, p. 486.*

Limitations to their study include its timing. The previous research may not be recent enough to cover contemporary views, and technological advances, including Web 2.0 and social media context. They further argued that there was "an absence of empirical studies examining the relationship between managerial information security awareness (MISA) and managerial actions toward information security (MATIS) in an organization" (p.485). This is not to say that papers on the topic of management information security awareness did not exist, but that there was little providing empirical evidence. In addition, "prior studies on ISA have mainly examined awareness at the employee level within an organization, not at the managerial level across organizations" (Choi et al., 2008, p. 485). They developed a model of MISA and MATIS to validate empirically the relationship between the two constructs. Their study compares manager's information security awareness with the actions taken toward implementing security controls and policies. In contrast, my research aims to discover motivations for “sharing awareness (advocacy)” as a way to extend the reach of the organization’s ISA communication.

Choi and colleagues (2008) reveal relevant literature examples of awareness in other multidisciplinary fields like social sciences, psychology, and information systems. This presents an opportunity to discover applicable attributes that fit the discipline of information security awareness.

Advocacy as a Catalyst of Change

Lippitt’s theory focuses on representing the people engaged in promoting change and on their roles during the phases of the change. “The focus on Lippitt’s change theory is on the change agent rather than on the change itself. Lewin’s change model attempts to analyze the forces (driving or restraining) that impact change” (Kritsonis, 2005, p. 6). This theory offers a framework or life cycle for the individuals or group serving as catalysts of change. The seven different phases highlight the key focus steps and serve as a progressive guide through the phases. The seven phases include: (1) diagnosis of the problem, (2) assessing motivation, (3) assess the resources and motivation of the change agent, (4) choose progressive change objects, (5) the role of the change agents should be selected and clearly understood by all parties so that expectations are clear, (6) maintain the change, communication, feedback, and group coordination are essential elements in this step of the change process, and (7) gradually terminate the helping relationship. These seven phases have potential usefulness in my research. As described by Kritsonis (2005), the following table maps my research with Lippitt’s phases of change. The concepts in Lippitt’s phases of change 1 through 3 can be matched to parts of the research question in the table 2.1.

Table 2.1: Lippitt's Phases of Change Related to My Research

My Research	Lippitt's Phases of Change
What motivates middle managers in favor of Information Security Awareness advocacy?	1. Diagnose the problem.
Motivating in favor of ISA advocacy	2. Assess the motivation and capacity for change.
Middle management	3. Assess the resources and motivation of the change agent.

Phases 4, 5, 6, and 7 would be implemented as guidance for the execution of recommendations.

My Research	Lippitt's Phases of Change
Organizational recommendations based on research conclusions	4. Choose progressive change objects.
Middle managers as advocates	5. The role of the change agents should be selected and clearly understood by all parties so that expectations are clear.
Information security awareness program	6. Maintain the change. Communication, feedback, and group coordination are essential elements in this step of the change process.
The promotion of advocacy may lessen, as advocacy becomes steady state and behavioral best practice.	7. Gradually terminate the helping relationship.

From Lippitt's seven phases, and previous literature, we can infer that motivating managers requires increasing their awareness of "the problem" as well as understanding their capacity for change. The variables to acknowledge are the constructs measured as part of the phase to assess the motivation:

- *Commitment motivation (attitudes, values) related to change*

- *Awareness (knowledge)*
- *Advocacy (behavior)*
- *Constraints (challenges)*

Variables

In this section, I review literature specific to the variables for my study: *commitment*, *awareness knowledge*, *advocacy behaviors*, and *constraints*.

Commitment (Motivation to Change, Attitudes and Values)

Whereas IT security personnel are explicitly responsible for ISA and security practices, non-IT managers are not. Clearly, the effective fulfillment of their work means following organizational policies and practices, however, actively advocating for information security awareness is outside of most middle managers official role. A non-IT manager's motivation to advocate ISA is intrinsically linked to his or her values and attitudes (Posner, Kouzes, and Schmidt, 1985; Rokeach, 1973). Similarly, any motivation to change their current advocacy behaviors is also linked to their values and attitudes.

Posner, Kouzes, and Schmidt (1985) highlight the influential power of values, both corporate and individual, and the importance of alignment. "Values are often considered the bedrock of corporate culture" (Posner et al., 1985, p. 293). At the individual level, "our values comprise the things that are most important to us. They are the deep seated, pervasive standards that influence almost every aspect of our lives; our moral judgments, our responses to others, our *commitments* to personal and organizational goals" (Posner et al., 1985, p. 294). At the organizational level, it is important to note which expectations related to *advocacy behavior* have been set for the middle management team. Furthermore, once an understanding of middle management’s *value* for information security awareness and its *advocacy* has been established, it can be compared with the organizational expectations relating to the matter. The two comparison points clarify the alignment status between the manager’s perspective and the organization’s expectations. “Any organization, in order to survive and achieve success, must have a sound set of beliefs on which it premises all its policies and actions” (Watson, 1963, as in Posner et al., 1985, p. 294).

Through research sponsored by the American Management Association, Posner and colleagues sent a nationwide questionnaire across industries of different sizes. The response rate was 25 percent of 6,000 surveys sent (N=1498). The purpose of the survey was to measure congruence of individual personal values with corporate values as an indicator of the “importance of the [alignment between personal and organizational values” (Posner et al., 1985, p. 295). The study shares several enterprise examples where leaders express the importance of alignment of corporate and individual values as part of a fulfilling career. As employees gain confidence and feelings of alignment with the organization, the organization benefits from a productive environment and lower employee attrition. These results also show the relationship between corporate value alignments and ethical standards. The higher the alignment of corporate and individual values, the higher the ethical standard to which the individuals adhere. The survey results further support the link between corporate value alignments and better ability to cope with job-related stress. Specifically, the lower the value congruence, the more likely the individual is to experience work-related stress that spills into family stress, unethical behavior, or unwillingness to act on the organization’s behalf.

With alignment of corporate and individual values, the importance of the corporation’s goals gains significance for those with greater value congruency than for those with less value congruence. As such, value alignment between the middle manager's perspective and the organizational values relates to information security awareness and advocacy. Corporate and individual value congruence is a factor to consider in ISA advocacy research in order to discover which organizational and personal factors motivate middle managers to practice *advocacy behavior*. This construct is of interest since high or low organizational-to-individual value congruence may influence productivity and other employee behaviors, either positively or negatively.

In his 1973 book *The Nature of Human Values,* Milton Rokeach explores common human values among different peer groups to infer personal priorities: In essence, everyone has a similar basic set of values, but not everyone assigns the same order of priority to the values. "A value is an enduring belief that a specific mode of conduct or end state of existence is personally or socially preferable to an opposite or converse mode of conduct or end-state existence" (Rokeach, 1973). He clarifies the difference between values and opinions, noting that a "value is a more dynamic concept than attitude, having more immediate link to motivation" (Rokeach, 1973).

Rokeach (1973) further explains the words chosen to define values. A value has the following qualities:

- It is enduring. Our values always exist, but our priorities may change during our lifetimes in response to life experiences or age differences.
- A value is a belief. It is a desired state, something a person wants to be part of. It can affect people at an emotional level. It leads or motivates an action or behavior.

- It refers to a mode of conduct or end-state existence. If a person believes the value to be of enough priority, it motivates that person to want to live in accordance with that belief.
- It indicates a preference, a goal, or something people want to reach. This is represented as the difference between where people are and how much closer they want to be to the desired state.
- It is socially preferable. It is a social norm accepted by peer groups.

He defines a list of terminal and instrumental values used to measure the differences between sample populations. Terminal and instrumental values are categories used to help define the function, purpose, or use of a value. Terminal values represent an end state, the expected consequence of living according to the priority given to a particular value. Instrumental values are the actions or behaviors a person does to help reach a desired end state. Since terminal and instrumental values help us understand the function of the value, they provoke *motivation*, which is an attribute of values. To pursue a value is to give a reason why people behave in a certain way to reach their desired end state.

Rokeach (1973) sees *attitude* as a term related to human values:

> *An attitude differs from a value in that an attitude refers to an organization of several beliefs around a specific object or situation" (1968). More than one attitude is grouped with an objective in mind that reflects more than one belief. An attitude, unlike a value, does not represent a goal or end state. It is a way of thinking about a situation that can be reflective of a value.*

In The Nature of Human Values, (Rokeach, 1973) provides several definitions of terms that help clarify the constructs to explore in the search for motivating factors affecting information security awareness advocacy. He describes the constructs of values and attitudes as intervening variables. He argues that understanding values, as the guides and inner goals that drive motivation, should help researchers predict behaviors. My study leverages feedback from an action research focus group (workshop) that questions the target participants about motivations.

Rokeach (1973) also describes the construct of values as an independent variable. In this case, through group discussions I intend to measure the perspective from the specific population sample (middle management). The data is validated with an analysis of the feedback of the awareness content presented.

Several ways exist to evaluate an individual's feelings about work; some good indicators are to evaluate the individual's work values or to look at the value congruence among other members of the organization. Value congruence or shared values can be an indicator of the climate within a group of peers, showing the feelings, group behaviors, and attitudes toward organizational commonalities.

Values "influence behavioral artifacts of culture, and provide justification for those artifacts" (Meglino et al., 1991, p. 482). That said *advocacy behavior,* if seen from the perspective of a behavioral artifact, would lead to a measurement of the value congruence toward *advocacy behavior*. Understanding what members of middle management think or feel about *advocacy behavior* serves as a factor contributing or hindering their part in the dissemination of information security awareness.

Organizational Culture and Security Leadership

The 1985 research by Posner, Kouzes, and Schmidt studied the importance of organizational values when they are clearly stated and communicated. It measured the appreciation and alignment (congruence) of organizational values in several levels of management across multiple industries. It examined what different companies are doing to successfully influence the organizational culture to align with the organizational values. This topic prompts exploration of the existing organizational efforts that support information security awareness and its advocates.

Meglino and colleagues define *work values* as “general modes of behavior that an individual ‘should’ or ‘ought’ to exhibit” (1991, p. 482). Work value congruence is an important construct from the perspective of its effect on the group’s exposed behavior of its own members. Organizational culture is defined as a state in which “employees with similar values are thought to interact with each other more efficiently. Thus, in turn, is believed to produce [a] more positive interpersonal affect” (Meglino et al., 1991, p. 482). They research middle management’s perspectives and attitudes as a collective or as a peer group. It gives the particular management group a voice to discern and communicate the reasons that enable or hinder *advocacy behavior*. The workshop instrument enables the setting in which the peer groups meet to discuss the subject. In the peer-group setting, people with similar work functions bring forth their individual perspectives. They have the opportunity to find similarities and differences based on their collective experience.

Leach (2003) addresses factors affecting employee security behaviors, the importance of information security awareness, and organizational recommendations to improve the security posture. Whether by mistake, or with malicious intent, internal security is a threat that specifically indicates vulnerabilities at the end-user level. The behavior of end users is a key threat to organizations, since they have a certain level of access by nature of being part of the organization. Their noncompliance with security best practices can place an organization in a vulnerable situation. Leach (2003) suggests using ways to “understand how a company’s culture and practices can affect people’s behavior” (p. 686) as a tool to manage the internal risk posed by end users. This is applicable for my research, since it prompts an understanding of present ISA best practices and an understanding of *advocacy behavior*.

Leach (2003) identifies three factors affecting end-user decisions on acceptable and unacceptable behavior: What they are told, What they see, and The end user experience.

What they are told. These are the organization's documentation guidelines, policies, and procedures. Often, a specific company security value is stated, but this is not always the case. Either way, the success of achieving the desired behavior depends on how well the documentation is prepared, as well as the "effectiveness at conveying what constitutes approved security behaviors, [which] varies according to: its accessibility; the completeness of its coverage; the clarity of the stated security values; the uniformity of its security values" (Leach, 2003, p. 687).

What they see. The examples set by the organizational management and peers influences the climate of acceptable behavior for the end users. Setting a good example is a way to influencing peers with actions.

The end-user experience. People make decisions every day based on situational experiences and on what they have learned. Not all organizational security "use cases" or possible scenarios are documented, so employees have to apply what they know and make a security choice that results in a behavior. End users apply the available information to make decisions about security best practice. This may include the documented guidelines, the examples set in the organization, and their own situational experience and values. Based on practice, industry-specific security incidents could be an example of the information available for making information security decisions. That said it would still be necessary to inquire whether the security incident bulletins affect the participants' own situational experience.

Leach (2003) further elaborate on the three factors influencing end-user decisions to practice the expected secure behavior:

- *The end users' personal values.* Most people have an individual sense of the values they follow that affects their ability to follow organizational values. When the values are congruent, end users adopts and complies more seamlessly with the organizational values. It is a win–win situation, since the end user does not suffer hardship, and the company values are being followed. However, problems may occur when values are not congruent: "Tensions can arise when there is conflict between the individual's values and the company's values" (Leach, 2003, p. 688).
- *Their sense of obligation toward their employer*. End users, specifically in employment situations, have expectations of behavior and a sense of loyalty toward their employer. Most choose to act within acceptable organizational norms because of their loyalty or mental "contracts" (Leach, 2003, p. 688).
- *The difficulty in complying.* This factor is important for all end users or employee expectations. If the organizational guidelines and policies are too difficult to maintain, it is likely that they will not be followed, simply because they are hard to achieve.

These factors are relevant to the research presented here. Middle managers' values, serving as role models, individual experience, ability to meet expectations, and personal feeling of obligation all weigh in as possible reasons why they would choose to practice advocacy in favor of information security awareness. Measuring for these factors helps in the exploration of the following constructs:

- ISA knowledge: The factor of “what they are told” (Leach, 2003, p. 690) brings clarity to the middle managers’ level of knowledge and its effect on *advocacy behavior*.
- ISA activities’ exposure: The factor of “what they see” (Leach, 2003, p. 686) brings clarity to the level of the middle managers’ ISA program exposure and its effect on *advocacy behavior*.
- Social norms: This construct is also affected by the factor of “what they see” (Leach, 2003, p. 686), since it brings clarity to the organizational climate or reflect what middle managers see as the example being set for them.
- Advocacy (behavior): This construct is also affected by the factor of “what they see” (Leach, 2003, p. 686), since it reflects what middle managers understand as normal behavior as it relates to *advocacy behavior*.
- Value congruence: The factor of “the end user’s personal values” (Leach, 2003, p. 688) brings clarity to the middle managers’ level of personal and organizational value alignment and its effect on *advocacy behavior*.

Ashkanasy and O’Connor (1997) explore how the leader–employee alignment of values affects the communication exchange of information. Leaders treat each employee differently based on the quality of “the social exchange with their leader” (Ashkanasy & O’Connor, 1997, p. 647). The greater the congruency, the more positive the experience will be. This could potentially be leveraged to explore the lack of leader–employee alignment regarding ISA and *advocacy behaviors* as a factor affecting middle manager’s actual ISA.

This theme is delivered in the Action Research workshop as *lack of realization that advocacy behavior or an understanding of information security awareness is expected*. The group’s dialogue may include topics of “members’ perception of similarities between their work values and those of their leaders” (Ashkanasy & O’Connor, 1997, p. 648). This would contribute organizational or personal factors to explain value congruency toward or against ISA advocacy. If the expectation is that a higher value alignment between leadership and middle management raises the social exchange of ISA advocacy, then the dialogue may be introduced differently. The dialogue in the focus group should include the middle managers’ understanding of the senior leadership expectation on ISA advocacy. It could be a contributing organizational issue of prioritization conflicts or a cultural misalignment.

Awareness Knowledge

Katsikas (2000) highlights the increased use of health information systems in all aspects of health care. Patient-related data are captured and processed as they relate to end-to-end patient care. This included patient data processing, as well as health diagnosis, treatment, and workflow processing. Katsikas (2000) also makes note of the transition in the environmental changes in the computing environment from stand-alone systems to networked environments. These changes expand the risks to the information system’s assets and the need for information security protection. In Katsikas (2000), the study attempts to identify the level of information security training needed by management of health care facilities, according to the management functions. Under the variable of knowledge, Katsikas (2000) defines three levels of learning needs, including *awareness,* which is informative; the learning objectives are recognition and retention. The level of learning *training* builds knowledge; the learning objectives are to build skills. E*ducation* is specialized training; the learning objectives are to the level of understanding. He defines awareness as a term used to draw attention to a topic. “Awareness activity aims merely at attracting the attention of individuals to the subject, in our case security, and at allowing them to recognize the concern for information systems security and respond accordingly" (Katsikas, 2000, p. 130).

Katsikas (2000, p 133) identified three levels of content for security awareness knowledge: *regulatory* is needed to be in compliance with a governing body; *policies* explain the guidelines established by the company; and *security controls* are the actual security implementations mandated by the company.

In my research, the variable *awareness knowledge* queries the leader to do a self-assessment of the level of learning needed. Gaps may exist in information only (informative), light training, or skills education. Assessing levels of *awareness knowledge* helps the researcher zone in on how comprehensive the leader's understanding of information security is. The *ISA content* covers the leader's assessment of the regulatory and security controls, as well as the policies materials presented. Feedback from the assessment may lead to recommendations for ISA program improvement. Comparing the feedback to the leader's job function helps identify opportunities for improvement in the level of learning. It is possible to identify gaps in level of learning by contrasting the feedback on *awareness knowledge* and ISA content. For example, low levels of *awareness knowledge* may indicate a need for increased exposure to content.

Siponen (2001) introduces different perspectives to categorize the depth of information security awareness that should be shared according to the audience group. His paper suggests that the level of ISA education depends on the level of technical exposure or understanding of the target audience. This means that the ISA message should be tailored according to the receiving group or person. For audience members who are in technical positions, the level of ISA education suggested may be more complex than for audience members who may just be casual end users.

> *"The scope of this paper is limited to setting up information security dimensions in terms of form and target groups by proposing a framework for awareness perspectives in order to raise certain issues and produce practical examples in the hope of inspiring further research and practical activities around the topic" (Siponen, 2001, p. 25).*

The paper proposes that anyone, whether a group, individual, or organization with exposure to information technologies, should receive the adequate level of ISA content. However, "target groups should receive only information that is relevant to their needs. As a result, there should be a classification of what is relevant/irrelevant information for each target group" (Siponen, 2001, p. 28).

In his paper, Siponen (2001) categorizes ISA as descriptive or prescriptive. *Descriptive* elements basically just share information security awareness, while *prescriptive* suggests that an action should be taken based on the information received. Both terms derive from the theory of universal prescriptivism. For organizations, the ISA shared is prescriptive, since it aims to modify behavior to protect the organization's assets. Within organizations, there are several target audience groups, which would suggest that the ISA message be shared on a need-to-know basis. For executive or top management, Siponen (2001) proposed providing ISA information that helped the executives understand the need for security. "Necessary information concerning information security issues must be shared and this information must be clarified to all the target groups to enable them to reach a state of commitment (the ideal state from an information security point of view)" (Siponen, 2001, p. 26).

Siponen's paper strengthens the argument for the construct of *awareness knowledge* and its relationship with middle managers. A self-description of *awareness knowledge* helps define if the ISA exposure is adequate for members of middle management. In addition, it helps determine if members of middle management understand the information presented and if the level of understanding of the information security awareness presented either hinders or enables *advocacy behavior*. These reflections may clarify whether middle managers are not practicing ISA advocacy because they do not understand the ISA material presented, or because it is not applicable to their business function. The ISA shared with middle managers should be at the level of complexity they need to know. A self-assessment helps identify the right level of information security awareness for middle managers.

Kevin McLean (1992) takes more of a marketing approach to addressing the need of ISA programs. In the study "Information Security Awareness—Selling the Cause" (p. 180), he first highlights the value of information as a factor to add value to a company when combined with ideas and intelligence. He notes that disseminating awareness information on its own is not sufficient to cause behavioral change. He stresses that people have to be told what to do with the information provided; therefore, a call for action. "The exact nature of the behavioral and attitudinal change we require depends on the role and seniority of each individual" (McLean, 1992, p. 180). If this were so, then what would be the expected behavioral and attitudinal changes we can expect from middle management? What type or method of learning would influence attitudes and behaviors to engage in ISA *advocacy behavior*? Will the delivery method significantly affect middle management's decision to share ISA content? My main interest in McLean's research is his marketing perspective lens. It is a point of view and language that is similar to the language used in practice.

McLean (1992) identifies marketing attributes and best practices applied towards ISA that may help motivate *advocacy behavior*; some of these include: structure and scope, designated facilitators, behavioral change and point of delivery.

McLean also argues that we must “appreciate that changes take time” (McLean, 1992, p. 184). From this perspective, potential research questions may include, do managers understand the scope of advocacy expectations? How effective are middle managers as IS advocates today? While McLean’s study (1992) addresses all staff members of an organization, my research focuses only on middle managers as target participants. Like McLean, I am looking for behavioral change and the manager’s perspective of the ISA content received.

- *Behavioral change,* McLean (1992, p.182). Since we cannot influence behavior without understanding it, as it exists today, it is important to evaluate whether the target participants understand the problem; this, of course, occurs after presenting the perceived issue. Do managers understand the benefits of sharing the perceived value of ISA?
- *Point of delivery,* McLean (1992, p.188). What potential delivery options are available? What, if any, do managers recommend as point of delivery for awareness information?

Challenges and Constraints

Based on practical experience in the information security field and research in the literature, factors that negatively affect advocacy best practices may come from a variety of sources. Some potential reasons include the following:

- The information provided is not relevant enough to share. “Target groups should receive only information that is relevant to their needs. As a result, there should be a classification of what is relevant/irrelevant information for each target group” (Siponen, 2001, p. 28).

- The audience does not understand the importance of the information presented, "lacking the understanding of, or being dismissive of, the risks" (Furnell, Gennatou, & Dowland, 2002, p. 353).
- Managers do not think it is their place to advocate for ISA. Desman (2003) suggests, "Make it clear that performing a specific action in a specific manner is good for the company" (p. 4).
- The format of the information presented is overwhelming. "Do not bury people under verbiage" (Desman, 2003, p. 3); lengthy material may discourage managers from engaging in the awareness activity.
- Guidelines do not exist or are not easy to find. The body of knowledge includes "legal, regulatory, ethical information security policies and system security controls" (Katsikas, 2000, p. 133).

ISA Advocacy Artifacts

In this research, the Action Research workshop is the motivator that influences employees to ISA advocacy. The factors in favor of ISA advocacy come from the collective opinions of a group of managers who have direct influence over employees. Through group discussions, the Action Research workshop encourages middle managers to self-assess their level of ISA knowledge, provide feedback on the ISA content presented, and reflect on their personal ISA advocacy experiences. Rich feedback on self-reflective levels of *awareness knowledge* may indicate positive attitudes toward ISA advocacy or the need for training. Self-reflection of present *advocacy behavior* among members of middle management positions the organization to take action toward motivating middle managers to increase their sharing of ISA with employees and peers. Discovery of organizational and personal attitudes and motivations enabling or hindering ISA advocacy provides the organization with recommendations for changes to increase its ability to practice *advocacy behavior*. Ultimately, it is the managers' *commitment* to action-driven change that fuels future ISA advocacy increases as a best practice.

Although based on the author's experience rather than on theory or experiments, Desman's 2003 publication acknowledges a common challenge most organizations face*: the frustrations of getting users of information assets to contribute to secure behavior*. The audience for security awareness is defined as an end user who uses technology, but does not necessarily support its maintenance and functionality. Before disseminating awareness messages, it is necessary to identify who the end users are (the audience) and to gauge the present state of end-user knowledge (what do they know today?), and then create a message that resonates with the majority of end users.

An organization should have policies and guidelines to set behavioral expectations for end users. Security awareness is an informal training used to reinforce positive security behavior. In other words, employees are given access to organizational assets in order to perform a function. Security awareness helps them understand their role in protecting the assets, including the information assets. Both the technical artifacts and information are considered organizational assets. Awareness is a way to communicate a consistent message of everyone's role in order to protect the organization's assets. An awareness program should bring contrast to formal education; it is a good practice to identify which other tools the organization uses as informal and formal employee education to gauge the balance an awareness program brings to the table.

Desman notes the source of the awareness material as the "baseline policies, standards, and procedures [at] the foundation of this concept" (2003, p. 2). The article lists ten (10) tips that can be used as guidelines for assessing the current state of an existing program and the present ISA *awareness knowledge* held by members of middle management. The tips contain step-by-step best practices to follow with an awareness program. According to Desman, every organization should consider the following guidelines as they launch an ISA program (Table 2.2).

Table 2.2: Desman’s (2003) Ten Commandments of Awareness Training

I. Information security is a people, rather than a technical, issue.
II. If you want them to understand, speak their language.
III. If they cannot see it, they will not learn it.
IV. Make your point so that you can identify it and so can they.
V. Never lose your sense of humor.
VI. Make your point, support it, and conclude it.
VII. Always let the recipients know how the behavior that you request will affect them.
VIII Ride the tame horses.
IX. Formalize your training methodology.
X. Always be timely, even if it means slipping schedules to include urgent information.

From these, I can extract attributes that may be potential factors hindering or enabling *advocacy behavior*. Consider the first example about whether the recipient understands the material, from commandment II. This speaks to the complexity of the content presentation. Similarly, commandment V suggests that the tone of the awareness material remain digestible, meaning it is light and absorbable, and not overly serious. The tone used should be readable and should motivate sharing. It also can be seen as an attribute that enables ISA knowledge, making the marketing material understandable, digestible, and brief, as well as contributing to ISA-related learning.

Commandment III speaks to the availability of information. If the awareness material is not easy to find, it may hinder middle managers' ability to share. If the material is not conveniently found, then it cannot contribute to knowledge. Easy-to-find information also enables ISA knowledge from the perspective of the materials' availability to be shared.

Commandment IV basically says that there needs to be a reason why the awareness material is shared, and it is important to communicate that reason with the audience. That said middle managers might see this as a contributing factor to the decision to practice advocacy. Understanding why the topic matters to the audience and what they should take away from this message contributes to the value of the information being shared. Understanding the reason why may motivate middle managers to learn and share this information, which contributes to *awareness knowledge*.

The length of the awareness material is an attribute that encourages or discourages readers to share the awareness information. In the section of the article elaborating on commandment VI, Desman warns the readers to "not bury people under verbiage" (2003, p. 3). Often, lengthy material may discourage employees from engaging in the awareness activity.

Commandment VII motivates middle managers to practice ISA advocacy through understanding the expectations set for the reader. Middle managers may simply need a reminder or some instructions to engage them in sharing the awareness material with their employees. Setting the expectation also contributes to *awareness knowledge* as a motivator for learning the message sent. Desman's suggestion to "make it clear that performing a specific action in a specific manner is good for the company" (2003, p. 4) implies a win–win situation for all parties. The middle manager and the employees gain knowledge and the organization gains a better risk posture.

Commandment X highlights the importance of timely dissemination of information. Keep in mind what is hot off the press from the industry or frequently mentioned during a special organizational event or incident. Sharing the information in a timely matter would be an attribute to consider, given that the urgency of a subject contributes to how motivated middle managers are to share awareness information with their employees. This would affect the construct of ISA advocacy.

Furnell, Gennatou, and Dowland (2002) introduce *challenges* with ISA programs awareness and artifacts that exist in small organizations. While security-related concerns are present, the lack of dedicated resources and budget and time *constraints* limit the effort. This research proposes a prototype, self-paced educational tools to promote awareness on security-related matters, and security training. It suggests that organizations need a test environment to learn and explore security threats that are appropriate for the type of organization.

Furnell and colleagues (2002) use the 1998 KPMG information security survey for their own study. The survey indicated that inadequate end-user awareness was the most significant obstacle to information security. While numerous resources are available to provide security advice and guidance without incurring significant expense (e.g., books, websites, newsgroups, and e-mail lists), these do not offer the ability to test one's own understanding in practice. It is desirable to be able to perform such testing before being faced with the task of applying security within an organization (Furnell et al., 2002, p. 354).

Summary of Constructs drawn from the Literature

As preparation for the study, I drafted an excess number of questions based on the literature constructs with the intention of gathering the main topics of discussion to promote dialogue and engagement. As I drafted and edited the questions, I primarily focused on probing questions meant to generate discussions. I was mindful of wording questions in a way that does not prompt a yes or no answer. The lead-in comments and questionnaire items had to be neutral from the point of view of the literature constructs, with wording that addressed the group. My intent was to elicit responses from all participants, not just the first person who decides to contribute.

My research is intended to encourage members of middle management to both increase their knowledge of security awareness and act as action-driven change agents through advocacy. During the research workshops, the goal is to learn about potential gaps in managers' *awareness knowledge* and receive their suggestions for changes that can drive future sharing of ISA awareness. The middle managers can help the organization by sharing their security awareness with their employees. Overall, the workshops contribute a way to increase the overall security posture of the organization, to help the employees take actions that may be new, and to introduce them to activities meant to help them share security knowledge.

Not only is the research valuable in terms of increasing the security posture of the participants by revealing methods for sharing security-related information, it takes the ISA lessons learned from the known reality as it is perceived by the research participants and through the Action Research workshop, transform them into a path towards developing best practices that include information security awareness as a routine, living cycle of sharing information. The cycle includes using ISA as tool as much for delivering information as for learning, sharing, and teaching.

The data source for middle managers' perspectives comes from responses gathered in the AR workshop activities. Questionnaire responses with low scores in the areas of *knowledge,* *advocacy behavior, and commitment*, may be seen as "*challenges* and "*opportunities for learning"* and expectation misalignments in an individual's perspective. The major constructs used in this study are highlighted in table 2.3 to summarize its definition and measure according to the literature.

Table 2.3: Advocacy Constructs Summary Used in Study

Constructs to be Studied	**Definition/Measure**	**Sources**

Level of Awareness Knowledge	A measurement of the understanding of Information Security and Awareness. "While there are numerous resources available to provide security advice and guidance without incurring significant expense (e.g., books, websites, newsgroups and e-mail lists), these do not offer the ability to test one's understanding in practice".
	Low level of ISA knowledge - Lacking the understanding of, or being dismissive of the risks
	High level of ISA knowledge= (*Awareness knowledge*) allows them (end users) to recognize the concern for information systems security and to respond accordingly
		Furnell, Gennatou, & Dowland (2002);
		Deyhle (2002);
		Dutta & Roy (2008);
		Katsikas (2000)
		Siponen (2001)

Level of Information Security Awareness	Middle managers recognize the importance and share concern for information systems security, and have ability to respond
	Low level of IS Awareness - That lack of security awareness on the part of end users can lead them to miss common attempts to breach security
	High level of IS Awareness - Emphasize the importance of security awareness as a first line of defence against unauthorized security breaches.
		Katsikas (2000);
		Dutta & Roy (2008);
		Choi et al.,(2008)

Level of ISA Advocacy Behavior	The choice to engage in actions that share ISA knowledge or that seeks to influence the ISA behaviors. Security activities, whether in terms of science or practice, are mainly stimulated by a concern to prevent certain activities that are interpreted as abuses. Low level of ISA Advocacy Behavior - People defuse the importance of their role in IS security by behaving in ways that deny responsibility, justifying or ignoring the injury resulting from neutralization of risk. High level of IS Advocacy Behavior = Ensuring that security awareness occurs both in the first instance and as an on-going factor of an organisation's operation	Siponen and Vance (2010) Furnell, Gennatou, & Dowland (2002) Leach (2003)
Level of Commitment/Motivation	Awareness can be driven by the perception of risk; a motivator of security compliance, as described by Ostowan in 2006: "A major motivator for end users to comply with [information security] policies is their perception of the risk of information assets being compromised" (as cited in Dutta & Roy, 2008). "Necessary information concerning information security issues must be shared, and this information must be clarified to all the target groups to enable them to reach a state of commitment (the ideal state from an information security point of view)" (Siponen, 2000, p. 26). Expressed commitment to ISA *Advocacy Behaviors* as a result of any one of many internal or external causes (e.g. social norms, values, risk of financial loss, risk of damage to reputation or career, legal compliance, job responsibility, etc.)	Dutta & Roy (2008). McLean (1992) Meglino et al.,(1991) Rokeach (1973) Siponen (2000) Leach (2003)
Perceived Challenges and Constraints	Participants point of view of reasons limiting their decision in favour of ISA advocacy.(Attitudes, limited time, lack of knowledge, lack of awareness or understanding)	Furnell, Gennatou, & Dowland (2002)

Action Research Workshop/Focus Group

Although the dominant methodology is action research, I find the focus group both influential and fitting as part of the Action Research workshop. The focus group technique helps to develop awareness on how to communicate with the participants during the Action Research workshop. As the researcher, I looked to gather data through a group discussion. I sought a collective voice based on the collaborative contributions from the managers, not just individual thoughts. In addition, an understanding of the focus group technique set my expectations on group dynamics. Since the workshops generate group discussions, I expected group dynamics that included non-agreement within the group. This can actually be helpful, challenging the individuals to consider different opinions during the discussions.

Focus groups started in the 1940s following the Second World War (WWII) in order to study the propaganda that had been spread through mass media. Merton and Kindall were some of the first researchers to develop this method as a way to "get relevant, specific information from relatively large numbers of subjects quickly" (Kamberelis and Dimitriadis, 2003, the origins of focus group research, para. 1). The authors present considerations and perspectives for researchers to think through as they decide on methodology for a study (See Table 2.6). As I examined the inquiry intent descriptions, I reflected on my own intent for the study, to understand the perspective toward ISA advocacy held by members of middle management. I also referred to what is it about my topic that I want to learn, specifically, the motivating factors and attitudes held that move employees in favor of advocacy. Table 2.4 show methodology examples, introduced by Kamberelis and Dimitriadis (2013), I considered as I planned to develop my study.

Table 2.4: Examples of Inquiry Approaches

Approach	Intent of Inquiry
Extensive observations	Studies in a natural setting Document and understand activities and practices
Quasi-experiments *Experiments*	Information reveals itself Researchers create situations in which people demonstrate skills or knowledge
Individual interviews	To reveal experiences and issues that really matter in a person's life (like grief or loss) To understand the participants' durable disposition (long-term inclination) and orientation to social activity in issues
Focus group	To generate information that is richer and more focused, complex, and nuanced, especially in relation to certain topics

My intention was to understand the collective attitudes and perspectives of members of middle management as a community and to think of the participants as the influencers of change in favor of ISA advocacy. The three key descriptors, collective attitude, community, and cause, contribute influence(s) from the focus group technique to the Action Research workshop.

- Extensive observations would not have been the best fit since they would lead to spending considerable amounts of time in the individuals' natural settings waiting for the phenomenon to occur on its own.
- Quasi-experiments and experiments would have given the participants an opportunity to reveal manifestations of ISA advocacy. However, this method may not have explained the reason why the participants chose one situation over another.
- Individual interviews could have created deep understandings from a selected number of middle managers. Still, this method represents the perspective of individuals, not

necessarily the perspective of a community. Individual interviews do not create a setting for collective dialogue and exchange of ideas.

- The focus group nature of semi-structured dialogue can create consciousness on the topic, and the group participation allows for contribution of ideas in favor of ISA advocacy. As a community, the participants have the opportunity to generate collective recommendations in support of or against ISA advocacy expectations. Kamberelis and Dimitriadis (2013) highlight three major functions of a focus group "pedagogical, political, and the empirical" ("Appropriation and use of focus", para. 7) that fit very well with my research objective of discovering motivating factors in favor of ISA advocacy through the Action Research workshop's.
    - *Pedagogical:* an ISA learning opportunity. The focus group discussion may evoke dialogue that transforms the participants' perspectives on the subject.
    - *Political:* an ISA advocacy opportunity. The focus group discussions may gather support in favor of ISA advocacy.
    - *Empirical:* an ISA advocacy data-gathering opportunity. From a pragmatic approach, the group discussions generate data on attitudes toward ISA advocacy as they are experienced by members of middle management.

My focus is specific to finding attitudes and perceived factors in favor of ISA advocacy; this methodology gives me the flexibility to focus the discussion topics and "group data gathering strategies" (Kamberelis & Dimitriadis, 2013, Focus groups, para. 5).

Focus Groups within Action Research

Kamberelis and Dimitriadis (2013) describe Participatory Action Research (PAR) as a method that engages its subjects from beginning to end: "PAR typically involves participants in the entire research process from the definition of the problem though the research itself through the dissemination of results" ("*Creating opportunities for solidarity",* para. 1). This has been my experience through the development of my research. I consulted with the organizational program that manages information security awareness to determine if there was a need for research. I also worked with professionals in discussing and visualizing the possibilities for research development and the uses for the data analysis. The problem definition started by considering opportunities in the ISA space and how the research itself would create awareness. I held a monthly meeting with two members of the program leadership to keep them informed about how my research was progressing and to validate that the end goal and end result were in alignment with results that would be useful for the organization.

Some topics of discussion included the participants' protection from harm and the knowledge that confidentiality was not guaranteed due to the nature of the method. In group discussions, the researcher is able to conceal the participants' identities, but cannot control their conversations after the group event. This detail must be disclaimed in the Institutional Review Board application, as well as clearly stated in all consent forms and articulated at the beginning of the focus group event. As the research progresses, there is a continuous need for keeping both the research committee and the organizational sponsors informed through discussions and full disclosure. Both entities have to approve in order for the research to continue to its end state. Tuck states (as cited in Kamberelis & Dimitriadis, 2013) "PAR is best described as an ethic, as a set of beliefs about knowledge, where it comes from, and how it is validated and strengthened" ("*Creating opportunities for solidarity building"*, para. 1).

Focus Group Affordances Applicable to the Action Research Workshop

Kamberelis and Dimitriadis (2013) describe the flexibility that is possible with a focus group due to the nature of the group setting:

- *Mitigating the authority and generating deeper understandings.* The researcher is encouraged to initiate dialogue and to empower the participants to take over the discussions as a way to gain insights that may be missed if the researcher tries to stick to an agenda. The discussions may take an unexpected direction that can reveal sensitive material or subjects the researcher had not considered. These unexpected discussions tie in with drawing out complexity, nuance, and contradiction, which is also described as an affordance this method accommodates.
- *Disclosing the constitutive power discourse and the lifeblood of the social activity.* The participants in the group discussions are a defined set of managers who are selected based on their functional job description. It is a homogenous group from that perspective, as its members share commonalities that are unique to their job function. A focus group affords these participants an opportunity to reveal the behaviors, perspectives, and opinions that may be suited to middle managers. It is possible that this group represents power and social activity that would (or would not) be in favor of ISA advocacy.
- *Approximating the natural.* The authors stress the importance of making the participants feel safe and at ease as an aid to establishing a comfortable discussion environment. The application for my research is to conduct the group discussions in the organization where the

participants work. The recruitment tools and invitations to the event are made using organizational tools for e-mail and meeting invites that the participants use regularly. In addition, the meetings are held on the organization's premises, in a conference room within the building. This familiar setting approximates meetings that would occur for any other work event. The meetings are held during working hours upon approval of the participants' manager.

- *Filling in knowledge gaps and saturating understanding.* Through the group discussions, the feedback on the ISA content (events, ISA presentations, and industry trends bulletins) may reveal attributes or factors that were not expected. For example, an article written about a particular subject may be described in the presentation in debt, while the focus group feedback on the same article may reveal that participants consider the content too complex or written in language that is too technical. The contrasting results help the researcher understand that the content provided is not affecting the audience as expected; furthermore, it may contribute as a factor not in favor of ISA advocacy.
- *Disclosing eclipse or invisible connections.* As the participants engage in group discussions, they may reveal gestures, comments, and ways of expressions that are unique to the community. These are described by the authors as invisible connections. These disclosures may not be familiar to the researcher or may not be described by the literature. They can likely be unique to the corporate culture or the management community. As the group discussions progress, the researcher may not notice the phenomena right away. It may be that during data analysis, while re-listening to the recordings or reviewing the transcription, the researcher discovers a point of interest that may turn into a reportable result.

- *Creating opportunities for solidarity building and political action.* My research enables and encourages the participants to join together in recommending ways that the organization and or the ISA program can present the ISA content to increase the chances for advocacy. It also allows the managers to voice concerns about ISA advocacy. Regardless of the sentiment expressed, the focus group is an opportunity for information security awareness as much as an opportunity for the middle managers to contribute feedback to the corporate ISA program for making recommended changes.

This collective voice is the strength of the focus group, one that could serve as an educational opportunity to both the organization and the participants. The organization gains the feedback and understanding of factors affecting advocacy and the participants gains raised consciousness of the value of information security awareness, which may work in favor of ISA advocacy. The community discussions creating a collective voice could not be reproduced by conducting individual interviews.

The Importance of Facilitation

The researcher leads the group discussions with semi-guided questions (See Appendix 6: Treatment Part 2: Action Research Action Exercise), with the intent of taking a more passive and non-directive role as conversation picks up to allow the group dialogue to take over. This is to allow every opportunity to discover invisible connections and facilitate free-flowing dialogue and other affordances that are possible with a less restrictive strategy. This method differs from structured interviews, where more directed researcher participation is needed. Not knowing what to expect from group to group, it is hard to predict the natural rhythm of the discussions; the flow of the conversations may be fast and steady or may begin slowly and increase in pace as the participants feel at ease during the progression of the conversations. Either way, as the researcher, my focus is on listening, giving acknowledgment and feedback, taking notes, and contributing probing follow-up questions to solicit more details and commentary.

Summary

In this chapter, I review literature used for the development of my research. Starting with the context of the study, information security and awareness, this review is based on my practical experience as an information security professional. The point of view is not focused on the technical details of information security, but on the attempts to educate and raise consciousness on the topic among the consumers of the information. Although many working environment manage the IT controls established to protect and safeguard corporate and personal information; the awareness education attempts to help the end users understand the security threats in the digital environment and the controls placed by the corporation as safeguards. Furthermore, the ISA sessions strive to create awareness on security topics so that the recipients may learn how the use of information affects them and what they can do to avoid, manage, and prevent information risks. The topics for the ISA informational sessions also cover industry incidents, which are drawn from a variety of industries like health care, and the use of tools available to the public, such as social media channels.

As my focus is a pragmatic approach, the development of this chapter centers on the known reality. My observations and wording of the problem statement, the stakeholders, and potential ways of managing the research are documented from real-life scenarios experienced in the participating organizations.

The body of the research revolves around both understanding the motivations, knowledge, behaviors, and attitudes experienced by the study participants and creating behavioral changes through actions they suggest. The participants of the study are a group of middle managers, chosen for their direct alignment with and influence on the employees, who are also the general audience of the organization. My intent in selecting middle managers as the participants for the study is to gain an understanding of motivating influences affecting ISA advocacy.

As middle management (i.e., direct leaders) takes center stage in the study, this research positions them as the champions of change. The change agent is the driving force of the desired shift in favor of ISA advocacy. As such, the study aims to understand the known reality from middle management’s perspective in order to set a path toward the desired reality. Through their influence on the employees, the change agents can best share recommendations on improving the reach of the awareness messages.

In chapter 3, I provide details on my methodology, including the action research process, instrument development, and techniques for data analysis.

Chapter 3: Research Design and Methods

Pragmatism

Before proceeding further, it is important to understand how pragmatism aligns into an action research design. Unlike worldviews that deal with an expression of ideas or concepts, pragmatism looks at the situation of interest from the perspectives of known reality and desired reality. From Goldkuhl's (2004) study, I drew upon the pragmatic perspective to help shape my research question. His study is based on the organizational and information systems, whereas my research is focused on organizational and information security awareness. Information security is a subset of information systems, and both are a subset of information management.

Goldkuhl (2004) suggests principles to consider as a practical guide in conducting research, for example, "the meaning (of an idea or concept) is the different actions, which we conduct, based on the belief of this concept" (p. 13). These principles apply to my study in all phases, starting with using action-driven words in the research questions, taking action to conduct the research, measuring actions as part of the data collection, and suggesting actions as part of the solution to the research problem. Table 3.1 below summarizes Goldkuhl's principles.

Using Goldkuhl's 2004 text as a guide, I have shaped my research question to reflect pragmatism, the known realities, and the actions and potentials that changes based on action can deliver. In my research, the known reality of the theme of the project includes the action of advocacy in the ISA field. The known reality and the potential that change can offer as a consequence to actions is the setting of this study, the people receiving ISA education, the stakeholders in the ISA program, and an unknown area of the boundaries influenced by ISA advocacy. The application of the pragmatic point of view to my initial research question leads me to consider modifications to reflect the practical approach of the study.

Table 3.1: Goldkuhl's (2004) Research Principles

Goldkuhl's (2004) Guiding Principles For Conducting Research
The meaning of an idea or a concept is the practical consequence of the idea/concept (2004, p. 13).
Pragmatism means an interest for action (2004, p. 14).
Pragmatism means an interest in action in its practice context (2004, p. 16).
Pragmatism means an acknowledgement of action permeation on knowledge (2004, p. 18).
Pragmatism means an interest in practical consequences of knowledge (2004, p. 20).
Pragmatism means an interest in what works and does not work (2004, p. 21).

The starting point in evaluating my study's research question is to ask how Goldkuhl's (2004) principles guide my research into action and research development. My initial research question—which factors motivate members of middle management to become ISA advocates?—begins by asking which influences should prompt me, as the researcher, to inquire about different motivations for members of middle management. The principle "Pragmatism means an interest for action" (Goldkuhl, 2004, p.14) prompts me to question what main actions are stated in my own research question. *Motivate* is the verb suggesting action for change. The expected consequence for the word *Motivate* would be initiative.

The motives reflected in peoples' actions imply that the environment effects change in the middle manager. Information would flow from the stakeholder to the middle manager in an attempt to influence a behavior. The principle "Pragmatism means an interest in action in its practice context" reflects that a transition needs to happen in order to effect change, but it does not account for the behavior in its present state. As part of the research, it is my intention is to query middle managers to self-evaluate the present state of their practice of *advocacy behavior* and to understand the actions needed to provoke desired consequences.

Further development of the research question is necessary to better reflect the pragmatic interest for action and the scope of the inquiry. Goldkuhl provides a list of guiding questions to help evaluate whether a research question is driving action and can be used as a form of measurement (2004, p. 15). These questions are listed in the table 3.2, as presented by Goldkuhl, followed by the comments as they apply to my own research.

Table 3.2: Goldkuhl's Guiding Questions

Goldkuhl's Guiding Questions (2004, p. 15)	Responses Applicable to My Research
What action is performed?	An information security awareness session is presented to a group of mid-level managers
Who is doing something?	The researcher
What is done?	Sharing information about security awareness
When is something done?	During the Action Research workshops
Where is something done?	The setting is the workplace of the management groups
Toward whom is something done?	The mid-level management
What should this action lead to? (What are the intended effects or purposes of the action?)	ISA advocacy should lead to the enrichment of information security awareness.
What was unanticipated during the execution of the action? (Did unintended effects arise from the action?)	In addition to the individual enrichment of information security awareness, an unintended ripple effect is ISA advocacy between employees and peers.

In addition to addressing Goldkuhl's questions, the research intends to evaluate the following question: What action can information security awareness lead to? My research seeks to investigate middle managers' engagements within the ISA events that lead to *advocacy behavior,* the ripple effect of sharing the message that is specifically focused on the ISA topic.

Goldkuhl's guiding questions helped me focus my original research question:

- *Original:* Which factors motivate members of middle management to become ISA advocates?
- *Proposed revision 1:* Which organizational and personal factors motivate middle managers in favor of information security awareness advocacy?
- *Proposed revision 2:* What is motivating non-IT security middle managers to advocate Information Security Awareness (ISA)?

The revised research question refocuses the inquiry to examine the action of engagements after exposure to an awareness event. Engagements affecting the practice of *advocacy behavior* are the "primary concerns for action" (Goldkuhl, 2004, p. 15). Engagements are happening on several points that could influence the dissemination of ISA material and its extended reach. Some example actions (engagements) include the following:

- Some organizations sponsor ISA programs.
- The technology departments share informational emails.
- Staff members, including members of middle management, are potential participants in the events (or have access to the ISA material in an indirect way).

The potential action engagements affecting the practice of *advocacy behavior* based on the existing actions that include the ripple effect of information dissemination, or how the information's influence and reach can be extended further. How do these actions and metrics "guide the researcher's way to inquiry" (Goldkuhl, 2004, p. 15)? Based on the engagements of all the staff members, including members of middle management, the focus on the practice of advocacy and its potential source for units of measurements leads researchers to investigate the perspective of existing practices in order to understand the audience's experience. This perspective also aligns with another of Goldkuhl's principles, "Pragmatism means an interest for actions in their practice context" (2004, p. 16). No finite unit of measurement exists that clearly account for the engagements affecting the practice of ISA *advocacy behavior*, which is why this subject is the focus of the inquiry.

The boundaries of the influences on ISA advocacy are not clear. In this area of ambiguity, the research seeks to contribute comprehension by finding, through inquiry, manifestations of influence toward ISA advocacy. The practice of ISA advocacy includes a holistic view of getting the information, gauging the effect, and resending informational messages. In 1980, Bleicher stated, "We can alternate between viewing the practice as a whole and viewing its different parts (e.g., different human actions) as going round in a hermeneutic circle when shifting between the whole and its parts" (as cited in Goldkuhl, 2004, p. 17).

By understanding and measuring the degree of present and potential practices of *advocacy behavior* among members of middle management, the organizations would be able to develop further their ISA program to empower and enable more information sharing. It is in the best interest of the organization for all staff members to enrich their ISA knowledge in the context of ISA and apply best practices and lessons learned in their environment. Calls to action and lessons learned may often be applicable in the business setting, as well as in their personal lives. ISA and the sharing of the knowledge are not restrictive to the business setting; they should naturally span and become part of a risk-awareness lifestyle. Employees should take into account the information learned and use it, within reason, to manage risk through actions that reflect their reality. The ISA knowledge is shared in a context that allows it to be applied to different social and organizational environments.

Information security awareness is often, but not always, embodied by an organization's information security department, which raises the awareness of threats within a context, shows how the threats may apply to the organization's environment, and helps the target audience understand what can be done to contribute to a safer environment. In this area of awareness and through the practice of sharing ISA information, this study seeks to promote change. The intended change is to shift the advocacy to the mindset of the target participants. In order to propose change, the researcher must first discover the present state of the participants' ISA advocacy practices. The researcher's contribution at this point is to inquire among the participants and recount the ISA knowledge and practices. The knowledge of the present ISA advocacy practices helps the researcher identify alternatives and contributes to improving information sharing. The study intends to discover and confirm those advocacy practices that are working among participants and identify *challenges* in the context of the organizational environment.

As presented in the previous chapters, the goal for this study is to discover social and environmental factors motivating middle managers in favor of information security awareness advocacy. This chapter begins with a rich description of action research (AR) approaches that help me center my perspective for the inquiry. I include examples of other studies I used as comparisons and consideration to focus the approach. My participation in the research was active. It included developing the awareness session presentation, soliciting organizations to host workshops, and facilitating the workshops. I provide details on the action research methodology design, guidelines, and experiences recruiting participants from multiple organizations. The AR workshop design includes a pre and post-test questionnaire, the ISA presentation, the group discussions, and an email follow-up. Each component of the workshop includes the selection protocols, data collection details and the data analysis plan.

Rationale for an Action Research Design

Conceptual study did not seem appropriate for several reasons. The inquiry for my research is focused on multiple organizational environments and the present efforts toward information security awareness. I used the literature to lay the foundation for the study, providing guidance in the context of relevant and existing knowledge. Instead of a theoretical approach, an action-oriented approach fit best: focusing on a practical problem, exploring the causes, and generating data based on the experience of participants in order to bring positive change.

Different Action Research Approaches

In exploring action research, the first discovery was that several types of action-oriented and collaborative approaches already exist. The studies below add to the body of knowledge through an action research approach to information. The perspectives come from the information systems, information technology, and organizational management industries.

- *Participatory* (Baskerville & Myers, 2004, p. 333), where active collaboration and participation between research and practitioners contribute to definition, inquiry, and development of solutions.
- *Dialogical* (Martenson & Allen, 2004, p. 507), where the driving force of inquiry and recommended solutions are based on dialogue between the researcher and the practitioner.

- Project-oriented or *control structures* (Avison, Baskerville, & Myers, 2001, p. 28), where the researcher and the practitioner define a scope called *controlled environment* and then explore it for a solution.
- *Collaborative practice research* (Iversen, Mathiassen, & Nielsen, 2004, p. 397) is an AR approach characterized by the working collaborative relationship between researcher and practitioner.

An alternative approach to action research would be to conduct a case study. As I learned about the different qualitative and quantitative tools available to develop the inquiry of the research area, my next decision was to choose between conducting action research or a case study. Two key points that led me toward action research were the desire to actively collaborate with corporate stakeholders and to bring change into the existing environment. One of the activities that helped me to make this decision was designing a case study for the same problem statement during a methods class. This process was instrumental in my decision, since it allowed for hands-on exploration of the potential parts that would be included in a study. The case study exercise helped me see the problem statement from a multidimensional perspective and understand how broad the inquiry can be. It also made me realize the importance of setting a clear scope and size for the research. The principle shortcoming of the case study was that, while both inquiry styles allowed for deep analysis and understanding of the same constructs, it would not be collaborative or inclusive of the participants to the point of bringing about action, learning, and change. Although the case study would have explored the same areas of interest, ultimately, it would not have been a catalyst or influence for change.

Chen, Shaw, and Yang (2006) take a multidimensional approach to conducting research on information security awareness. Their study, which included interviews of a group of managers from the insurance industry, suggested that information security controls alone would not reduce risk. Although participants of the study engaged in the research, the case study did not take an active approach to changing the organizational risk posture. An awareness learning process is necessary. Similarities among the subjective approaches included a multidimensional analysis drawn from multiple sources of data. Anthony Stephanou (2008) applies a case study to understand the effectiveness of ISA on employee behavior, where he consistently states that ISA dissemination in an organization does not guarantee *commitment* or behavioral change among employees. His 2008 research findings list the following key points of concern in the awareness efficacy (Stephanou, 2008, p. 10):

- Lack of empirical evidence on the efficacy and appropriateness of using certain awareness mechanisms
- Lack of a theoretical foundation for most research work
- Lack of direct observation studies of security behaviors
- Inadequate/ineffective learning and educational principles used in security awareness techniques
- Susceptibility of much of the research methodologies to the subject expectancy effect
- Neglect of some security topics (e.g., mobile computing risks) while others are emphasized (e.g., phishing threats)
- Inadequate research on the role that internalized knowledge plays (of awareness material)

These findings strengthened my belief that an action approach was needed to look for motivations affecting ISA *advocacy behaviors* that will contribute to generating empirical data to fill these gaps.

Drawing from the lessons in my qualitative methods class, I considered the case study design; however, the comparison in Table 3.3 summarizes what guided my selection of the Action Research approach. Action research allows for active participation and organization collaboration during the stages of diagnosing and treating the problem. The goal is also to increase learning and affect change, rather than simply to document the status quo.

Table 3.3: Comparative Considerations on Methods Approach

Attributes	Action Research	Case Study
Motivation	Active participation Organization collaboration	To study a phenomenon
Goals of the approach	Affect change	Discover patterns Understand influencing factors in favor of ISA advocacy
Researcher role	Participant observation To ask respondents about factors influencing ISA advocacy	Observer Contributor
Sample literature	*Iversen et al., 2004* *Baskerville & Myers, 2004*	*Chen et al., 2006* *Stephanou, 2008*

My study aimed to understand how the ISA message could be extended further by engaging members of middle management to practice advocacy. It intended to discover insight into potential motivators by exploring the subject *in collaboration* with a group of middle managers who could contribute their point of view from practical experience.

An Action Research workshop is used to recommend change by using group discussions derived from focus groups techniques. The group participants are prompted to reflect on their own ISA advocacy experiences and knowledge, as well as to recommend changes in favor of ISA advocacy. This experience is, in its own way, an information security awareness activity.

From a participatory action research lens, the stakeholders include the researcher, the organizations, and the group of middle managers participating in the workshop. The collaborative experience may contribute to a transformation in a manager's thinking in favor of ISA advocacy. As the *researcher*, I contribute the element of influence towards change in *advocacy behavior* by sharing the problem statement and the information exchange process, with the aim "to transform the conditions of existence for particular stakeholders" (Denzin & Lincoln, 2011, *Multifunctionality and Focus Groups*, para. 3). The *participants* collaborate with the study by contributing their perspectives and attitudes about the constructs, which helps "to explain, predict, and control both natural and social phenomena" (Denzin & Lincoln, 2011, *Multifunctionality and Focus Groups*, para. 4). The organizations leadership contributes by sponsoring the research.

Action Research from an Internal Practitioner Perspective

Reading McNiff and Whitehead (2006) reassured me that the methodology I have chosen for my research is appropriate. The guidance questions also helped me think through my research goals. I saw an alignment between what I am trying to accomplish and the main reasons for doing action research that McNiff and Whitehead present in their 2006 book (introduction, para. 2), which are:

1. *You can improve learning in order to improve educational practices.*
2. *You can advance knowledge and theory, that is, new ideas about how things can be done and why.*

As I read the guidance questions from McNiff and Whitehead (2006), I recognized that I have written on several of them while developing my research documentation. The first few questions addressed my specific concerns as a researcher, the *what, why,* and *how* of the study described in chapters 1 and 2. The following is a summary of my writing:

1. *What is my concern? (*McNiff, 2006, *Reading this book,* para. *4).*

Too often, IT security issues are presumed to be the sole responsibility of the IT area. I am concerned with extending the range of information being spread by promoting advocacy to a group of non-IT middle managers. I want to find ways to stimulate ISA advocacy by investigating middle management's motivations, attitudes, *challenges, and behavior,* with the intent of positively influencing their security learning and gaining support in favor of ISA. My concern is articulated through the problem statement and is further broken down into sub-problems related to management's present *level of knowledge* and *advocacy* practices. I seek to influence middle managers' advocacy best practices by "increas[ing] opportunities for learning" and "producing ideas [that] can influence the learning of others" (McNiff & Whitehead, 2006, *Introduction,* para. 4).

2. *Why am I concerned? (*2006*, Reading this book,* para. 4*).*

I aim to contribute to "learning with social intent" (McNiff & Whitehead, 2006*, The Underpinning Assumptions of Action Research,* para. 3), and generate ideas for organizational improvements; in particular, to increase effective sharing of information security awareness. I intend to create a positive impact in the participating organizations by using the knowledge and methods I've gained from experience, and in earning my degree, as a foundation to facilitate learning and encouraging the practice of sharing information through advocacy. My research aims to improve the business practice of ISA advocacy.

*3. “How do I gather evidence to show reasons for my concern?” (*McNiff & Whitehead, 2006, *Reading this book*, para. 4*).*

One of the first things I did when I began considering ideas for my research was to evaluate my own business practices for potential improvements. As an information security professional, I have several duties, including the management and delivery of an ISA education session offered to all employees.

My curiosities about research possibilities led to informal conversations with my own management and the corporate security awareness program managers. I explained my interest in the research area of information security awareness, and we discussed areas of inquiry to pursue. Informal conversation with my own management led me to believe that potential opportunities existed in security training dissemination or security awareness sessions, which is designed for non-IT security professionals.

During the process of evaluating research opportunities, I conducted literature reviews to enrich my understanding on leadership (Falkenberg & Herremans, 1995; Kaarst-Brown & Robey, 1999; Grojean, Resick, Dickson, & Smith, 2004); information security awareness (Loch, Carr, & Warkentin, 1992; Wada, Longe, & Danquah, 2012; Dutta & Roy, 2008), management’s (IT and non-IT) information security awareness (Choi et al., 2008; Kritsonis, 2005), and other similar keywords that would help me find existing studies for improving middle managers’ security awareness.

I proceeded to discuss my research interest with the other awareness program managers in search of opportunities for research in the ISA space, specifically targeting middle management. I focused on middle management for several reasons. First, most corporate ISA programs focus on the general public, not specifically on managers. I saw this as a potential opportunity to contribute to the practice. Second, through the literature review I found an abundance of literature on how to manage security awareness programs (McLean, 1992; Katsikas, 2000; Siponen, 2000; Desman, 2003). In contrasts, my research interest focused more on a specific group of people. Third, my experiences managing the ISA informational sessions motivated my interest in the direction of advocacy. As I described in chapter 2, through work-related observations, I realized that some employees did not think the informational sessions pertained to them. Therefore, I thought of forms to encourage the practice of *ISA advocacy*. It is also an opportunity to increase the management learning through information security awareness.

4. "What do I do about the situation?" (McNiff and Whitehead, 2006, *Reading this book*, para. 4*).*

My approach included an Action Research workshop where I asked managers their opinion about what needs to happen in order to improve *ISA advocacy*. To fully understand their perspective, I asked about their perspectives on their own *level of knowledge*, what they were presently doing about *ISA advocacy*, and the *challenges* they faced, as well as for their recommendations to improve ISA.

In support of my choice to conduct an action research, I reviewed several action research studies to find similarities and differences with my own research process. In the Nairobi model, Mwanahiba and Luke (1991) set actionable goals and solutions to approach a skills development workshop. The following table 3.4 compares the action-driven change goals from their work and my research.

Table 3.4: Actionable Goals and Solutions Comparison

Mwanahiba and Luke (1991, p. 521)	Grace Giraldo
"Review approaches and skills appropriate for learning."	Understand level of ISA knowledge. Review existing advocacy activities.
"Find fitting solutions to management and organizational problems."	Obtain participants' recommendations in favor of ISA advocacy.
"Enhance participants' capabilities for formulating, designing, and implementing."	Learn the challenges and constraints affecting participants' ISA advocacy.

My research design has a multidimensional perspective. Like Mwanahiba and Luke, who designed their workshops "to model action learning value" (1991, p. 521), my Action Research workshop design includes a learning opportunity. However, it also solicits active engagement from the participants in favor of ISA advocacy. Furthermore, Mwanahiba and Luke (1991) set the participants' expectations of the workshop deliverables by circulating the information prior to the event date. I used this practice by sending the workshop description and expectations through e-mail. It seemed important that the participants received the information in advance so they can prepare to contribute during the workshop. The expected contributions were recounts of existing ISA advocacy practices and recommendations from and for the participants to practice ISA advocacy.

Ramsay and Anderson (2008) used a participatory Action Research workshop to change the scope of a nursing training format from theoretical to practical. Similar to my own research, the researchers use AR methodology to promote change, increase learning, and boost awareness. Through the workshop, they introduced a change in the educational delivery method based on therapeutic practice instead of theory and process. By using role-playing exercises, the nursing students learned practical ways of interacting with patients. Furthermore, the workshop itself created awareness among the students by leading them through self-reflection of their own capacity to interact with patients.

King and Stuart's (2012) research grew from the desire to change the way first grade students increased their reading comprehension, and to encourage student independence. The workshop objectives were primarily focused on helping the students learn through action-driven activities. In addition to reading, the students' learning activities included drawing pictures and recounting the stories they had read with meaningful phrases. The teachers influenced the students in the reading workshops by guiding them toward collaborative discussions. "The sharing of these activities with peers can help bring validation to what a student believes or help that student add to or reshape their original thinking" (King & Stuart, 2012, p. 36). My workshop design included collaborative discussions and an exchange of ideas to promote learning from each other.

Focus Group Techniques and Influence

In preparation for the group discussions portions of the AR workshop, I decided to approach the group dialogue as I would a focus group. My thought process was to prepare myself to effectively communicate, lead group discussion, and manage group dialogue dynamics in order to allow the participants a to have a strong voice. Their voice was then the means to study the phenomena from the participants' perspective.

The focus group approach aimed to obtain the multidimensional perspective of the research topic by learning, creating awareness, and asking for information. My research also took a multidimensional approach by including social and organizational perspectives in a traditionally technical environment. The social approach looked to understand the groups' collective set of beliefs (Kamberilis & Dimitriadis, 2013). The organizational dimension contributed policies, programs, and dynamics from an industry perspective. Context and information security awareness are technical in nature. The focus group enabled discussion points and questions leading to the discovery of attitudes, perceptions, *advocacy practices*, workflow *challenges*, corporate culture, and value alignments expressed by the middle managers toward ISA *advocacy behavior*. Focus groups have been applied in a variety of industries and in different settings to solve practical problems (Kamberelis & Dimitriadis, 2013). Taking an example from a study by McKnight, Sharif, and Van de Wijngaert (2002), who used this method to assess the end users' perspective on the value of the wireless grids, my research in part, looked for the value of ISA advocacy. In Ruben's 2012 study on participatory behavior in animal advocacy, she used focus groups and interviews to understand how people engaged in an activity, and how they maintained this level of engagement among other activities related to animal advocacy. The inclusion of the communication strategies adds multiple dimensions to her study, and to mine.

The Researcher's Role

My intention while developing the study was to take an active approach to addressing an issue in a real-life setting. Aligning my practical experiences with the scholastic research allowed me to contribute to opportunities in the information security field. An action research (AR) approach is characterized by taking an active role in exploring, analyzing, and developing recommendations that bring about change through problem solving. The organizational practitioner and the researcher collaborate in defining the problem and finding solutions.

My professional role is in the information security department. My experiences expose me to events management practices, which served as experience for managing the research workshops. A part of my role is to produce, plan, and execute informational awareness sessions for the business community. That involves all logistics related to offering the ISA session to the employees, for example, selecting a speaker or, in some cases, presenting the information myself. As the event manager, I secure all necessary resources, event announcements, audio and visual support, post event survey, and post event reporting. These particular skills are useful for my action research.

In order to conduct a workshop, I first had to approach businesses and solicit support by asking for an invitation to conduct my research workshops in their organizations. This included, networking in professional organizations, cold calling businesses that may benefit from my workshops, and sending emails to help the sponsor understand my research goals and set expectations about the workshop itself. (I described details of these activities in the description of the workshops later in this chapter, even though this activity could be considered a pre-workshop activity).

Given that I was the facilitator and moderator driving the discussions, I had to be very mindful of my objectivity. As part of the workshop introduction, I explained that my role was to orchestrate the dialogue, but it is also to listen actively without introducing bias. Especially since I work in the information security field, I did not want to give the impression that ISA advocacy is mandatory; however, I did want to inspire a sense of duty. It was also important to articulate that participation was voluntary; no negative repercussions would arise if one did not wish to volunteer. (Appendix 11: IRB Consent forms are obtained from participants.)

I was uniquely positioned for this research since I am connected both to the field of information security and have experience communicating this type of information to business communities through my line of work. However, for this study I visited organizations where I was not an employee and hold no position of authority.

The resources in this study are information security professionals, peers outside the research activities. Most belong to professional organizations where they contribute with lectures in their field of expertise, share with related industry professionals, and learn from other organizations. The research resources have extensive technical background in information systems, including information security. To help me with my research, they have listened to my research plan; peer reviewed my awareness presentation, and helped with mentorship and constructive feedback to help me reach the goals of the project.

The Action Research Process

There were several steps or stages in the Action Research design. These included: recruit participants, run the workshops that were central to the Action Research approach, determine appropriate means to gather data, measure change, and analyze and integrate findings in comparison to the research question and literature.

Gaining Support – A Pre-Workshop Activity

As I began to prepare to execute the workshop, I realized the need for a pre-workshop activity, securing a place to offer the workshop. One of the first concerns to address was to find locations to share my workshop and how would I go about showing value added or the benefit for the companies should they elect to sponsor the workshop. Based on my professional experience, I knew that I had to prepare something similar to a sales pitch to articulate clearly my request for sponsorship. I started by writing an email titled "*Request for Sponsorship*," see Appendix 2: Request for Sponsorship Email. This was a written representation of how I would go about requesting sponsorship. I imagined having this conversation with my own management. I even had a mock conversation with a critical friend and supporter who listened and asked questions to help me craft an approach. I needed to have a clear and convincing articulation of the mutual benefit for the researcher and the company. This email answered the basic questions: What am I doing? Why am I contacting them? What am I asking for? How much time and resources is needed? Who do I need within their company? What am I offering? How is it a benefit for the company? I peer reviewed the intended email with a professional who is a leader of a company to ensure it had clarity and purpose. One of the lessons learned through this process was that there has to be a balance of providing enough information in a concise manner, while at the same time personalizing the letter.

The next step in the process was to actually call and email businesses seeking support for my research. I began by having conversation with friends and research supporters to brain storm potential sponsors. One approach was through professional networks. This approach included going to professional networking meetings, creating new connections, or reacquainting myself with prior connections in order to share my research and ask if there is a sponsorship interest. This approach was the least fruitful. In hindsight, in order for this approach to be more effective, I should have been developing these relationships with the specific intent of exploitation for future research well in advance of the actual time anticipated for accomplishing this task.

One potential approach was to solicit participants from the Internet. It would include posting in several professional networking sites information about my research, and explaining the support needed and how to get involved. While the approach seemed feasible, I thought of other implications that would arise from an invitation to conduct the workshop in a remote location.

Another approach was to do an inventory of leaders that I might know through my own experiences and approach them about my research. Perhaps if they were not able to help me they may know someone in their network grid who could. I looked through my contact lists, through my professional and educational associations, and spoke to my peers, critical friends, and research supporters about this subject. I created a list of businesses which whom I have done business in the past, worked for, consulted to, or volunteered in a project. This became my target list of businesses I approached to solicit sponsorship for a workshop. The next step was to call and email leaders within the list of businesses to ask for their support. I repeated the same steps with all the business on the list with mixed results.

My first attempt for sponsorship was with my own employer in the financial industry. I called and emailed leaders within the organization for support. My proposal for the workshops was well received by management. Unfortunately, due to legal implications it was not possible to accomplish at my place of employment. I then contacted a non-profit firm in the Education industry. This organization offers the public a variety of events and displays on history. Although they would have liked to support my research, and recognized the value in the workshop session, the business priorities required their full attention since they were short staffed.

My third attempt proved to be more fruitful. A leader of a financial company responded to my request for sponsorship with curiosity. After receiving my email and listening to my follow-up voice mail, I received a response inviting me to teleconference. During this conversation, and following the script developed from my pre-invitation preparation, I was able to provide information of my research, the workshop format, and the benefits for his company. At that point, I received a verbal invitation and the name of the person who would be my point of contact for the duration of the engagement. Using email as the main communication tool, I asked my point of contact basic questions to gather information that I would use when writing the company descriptions for the thesis. My questions about the company included: What industry is this company part of? How many employees does the company employ? How many managers does this business have? How many business units or departments does the company have?

During the preparations for the workshop, I sent an email with the workshop plan in short bullet points and offered to manage and provide status reports as we made progress. Every week prior to the workshop, I provided an update to show progress, to set expectations and to provide as much transparency as needed about the workshop. The bullet points included the following pre workshop activities that I consistently used for every engagement.

1. Send a copy of the research design and workshop questionnaires.
2. Send a copy of the Information Security Awareness informational presentation.
3. Obtain letter of cooperation and submit to the IRB for approval.
4. Send the volunteer recruitment email to managers through my person of contact.
5. Align the workshop date with the IRB approval.
    a. Securing the conference room and projector.
6. Print all the materials necessary for the workshop.

Although these tasks are not part of the workshop design, these activities were necessary to clearly communicate and maintain engagement with the companies that sponsored a workshop.

Continuing through my attempts for sponsorships, I emailed and left voice mails for several companies in the Pharmaceuticals, Health Care, and Financial industries, but did not receive a response. These rejections were accepted as part of doing research. I also had conversations with companies that may not have been a good fit for a variety of reasons. In one case, the company was very small, with one owner and two employees. In another case, the leader pointed out that the nature of their business was in the Technology industry, and part of their business model was heavily associated with Information Security. This meant besides the data, these would be IT security managers, which were not in my target audience.

Another success in sponsorship came from a non-profit organization providing services to the local community. In this particular case, during the pre-workshop activities I had several follow-up phone calls to ensure the business point of contact understood the layout of the workshop and the benefits for the participants and the business. During my conversations, I minimized the benefit to my research and focused on the learning opportunity as a benefit for the participants. This particular experience was a learning opportunity for me. As I was trying to gain an invitation to conduct a workshop, I had to focus on the benefit for the organization and the participants. My own needs in this case, and probably in every other instance, were secondary.

In the Manufacturing Company, I was invited to conduct the workshop in a light manufacturing company supplying the steel industry and quickly was appointed a point of contact to work through the stages of the workshop. I proceeded to use the repeatable tasks outlined for pre workshop planning and workshop execution. The following table 3.5 describes the participating firms and the participants.

Table 3.5 Participating Firms in this Research

Industry	Approximate Number of Employees	Source	Number of Participants
Financial	300	Email Request for Sponsorship	4
Not For Profit	100	Email Request for Sponsorship	10
Light Manufacturing	500	Email Request for Sponsorship	24

Details on the Action Research Stages and Methods

I used participatory action research approach to model the activities in order to diagnose the problem and to develop ideas that lead to action-driven change in favor of ISA advocacy. I collaborated with practitioners in the business to identify the problem and focus of the research. The problem statement was based on a real-life industry experience and organizational settings. The workshop was designed to solicit active engagement from the participants. The steps included an introduction to the problem, a knowledge self-assessment, group discussions, and recommendations toward actionable solutions. Participants of the research contributed recommendations and drive change by providing potential solutions to the problem through an exchange of practices and ideas.

The following steps are specific to the workshop design and instrumentation. Even though companies invited me to conduct a workshop, as a researcher I still had to recruit volunteers within the company. Through the email solicitation, I invited the group of middle managers to participate in an Action Research workshop. With the intent of setting the workshop expectations, the invitation included the goals of the Action Research workshop, an introduction to action research, and a description of the activities planned for the event. The same information was repeated at the beginning of the workshop, during the introduction to the study (Appendix 3: Security Awareness Action Research workshop Facilitator Form).

The workshops began with an introduction to my research and my professional background. It helped the audience understand who am I and why I did this workshop. I promptly went over the workshop agenda to help set the expectations of the event activities. The workshop agenda included the following bullet points in the presentation:

Workshop Agenda:

- About me and the workshop
- Consent Procedure
- Pre-Test Introductory Questionnaire
- Information Security Awareness Presentation
- Discussions and Idea Exchange
- Action Exercise
- Post-Test Questionnaire
- Close and email follow-up

After the introduction and the workshop agenda, the consent form procedures were completed and I collected the signed consent forms. I started the first workshop activity (the pre-test questionnaire) with the introduction of the activity and a description of the main areas covered in the questionnaire. I also explained to the participants that the purpose of the pre-test is to allow me to compare whether this workshop is an effective way to generate change in Information Security Awareness *advocacy behavior* or knowledge.

The next step in the design was the introduction to Information Security Awareness informational session through a PowerPoint presentation. This helped me show factual examples of awareness content and provided context of the problems to which they would seek solutions during group discussions. I explained to the audience that the presentation examples were industry facts, and hopefully would convince the participants of the importance of information security activities, the importance of awareness on the part of their subordinates, peers, and even superiors, and the importance of their own *advocacy behaviors* on behalf of the company.

The participants discussed as a group the need for ISA advocacy and recommended driving changes intended to influence behavior in favor of ISA advocacy. The recommendations and feedback from the managers were collected and shared among all participants as examples of actionable items that all middle managers can do to enhance ISA advocacy. This data served as the foundation to explain the influences of AR workshop on advocacy.

After the ISA presentation, the workshop design included the group discussion and commitment to action. These design components were when participants contributed to group discussions and proposed actionable change they consider accomplishable. The discussion was driven by leading questions, but the group drove the dialogue dynamics. At this point, the researcher's role was to listen and write responses on the white board.

The workshop ended with group goals set in favor of ISA advocacy and inviting them to participate in responding to follow-up e-mails. The timelines and detailed steps of the workshop are listed in the table 3.6 below.

Table 3.6: Security Awareness Action Research Workshop Design

Time period	Step in research design	Explanation	Rationale	Data to be collected
2 weeks prior	Invitation with purpose and description	Confirm attendance	Need sufficient size and diversity	Name, functional job description
Workshop	Introduction with purpose and facts	Action research information provision	Need to remind and clarify purpose and process	Consent forms and early questions from participants.
Workshop	Pre-test	Test pre-workshop knowledge	Helps identify bias in quasi-experimental, non-random assignment to group	Quantitative and Qualitative data: Pre-treatment level of knowledge and behaviors, demographic data
Workshop	Treatment, part 1: Facts	Present facts about ISA in general and at firm	To engage and problematize issue of IT security and security awareness	Qualitative data: reaction to facts, verbal comments
Workshop	Treatment, part 2: Action research, action exercise	The group work to develop actionable items related to security awareness behaviors	To share and develop ideas about behavioral changes at individual (not organizational) level	Qualitative data: Larger list of ideas, insight to self-critique, data on potential inhibitors to security awareness behaviors
Workshop	Treatment, part 3: Commitment to action	Develop short list of specific actionable items	To set goals for individual security awareness actions	Qualitative data: Baseline commitments to changes or continued security awareness behaviors
Workshop	Post-test 1	Test pre-test/post-test differences Time period 0	Capture impact of treatment at time 0	Quantitative and Qualitative Data: Comparison awareness data right after treatment
Workshop	Close	To set expectations for follow-up	To set clear expectations and gain support for future contact	No specific data collected

Time period	Step in research design	Explanation	Rationale	Data to be collected
3 weeks later	E-mail post-test 2	Test post-test residual differences for time period 1	To determine behavioral changes, knowledge retention	Qualitative data: Residual knowledge and awareness retention; data on behavior changes in relation to commitment
6 weeks later	E-mail post-test 3	Test post-test residual differences for time period 2	To determine behavioral changes, knowledge retention	Qualitative data: Residual knowledge and awareness retention; data on behavior changes in relation to commitment

The Action Research workshop was designed as a learning opportunity, a forum to drive change, and an event to generate empirical data. Through the informational presentation, the activities, and the instruments, the participants learned of the resources available to enhance their understanding of ISA. In addition, the workshop helped create consciousness of the need for support to drive change in favor of ISA advocacy. Table 3.7 shows the new data for the research was gathered through the workshop events, including the group discussions that focus on the following themes:

Table 3.7: Data Collected Based on Theme Discussions

Discussion Themes	Recap of the Data To Be Collected
ISA awareness	The participant's perception of knowledge
ISA advocacy	The participant's recount of advocacy behavior experiences
Constraints and challenges	The participant's point of view of organizational and personal influencing factors promoting or preventing middle management's advocacy
Commitments	The participant's recommendation for changes in favor of ISA advocacy

The following sections address the different workshop phases in more detail.

The Pre-test and Post-test Questionnaires:

The pre and post workshop questionnaire captured the middle managers' point of view on their individual knowledge level and gauged their own understanding of the ISA content. (See Appendix: 4 Pre-Test Questionnaire, and Appendix: 7 Post-Test Questionnaire). The self-evaluation affects the variable of ISA knowledge, and the data yielded a measurement of knowledge as a contributing or hindering factor motivating the ISA *advocacy behavior*. This data can also constitute a scorecard or gauge for training and awareness development. The acceptance criterion for inclusion of the data is that they include middle managers' self-reflection of knowledge based on the workshop experience.

The pre-test workshop activity was a learning opportunity as it includes samples of sources of Information Security as part of responses to one of the questions. For some participants, these multiple choice responses were new information related to where to seek awareness information. The sample question below is from the pre-test questionnaire. This question is a learning opportunity for a participant that had not engaged in awareness activities prior to the workshop may not know where to look for information security awareness material. While completing the pre-test activity, the participant read the questions, learned of the different sources available to find awareness information, and generates empirical data by responding. (After reading the question and learning of sources of information, this question itself may have provided the tool~~s~~ a participant needed to engage in action driven change). Figure 3.1, provides a sample question from the pre-test questionnaire.

Figure 3.1: Pre-Test Assessment Sample Question

Pre-Test Assessment Sample Question
Describe the sources you use to learn about information security awareness. This is a multiple choice answer that includes the following selection:
□ I search for bulletins published on the company intranet. □ I learn from my colleagues and peers. □ I attend ISA presentations and events. □ I watch company-posted webinars and videos. □ I receive information security awareness e-mails. □ I ask my local information security officers when I need information. □ I am not aware of the resources available to learn about ISA. □ I research ISA independently from external resources like the Internet. □ Other: ____

As the pre-test also asked for a recount of activities the participant has previously engaged, it was possible to measure those who were positively impacted by the workshop towards ISA advocacy. If in the pre-test questionnaire the participant responded with no previous or present engagement, but the post-test or follow-up emails show new engagement, then it would be reasonable to attribute an influence of the workshop to the action driven change.

The Information Security Awareness Presentation

The workshop activities included a sample industry related ISA presentation. The sources for content were artifacts commonly used by organizations to present security related information. These include individual common practices, industry incidents, websites, audiovisual presentations, and other guidelines serving as sources for the creation of information security awareness. The acceptance criterion for inclusion is to use existing content that is accessible to the organization. In other words, the source of the artifact can be an industry website, or an industry report. The sample content contributed attributes as data affecting the variable ISA contents and providing insights of format, accessibility, relevance, length of material, and complexity.

The ISA presentation showed factual samples of industry breaches across multiple industries where the number of records exposed were thirty thousand (30,000) or greater (see Appendix 5: Treatment Part 1: Facts). This is publicly available information. It is presented (narrated) from the point of view of a person engaging in normal online activity and it uses simple language. Each slide followed a repeatable format to show the name of the company, the industry, the data fields exposed, and the risk presented within the use cases. This informational session served as a learning opportunity for the participants. As the presentation was narrated, online user behavior examples were discussed to prompt the participant to reflect on their own online behavior. The explanation of risks helped the audience understand how a person's behavior could lead to contributing to a breach. The participants not only learned a factual industry incident, but also learned about behaviors they can do to reduce the risks. The sample incidents with the description of user behavior and risk explanations were meant to drive actionable change. Users do not always understand that security starts with how they manage their personal information. The empirical data generated included the participant's reactions and comments. While some participants may have a level of familiarity with the information presented, others may be surprised or alerted. These reactions contribute to measuring if the AR workshop was effective in driving change.

The Action Research – Action Exercise

The Action Research – Action Exercise (ARAE) are the discussion points and questions in the group dialogue that lead to the discovery of attitudes, perceptions, *advocacy practices*, workflow *challenges*, corporate culture, and value alignments expressed by the middle managers toward ISA *advocacy behavior*. The ideas that were exchanged served as a learning opportunity for the participants as they may have realize through self-reflection and by sharing with their peers the need for additional knowledge, or the importance of engaging in advocacy of ISA. The acceptance criterion for inclusion of the data was the validation of level of management aligned with the participant selection. Feedback from individuals who work in the information security field was not included during the analysis of data.

The ARAE question number one prompted the participant to express their opinion on advocacy, for example, *what do you see as the benefits of middle managers being active advocates for information security awareness and behavior at this firm?* This question was directed towards the participants, making them consider the possibility that they may have some form of ownership toward sharing information. The intent was to prompt the participants to verbalize their personal perspective on the value placed of their contribution towards advocating for ISA. This question helped determine if the participants understood the importance of the subject matter and was it important enough to motivate engagement. The data yielded from the question contributed attitudes, perceptions, and value alignment attributes that motivated or counter incentivized a middle manager toward ISA *advocacy behavior*. In ARAE #2, the participants were presented with the following:

> *If you currently advocate for information security awareness in your company, what are two reasons you do it? If you feel that you are not currently a strong advocate for information security awareness, what are two reasons for this or that hold you back?*

These questions were designed to prompt the participants to articulate their personal motivations or perceived *challenges* towards activities they currently do towards advocacy of ISA. The questions looked for the participant to self-evaluate and verbalize their attitude towards advocating for ISA. It served as a learning opportunity by giving the participants a chance to evaluate their own perspective on the subject and question if engagement of ISA advocacy is an activity they see necessary or welcome. In ARAE #3, invites the participants to share among the group their experience sharing ISA.

> *On the flipchart, white board, or comment area, please record four or five Information Security advocacy activities and best practices that your group presently engages in to promote, share, and direct the attention of your employees or peers to ISA learning.*
>
> *One the flipchart, white board or comment area, please record challenges or constraints you presently experience that you feel makes it harder for you to engage in information security advocacy behavior.*

The workshop was an idea exchange; bringing many views to light on the subject was also a form of learning from each other, sharing accomplishable activities and best practices that increase awareness, as well as sharing perceived challenges or inhibitors.

Some participants may have more experience or ideas than others, and supported why group participation is part of the research design. In ARAE #4, the question asks for the participants recommended changes to their present challenges sharing ISA.

> *Are there ways that you could overcome or remove these [challenges or constraints]? Is there support that the company could provide to help you overcome them?*

Constraints and *challenges* included the participant's point of view of personal perspectives promoting or preventing middle management's advocacy. This was a learning opportunity, as some of these *challenges* may be viewed as *challenges* to be mitigated through sharing of information with peers. Other *challenges* may be managed through increasing the level of knowledge, and some *challenges* may be in realizing the level of effort it may take to accomplish tasks to share information. As the researcher, I had the opportunity to learn from the participants' perspective for the research, and apply the lessons learned toward my own professional practice.

The ARAE discussions close with presenting the audience with an opportunity to commit to ISA advocacy.

> *Please think about what you have discussed. One of the goals of this Action Research workshop is to engage you in helping us address the problem of Information Security Awareness. An important part of this is developing personal, actionable plans for ISA advocacy activities that are within your control. Highlight, write in, or circle on your individual sheet two or three ISA Advocacy activities that YOU feel are accomplishable and that YOU personally will commit to.*

Commitments and recommendations involved the participant's point of view of potential changes to drive in favor of ISA advocacy. This construct included attitudes toward ISA advocacy that positively influenced their employees to create consciousness of the importance of a good information security posture. The realization or learning of the importance of awareness or understanding what some accomplishable tasks are may help an individual decide to resolve personal conflict related to advocacy and engage in the practice of sharing information. Any act towards advocacy of ISA is a step towards action driven change. The follow-up emails help measure if the personal *commitments* were effective long term. (See Appendix 9 and 10, Follow-up Emails).

Data Collection Procedures

The AR workshops were held between November 2013 and February 2014. The data collection occurred in different stages in the Action Research Design. During verbal discussions, audio recordings and note taking were used to collect dialogue. Participant job function or title information was collected prior to the workshop through the point of contact at each participating organization. The variety of workshop activities yielded data on the employment demographic information, verbal descriptions from the group discussions on their reactions to the awareness facts presented, recommendations and *commitments* to improve ISA advocacy, and post-workshop feedback on the lessons learned. Workshop participants contributed their individual experiences with the group, making the discussion topics such as *ISA advocacy*, *challenges* an opportunity for the larger group to learn from the experience. The diverse source of data generation during an interactive workshop has risks associated to its data collection method; some examples are listed in table 3.8.

Table 3.8: Research Study Execution Resource Challenges

Resource	Constraints and Challenges
Middle management	Time limitations, not available the day of the workshop
Content samples	Too technical for some of the audience
Reponses to semi-structured group interviews	Capturing the data using audio and visual tools may introduce bias.
Reponses to semi-structured group interviews	There is a risk of losing data if the quality of the audio or visual is not appropriate for transcription.
Organizational facilities	The use of conference rooms, audiovisual equipment, and electronic tools like e-mail must be approved by the sponsoring management.

The workshops were in a group setting. To create consistency and a repeatable process for all activities all instruments were grouped for each participant in a white large envelope creating a workshop packet. Each workshop packet contained a copy of the consent form, the pre-test questionnaire, the action research/action exercise, a post-test questionnaire and a copy of the ISA presentation PowerPoint. As the workshop progressed as designed, the facilitator instructed the participant which instrument to select from the packet. As the participants completed an assessment, the researcher instructed the participants to place the appropriate document in the white envelope. Each envelope collected at the end of the workshop contained contributions to data. This step kept them separate until the responses are coded and de-identified.

Using Creswell's (2009) data collection guidelines, I followed this data collection approach and repeated the same steps in every workshop:

- Data collection for AR workshop
    - Ensured the participants consent to the audio recording.
    - Audio taped the workshop.
    - Transcribed the audio tape.
    - Conducted data analysis.
- Data collection procedure for middle managers' functional job description
    - Collected employee profile from the organization's point of contact.
    - Parse data for descriptive analysis.
- Data collection for pre and post workshop questionnaires.
    - Instructed the participant to select the pre-test / post-test instrument sheet from the envelope.
    - Allowed time for middle managers to complete the assessment.
    - Each participant placed the instruments in their individual white envelope.
    - At the end of the workshop, I collected the envelopes.
- Data collection for group discussions.

    - Discussed ISA advocacy best practices
    - Wrote ideas and comments on the Flipchart or Whiteboard
    - Discussed perspectives on *constraints* and *challenges*
    - Wrote ideas and comments on the Flipchart or Whiteboard
    - Discussed potential contributions towards advocacy
    - Wrote ideas and comments on the Flipchart or Whiteboard
    - Collected the flip chart sheets or copy of the white board for data analyses.

During the group exercise, the researcher collected best practices, perspectives, and recommendations. These were consolidated into a list of actionable items to encourage the participants to pursue action-driven advocacy goals and *commitments*.

- **Data Collection for the E-mail follow-up**
    - During the workshop, I reminded the participants to contribute to the email follow-up.
    - Sent a follow-up e-mail to all participants three weeks after the workshop. This was intended to collect their knowledge, behavioral changes, and *commitment* perspectives. The e-mail asked simple questions on the understanding of the ISA presentation, their personal self-reflection on improvement of ISA knowledge, and their thoughts on improving advocacy best practices in the organization.
    - Sent the same follow-up e-mail to the participants six weeks after the workshop. Although the data to be gathered remained the same—the participants’ reaction to the workshop activities and lessons learned—the goal in capturing perspectives over the longer term is to measure residual knowledge and awareness retention.
    - The participants responded to the e-mails with their perspectives for data analysis.

My study collected data from the participants' group discussions and recommendations to motivate ISA advocacy. Table 3.9 summarizes the data collection methods and the data it yielded by workshop activity.

Table 3.9: Data Collection by AR Workshop Activity

Step in Research Design	Format/Source of Data
Pre-test	Questionnaire assessment survey responses
Treatment, part 1: Facts	Audio recording and/or note taking during ISA presentation
Treatment, part 2: Action research, action exercise	Written collective lists from group discussions
Treatment, part 3: Commitment to action	Written list from individuals
Post-test 1	Post-workshop questionnaire survey responses
E-mail post-test 2	E-mail responses
E-mail post-test 3	E-mail responses

Sampling Protocols

Study Participants

The participant selection was purposeful and specific to those who qualified as middle managers in the host organization. It is also a convenient sample because I had to solicit an organization to allow my research before I can recruit volunteers.

As noted earlier, I started by emailing an organizations leadership asking for support for my research by allowing me to conduct a workshop in their organization. Once I received an informal yes, I proceeded to use the protocols to ensure the steps taken were repeated in the same fashion for all the participating organizations to maintain consistency. The second challenge was identifying a suitable participant sample.

Identifying Middle Managers

Different organizations have different management structures. They can appear to be grouped in a similar manner but all are not exactly the same. Multiple management groups may exist representing several lines of business. Each business unit could be composed of multiple layers of management. The researcher grouped the levels of management in the following structure to distinguish for validation of acceptance criteria and mark the boundaries of inclusion to the study:

Executive Management

Non- Executive Management (Middle Management)

Non-Management

IT Security Related Manager

Those in the middle management layer were the target participants of the research study. These individuals include business and technical managers, but not in IT security related and Non-Managers. (IT security related managers are professionals that work in the information security field). Executive Management or the C-Suite represents the executive branches of the businesses, for example: the Chief Executive Officers, Chief Financial Officers, Chief Technology Officers, Chief Operating Officers, and Presidents. During the collection of demographic information, I asked the participants to select the closest match to their managerial level. Of the four managerial categories available, only the data Non-Executive Management would qualify to include for data analysis.

The target management tier is the middle layer of leaders. That means not executive management and not the employees that are their subordinates. The characteristics of the middle layer manager include the existence of a reporting structure vertical and horizontal. Middle managers have an audience, their employees, and peers, to influence or guide in matters of information security awareness.

As seen on table 3.5, the organizations were of different sizes, which also meant that these different businesses have a different number of managers available to solicit for volunteering. During the planning stage of the research, there was no way of predicting how many potential participants any one specific organization would yield. Smaller organizations could have a workshop with as little as 3 or 4 participants while larger organizations could have multiple workshops with 8 to 12 participants. My goal was to reach at least a total of 30 participants or more. This is based on my committee's recommendation during my proposal defense. Initially, the number sounded very accomplishable, but in reality, the experience of soliciting businesses to host a workshop turned out more challenging than expected. (First, I had to sell the idea of the workshop to be invited to conduct the research. Once invited, I had to recruit volunteers from the pool of available management).

The participants were reached through the point of contact using their work email; I solicited their voluntary participation by the recruitment e-mail and meeting invitation.

In the workshops, participants were similar (homogeneous) in the following ways:

- The participants all worked for the same business, sharing organizational human resource guidelines, corporate vision and goals, and IT and security policies.
- They worked in the same industry.
- The managers were not under one another's reporting structure.
- The managers worked in the same general department, such as marketing, finance, or technology.
- The technical or nontechnical nature of the job differed among participants.

In contrast, since workshops were offered in different organizations, the participants shared heterogeneous qualities.

- The workshop groups came from diverse businesses, not necessarily sharing organizational human resource guidelines, corporate vision and goals, and IT and security policies.
- The business industries varied, which could serve as an opportunity to gain different insights.
- The businesses shared similar department names, such as marketing, finance, or technology but the management's job function may be different given the nature of their industry.

After the data gathering, I used Excel spreadsheet functions and charts to code and analyze the demographic characteristics of the participants. The population of the study was thirty-eight individuals (N=38), the selection of the participants was purposeful, and all are members of middle management in their organizations.

During the data analysis, I listened to the recordings and consulted with the company point of contact to verify the functional job description with the answers provided in the demographic section of the pre-test questionnaire. Upon validation, several corrections to the demographic data field Management Level were made. I included the responses from the light manufacturing industry where the functional job descriptions is called "supervisor" as these are positions that do have a responsibility to manage employees (the same as a non-executive manager). Similarly, I included the responses from the financial industry and the non-profit organization where the functional job description did not have the word "manager" but the individuals nonetheless did manage direct employees. Also, in the financial industry, I included the responses from a department manager as this role was not equivalent to an Executive Manager as defined in the study (CEO, CFO, CIO or COO), also known as the C-suite. These errors in selection could have been prevented had I communicated a better definition of the functional business activity of a manager during the introduction of the study and pre-test questionnaire rather than assuming a cross business unified understanding of the title. None of the participants was IT Security Managers or Non-Management whose omission was requested. All thirty-eight (38) participants were verified to qualify as a Non-Executive manager in the study. The following table 3.10 shows the participant demographic summary.

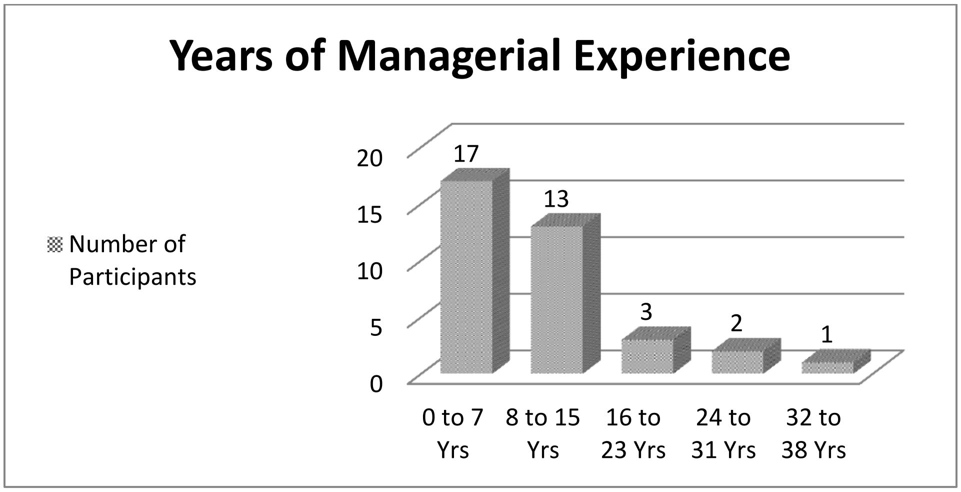
Table 3.10: Summary of Demographics of the Survey

Demographic Attributes	Responses
Response rate	38 Purposeful Sample
Level of Management	38 Non-Executive Management
Gender	16 females (32% of 38) 22 males (68%)
Age	2 were between 20-29 yrs. 11 were between 30-39 yrs. 11 were between 40-49 yrs. 9 were between 50-59 yrs. 5 were between 60-69 yrs.
Length of Management Experience	Mean: 9.31 Median: 8 Range: 35
Length of Employment with the Present Organization	Mean: 6.48 Median: 4 Range: 25
Participating Industries	Not for Profit Financial Institution Light Manufacturing
Managers in the IT Related Job	1 manager works in IT

When asked for the industry participating in the workshop, many participants provided a field description, which in order to protect the identity of the sponsoring organizations, I summarized to a generic industry name. The majority of the participants were from the Light Manufacturing industry (24 participants), followed by the Non-Profit (10), and the Financial industry (4).

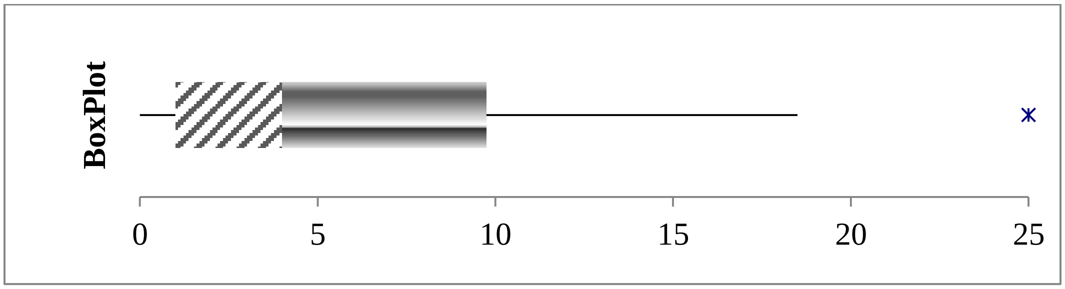
The participants' overall length of management experience ranged between less than one year and thirty-five (35) years. The average length of experience in a managerial position was 8 years. The figure 3.2 shows the range of managerial experience by years. Two responded left the question unanswered, making n=36. The majority of the manager's experience is between zero (0) and seven (7) years. Seventeen (17) managers in the sample have between less than a year (1) and seven (7) years of management experience. Using the median eight (8), I divided the data to represent the group gain insights of the experience levels. Thirteen (13) participants have been a manager from eight (8) to fifteen (15) years. Three (3) have been a manager between sixteen (16) and twenty-three (23) years. Three (3) have been a manager between twenty-four (24) and thirty-one (31) years. One participant has been in management for thirty-five years.

Figure 3.2: Number of Participants Shown in Years of Managerial Experience



When asked, "*How many years have you been a manager at this institution*?" the median number of manager's years of experience at the same institution is four (4). Nineteen (19) managers in the data set are between less than a year and four years of management experience at the same institution. There is a spread of twenty-five (25) years of managerial experience working in the present institution in the sample (n=37). Figure 3.3 shows the box plot distribution of responses with a minimal score and outlier of zero (0) and the maximum score and outlier of twenty-five (25). The tendency of the responses is between the first and third quartile. This clustering of data suggest the concentration of managerial experience is between four (4) and nine (9) years.

Figure 3.3: Length of Employment at the Present Organization



The participants' genders were represented by sixteen (16) females or thirty-two percent (32%) and, twenty-two (22) males or sixty-eight percent (68%). A little over a third of the participants were females. (Table 3.11 shows the data sample (n=37)).

Table 3.11: Managerial Experience by Gender Representation

Years of Experience	**Total Number of Participants n=38**	**Male Participants**	**Female Participants**
0 to 7	18	8	10
8 to 15	13	8	5
16 to 23	3	2	1
24 to 31	3	3	0
32 to 38	1	1	0

The age range of the manager participants are represented in the tables 3.12, showing the majority were in the thirties (30)'s and forties (40)'s age range with eleven (11) managers in each range. Except for managers in their twenties (20's), all other ranges had both male and female representation.

Table 3.12: Participant Age Range Groups

Age Range	Number of Managers in Age Range	Number of Female Managers in Age Range	Number of Male Managers in Age Range
20's	2	2	0
30's	11	5	6
40's	11	2	9
50's	9	2	7
60's	5	1	4

Participant Solicitation Protocol

I planned to solicit workshop volunteers through e-mail and email meeting invitations. The purpose of sending the research information through both means of communication was for the convenience of the participants. In my attempt to be sensitive to an individual's busy schedule, I wanted to make sure that the research documentation was readily available. The solicitation protocols are in the appendices. In summary, the communications included the following:

- The introduction to the study
- The organization's approval letter
- Consent form
- Statements of privacy
- IRB statements of protection from harm
- Action research description of goals and procedures
- The statement of participant expectations

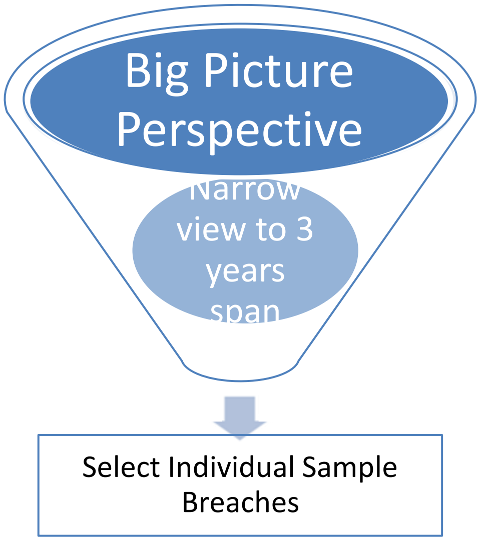
- Invitation to AR workshop

Artifact Sampling Protocol

The sensitizing artifact used in action research required careful, thoughtful development. The sample informational presentation purposeful, and specific to cyber security awareness or an industry incident report. (See Appendix 5: Treatment Part 1: Facts). In the end, I developed a PowerPoint presentation based on a publicly available website that illustrates The World's Biggest Data Breach: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ .

The flow of the information presentation was also critical. I started with the high-level view of the website, which was the visualized data shown on the website page. As I developed the presentation, the aim was to send a message that helps the participants relate to the message at a personal level. With that intention, the presentation began with a high-level view of a collection of security incidents; it is presented as the big picture. The next step was to narrow the view, to guide the audience in a story that drills down into a narrower timeline (three years) and begin to show how our personal activities online may contribute to leaving traces of personal information across the Internet. Simple everyday online activities, common to all, (students, employees, gamers, shoppers) expose pieces of data about us. In order to help relate the message as a people concern, I took another step in narrowing the view to individual samples of specific breaches and then took the presentation from historical facts to details relating our online activities with information security awareness. Following the threat model defined by Loch et al., I create the incident slides to present the threats from Loch's four-dimensional perspective: "the source, perpetrators, intent, and consequence" (Loch et al., 1992, p. 176).

Figure 3.4: Presentation Perspective


Big Picture Perspective
Narrow view to 3 years span
Select Individual Sample Breaches

Once the presentation reached the example of individual security incidents, I presented the slide from the perspective of the online user behavior. For example, one slide presents an industry incident where malicious users compromised the security of a website and stole the passwords of the website users. I presented the information from the lens of a person that uses the online service on the slide and used words that appeal to a personal level:

> *Think about modern activities we engage in like professional networking. In this incident only passwords were stolen but the intruders gained access to customers employment history, contact lists and contact information. This information was used to craft phishing emails to target people for more detailed information. In addition to gaining access to the contact, information may give them details like a person's email address the malicious user will try on other on other online services.*

The personalization helped the audience understand that we are all at risk of information disclosure and it is important that we understand the risk and potential harm. It is also important that we behave as the stewards of our own information and that we are the first line of defense of our personal information. Validation of the presentation artifact was also an important step. The presentation validation consisted of a peer review with two industry experts. The reviewers are two individuals that are experienced professionals in financial ethical hacking and online fraud investigation fields. They evaluated the presentation for structure and content to ensure the slides contained factual samples of online exploits and the proper explanations of the consequence or impact on the cybercrime victims. Their feedback lead to adjustments to the flow of the presentation, from high level, introduction to terms, down to individual examples of industry breaches. In addition, they validated the preventive recommendations presented for the audience and the guidelines were reasonable and accomplishable by individuals. These adjustments helped the audience understand how their individual actions and online behaviors can contribute to the disclosure of information. Presenting the information in this matter is what helped the audience relate with the industry incidents at a personal level.

The participants learned from the PowerPoint presentation that they are the first line of defense of their personal information. They learned that industry breaches could be traced down to how it affects an individual person. The learned that most common online activities lead to leaving traces of our personal information online. They learned about best practices to reduce the risk of information disclosure. As a reference, I included sample slides in Appendix 5: Treatment Part 1: Artifact Presentation Description. I am hopeful that these lessons learned strengthened their value for awareness and advocacy of ISA.

Instrument Development Procedures

There were several different instruments designed to execute the Action Research workshop. This study has three main types of instruments, which are included in the appendices; these include questionnaires (with multiple choice, scales, and open text); group discussions, and email follow-ups (Spears and Barki (2010), Siponen (2010)).

Questionnaire Procedures

The demographic questions in pre-test questionnaire included six questions to help obtain descriptive information about the participants. Figure 3.5, list the demographic questions designed for a participant to write in the answers to the queries, which include the length of management experience, the number of years working at the same organization, their age, industry and an indicator that distinguishes if their job is technology related. (The detailed codebook for the demographic data is included further below).

Figure 3.5: Demographic Questions

Demographic Questions included in the Pre-Test Assessment

1. How many years have you been in a management position in your overall work experience? ____ Years

2. How many years have you been a manager at this institution? ____ Years

3. Select the closest number to your age range (circle only one):

20s 30s 40s 50s 60s other

□ I do not want to disclose my age range

4. Please select the closest match to your management level:

___ Executive Management
___ Non- Executive Management
___ Non-Management
___IT Security Related Manager

5. What is your industry? ________________________________

6. Is your job function IT related?

□ YES, I work in IT or have IT related responsibilities.

□ NO, I don’t work in IT or have IT related responsibilities

In Spears and Barki (2010) the population they examined in their study examined "how (user participation) is perceived to impact Information Risk Management" (p. 504). My research is similar in that it examined how managers perceive their own knowledge and actions influencing Information Security Awareness and advocacy. Following the similarities to the mixed-method approach used by Spears and Barki (2010), I leveraged the use of survey question format and interview questions. Their research used instruments with interviews and surveys to obtain both rich descriptions of the phenomena, generate empirical data, and to measure participant sentiment on specific behaviors, attitudes, and activities. My research used group interviews instead of individual interview, with discussions based on semi-structured questions meant to guide the topic of discussion and allow the group of participants to drive the dialogue. In a similar manner, my research used survey questions to measure activities, behaviors and attitudes towards Information Security Awareness advocacy.

I pre-tested the Action Research workshop instrument questions by conducting a peer review with a colleague. The mock workshop revealed clarifications needed in the wording of the questions and it revealed the need for consistency in the constructs across the pre-test, treatment and post-test. One major change I did was to rewrite some questionnaire items to use Likert scales, to measure the participants answer in a measureable range. For example, when asking about perspectives regarding the level of information security knowledge, instead of providing the options of low, moderate, high; I leveraged a scale found in Spears and Barki (2010), to show a larger range of options that spanned from very low/strongly disagree valued at the lowest score of 1, to very high/strongly agree valued at the highest score of 7. Figure 3.6:

shows the Likert scale format adopted. This enables the data gathering to capture more subtle changes in the Action Research workshop ISA learning experience.

Figure 3.6: Likert Scale Format Adopted

I have a high awareness level of Information Security.

Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)

Please select the box of a single score from 1 to 7, 1 means you strongly disagree with the statement and 7 means you strongly agree with the statement.
Legend:
1. Strongly disagree (my level of Information Security Awareness is very low)
2. Moderately disagree
3. Mildly disagree
4. Agree and disagree equally (my level of Information Security Awareness is as expected)
5. Mildly agree
6. Moderately agree
7. Strongly agree (my level of Information Security Awareness is high)

I selected multiple-choice questions as a method to query the participants on a subject, as well as educated them on the same subject. For example, on the pre/post-test questionnaires I queried for a description of ISA learning sources. This particular format was selected in order to help the participant recount how they go about finding awareness information. In addition, in case they were not familiar of the potential sources of awareness, the verbiage also helped them think of places to go to find information going forward. The question on the pre-test and post-test differed from a verb tense perspective. When querying the participant in the pre-test, I structured the question and multiple choice answers in the present tense. The intent was to have them recount activities that they are presently doing, not ideas of what they should be doing. Similarly, when I asked about experiences in ISA advocacy, I posted the multiple-choice answers using a past tense verb as I was collecting facts on actual activities, not ideas about possible activities.

During the pre/post questionnaires, regardless if the question is scalar or multiple choices, I provided the participant with a space to elaborate on their answers or to add a related comment. This was meant to provide opportunities of expression on the topics on the questionnaires.

Table 3.13 shows some common assessment topics across the ISA material content, discussion points, and questionnaire topics. These commonalities serve as cross validation during data analysis.

Potential contributions to learning and practice were drawn from this activity. If the level of knowledge was high for most participants, then the organizational investments in this area may remain status quo, and validation would be given to the organization's security posture. On the contrary, low knowledge self-assessment scores may lead to opportunities for improvements.

Table 3.13: Common Assessment Topics across Instruments

AR Workshop Pre/Post Questionnaire	Validity in Artifact Sampling Attributes	AR Workshop Group Discussion
The ISA content provided is in a language easy to understand.	ISA material presented is not complex.	If you are not an advocate for ISA, what are two reasons that hold you back?
I receive information security awareness e-mails.	Availability of content, format, timing and value	Please record ISA advocacy activities
I am comfortable and fluent with topics related to information security.	The informational session source is an industry related topic.	Please record challenges to ISA advocacy

Group Discussion Post Presentation

Spears and Barki (2010) used guided questions to conduct interviews to gather a deeper understanding of the phenomena in their study; I used the same approach to conduct group interviews (focus group) and share the same intent to explore phenomena from the point of view of the participants. The main difference is that my semi-structured questions were formatted in plural for the group setting. I was looking for the collective voice of the group when exploring behaviors, attitudes, and perspectives about ISA advocacy, while at the same time the same exchange of ideas served as a learning opportunity.

When discussing as a group, the participants had a copy of the data collection instruments and were able to write their answer on paper as we worked through the questions. To promote exchange of ideas, we recorded on the flip chart or white board the topic of discussion. I read the question aloud to the group, prompting them for their thoughts. My role at that moment was to record the answers given by the participants, to answer questions or provide clarification, to acknowledge their contributions and to listen. This allowed the participants to hear each other and verbalize their contributions for the discussions. Some participants contributed more than others did, and in some cases, a question was directed to the researcher for her input. This measurement is reflective of Lippitt's phases of change to "assess the resources and motivation of the change agent", and is part of diagnosing the problem, as described by Kritsonis (2005, p. 3).

Follow-up Emails

I used follow-up emails as the way to communicate with the participants after the workshop, once after three weeks had passed and again after six weeks. The intent was to measure the residual effects of the workshop on the participants. Using this method facilitated communication with the participants without the need to have an in-person meeting or a scheduled phone call. It also minimized researcher bias.

The emails only had two questions designed to query continuity of *advocacy behavior* and learning experiences. The first question prompted the participants to recount ISA advocacy activities they have done since the workshop. The second question prompted for learning opportunities, new or continued since the workshop. These email follow-up questions were similar to the format used during the workshop assessments, ensuring continuity in language.

Data Analysis and Interpretation Procedures

The techniques in this study compose the data analysis for this research, each adding to the multidimensional perspective of the study. I followed the guidelines described by Saldana (2013), Denzin and Lincoln (2011), and Creswell (2009) to maintain a structure to the approach. First, to identify the material that is included in the analysis. Table 3.14 summarizes the data source and analysis techniques used for the dimensions of the research.

Table 3.14: Data Source and Analysis Techniques

Sources from Instruments	Data Analysis Technique	Target Data	Measures	Contribution

Pre/Post Questionnaire: space for additional comments,
and
Group interview
	Content analysis	Attitudes, perceptions, behaviors;
		challenges;
		knowledge,
		change
			ISA advocacy,
			awareness;
			challenges and constraints;
			commitment
				Discovery of themes that motivate points of view

Pre/Post Questionnaire: Scales	Descriptive Statistics	Attitudes, perceptions, behaviors;
		challenges;
		knowledge,
		change
			ISA advocacy,
			ISA awareness;
			challenges and constraints;
			commitment
				Measurement of the themes that motivate points of view

Participant demographics	Descriptive Statistics	Demographic section of the pre-test questionnaire		Description of the participants' functional titles, and industry

Email follow-ups	Content analysis	Attitudes, perceptions, behaviors;
		challenges;
		knowledge,
		change
			ISA Advocacy	Residual differences for time periods after the workshop

Analysis included both inductive and deductive content analysis of data gathered during, and after the workshops. Leedy and Ormrod (2009) call to define the qualities of the material under examination. These are the codebooks defined later in this data analysis section. They also call to prepare the data in manageable pieces. The final step would be to follow the procedures to conduct the analysis steps Saldana (2013).

Preparing the Data for Analysis

The first step was to read all the information collected in a workshop, organize, and store the data. At this point of the study, each workshop respondent placed their responses in a sealed white envelope for temporary storage.

I began by de-identifying the respondent upon opening the envelope. This was done by creating a participant code like "Participant1" and writing that code on the top right corner of each assessment and on the consent form for all documents in the white envelope. From this point on, the data management utilized the corresponding participant code and never the person's actual name. Once all the envelopes were de-identified, all the consent forms containing the names of the participants were placed in one envelope. The envelope was sealed and stored in a secure location to protect the identity of the participants.

Preparing the Recordings for Transcription

I personally transcribed the recording into a Word document within 3 days of the workshop. This was important for a couple of reasons. One, since I facilitated the workshops it helped me recollect the experience, and this allowed me to enter my notes as I transcribed. Two, I felt the transcription would be more accurate since I am familiar with the context of the workshop discussions. I listened to the recording, hit pause and typed word for word the verbiage as it was articulated by the participants. When I thought of a note or reflection, I used the {NOTE: using bracket symbols} to enclose my note, and used the label NOTE to clearly identify this is a notation I added and not a participants comment. I labeled each participants comments with their coded pseudo name, and kept my name as is in the labeling to prevent confusing my comments from a participants comments. Figure 3.7, provides an example of Notes taken during the recording transcription.

Figure 3.7: Example of Notes

Example of Notes Taken During the Recording Transcription
[MD] So you are talking about what just happened with Target? [Grace] Yep [MD] OK I wasn't quite sure what you were talking about. OK now I understand {NOTE: I used this experience to introduce the subject of the workshop to future sponsors.}

As the topics of the discussions changed, I left a couple of lines in between, to differentiate the discussion topics and prepare the transcription for inductive coding. I also made note of what part of the workshop was I transcribing. If the comments were made during the presentation, I jotted which slide I was speaking to when the participants made the comments. I did this as marker to keep in mind the context of the comments in consideration when I began coding. Figure 3.8, shows an example of spaces inserted for clarity of the recording transcriptions.

Figure 3.8 Example of the Use of Spaces for Clarity

Example of Using Spaces for Clarity of Recording Transcription
{NOTE: Slide with Online Coupons} [Grace] Questions… [MD] No. [Grace] Sorry… [MD] Starting to worry. *SPACE inserted intentionally as a visual aid when the topics change.* {NOTE: Slide closing slide} [Grace] Any questions about this? [MD] Is there a way to erase your digital footprint? [Grace] We will get to that. [TC] I have a question, your previous slide, the seeking employment part, there, the second one, so how do they, how do people get into your information? Can you elaborate more on that? [Grace] Sure… {NOTE: looking for slide}

there is one about employment history [AV] yeah that one, Linked In. So in a site like monster.com so what they do is focus in just gaining access to that system but quickly harvest the databases of the users [TC] Got it, [Grace] Any other questions? No.

SPACE inserted intentionally as a visual aid when the topics change.

{NOTE: Slide Attack Motivators}

[CR] So don't share passwords with your friends and significant others. [Grace] ….

Once the recording transcription was completed, the Word document was formatted to aid in the content analysis procedures.

Preparing a Spreadsheet for the Questionnaire Responses

The pre-test, post-test assessments contained the responses to the Likert Scales and multiple choice questions. In preparation to the data analysis, I prepared a spreadsheet to enter the coded data. Following the guidance of Newton, R. & Rudestam, K. (1999), I prepare the spreadsheet columns for data entry of each case. I define my unit of measurement as each set of assessments, or workshop packet completed by each participant. The spreadsheet included all data collected from the workshop for each participant. The data coding process includes the data collected from the Likert scales, procedures for coding blank or missing responses, procedures for coding optional responses and procedures for coding open ended questions (write-ins).

Each spreadsheet tab represented the organized by assessment type, for example, the responses from all the pre-test questionnaires go in the PRE-TEST Tab of the spreadsheet. The columns were labeled by question number. Each row represents the participant's responses. The numeric values were included in the codebook as well. I added special codes for the cases where no responses where provided. In the cases where the participant left a question unanswered, the numeric code, ninety-two (#92) is entered in the data field of the spreadsheet to avoid problems during data analysis. In contrast, if the response was optional, and the participant chose not to disclose, the numeric code ninety-one (#91) was used. To increase data accuracy during data entry and facilitate the process of entering the data into the spreadsheet, I created a drop down box including the valid codes for most questions. The drop down box allowed me to select from the valid codes when entering the participant's responses. I used a small sample of participant's responses to pilot the data entry spreadsheet, the coding scheme and procedures. This was very helpful in documenting clarifications in the procedures to follow with the greater body of data. Figure 3.9 shows an example of the drop downs available for date entry of the age range of the participant.

Figure 3.9: Data Entry of Age Range

Data Entry of Age Range
20 - Representing the age range from 20 to 29
30 - Representing the age range from 30 to 39
40 - Representing the age range from 40 to 49
50 - Representing the age range from 50 to 59
60 – Representing the age range from 60 to 69
Other: A numeric Self-Coded entry for other, numeric value, representing the age range of the respondent.
91 – Respondent chose to not disclose

The codebook had the detail on valid codes for each variable that is entered into the spreadsheet as preparation for data analysis. For the question where an option is to enter additional entries, such as sources of ISA where the response is open ended, I created a list of entries as provided by the respondent.

Inductive and Deductive Content Analysis

The purpose of this component is to analyze the responses to the group dialogue, the additional comments provided in the pre/post questionnaires, and e-mail responses. In addition to the group discussion contributions from the workshop flip charts, data sources include transcripts from audio recordings. The expected results of the content analysis included themes, motivators, attributes, deep insights, and descriptors of reasons why managers are willing to share ISA with their employees. Following the foundational guidelines from Saldana (2013, p. 64) the first cycle of coding was deductive. The responses were coded into values derived from the literature. These are the codes that affect the variables of *ISA awareness, advocacy, challenges, constraints,* and *commitment* listed in the codebook for content analysis. I then proceeded with an inductive analysis looking for themes or schemas emerging from the participants' responses and created a consolidated list as output.

Saldana (2013) encouraged the coder to consider epistemology (action research methods) and ontology (pragmatism) alignment. In order to accomplish this I needed to revisit what insight I was seeking from the answers to my questions. My Action Research Exercise questions try to get a sense of the participant's real life settings and understand first hand, by giving the participants a voice about their advocacy best practices. The following is an example taken from appendix 6, which explores ISA advocacy experiences by asking the participants, *what are you doing*?

> *On the flipchart, white board, or comment area, please record four or five Information Security advocacy activities and best practices that your group presently*

engages in to promote, share, and direct the attention of your employees or peers to ISA learning?

As I searched for motivators towards or against ISA advocacy, I followed up the question with a question intended to understand, *why are you (not) doing*?

If you currently advocate for information security awareness in your company, what are two reasons you do it? If you feel that you are not currently a strong advocate for information security awareness, what are two reasons for this or that hold you back?

As I explored attitudes, beliefs and values, I asked the following:

What do you see as the benefits of middle managers being active advocates for information security awareness and behavior at this firm?

> *One the flipchart, white board or comment area, please record challenges or constraints you presently experience that you feel makes it harder for you to engage in information security advocacy behavior.*

Moreover, as I looked for action driven change, I explored what the participant are willing to do:

> *Highlight, write in, or circle on your individual sheet two or three ISA Advocacy activities that YOU feel are accomplishable and that YOU personally will commit to.*

The data was my source to explore and interpret the meanings within the answers. Saldana (2013) guides the readers to several methods like Process, Emotion, Values, Dramaturgical, and Focused coding for the First Cycle Coding methods. My first step in deciding on the proper coding method to use was to examine the characteristics of these methods against my pragmatic approach and action research method and select the potential coding methods by process of elimination. As I examined the options, I used Saldana's guidance and descriptions in a table 3.15, to help in my decision process.

Table 3.15: Sample Coding Method Considerations.

Coding Method	Appropriateness in Exploration	Characteristics at Glance	Why I Choose or Reject
Process	Extracts the participants actions and consequences	Looks for action in the data, sequences	My focus includes activity inquiry and motivations. I may in part support AR as a theory that brings change.
Emotion	Emotions recalled by the participants	Labels the emotions	Participants' feelings are not the focus of my study
Values	Codes reflecting values, beliefs and attitudes	The codes represent the participants point of view	My study does look for participants viewpoints.
Dramaturgical	Personal experiences. Action in case studies. Power relationships. The process of human motives.	Applies the terms and conventions of characters, play script and production analysis	My point of view is not focused on the participants as 'characters in a play' but from their motivations and experiences towards.
Focused	Categorizes code data based on thematic or conceptual similarity. Searches for the most frequent or significant codes first develop the major categories	Builds from the data, grounded theory	My study is based on exploring motivations in favor of ISA advocacy.
Descriptive	It is a summary of the finding using a phrase or a word.	Appropriate for data forms	My study uses forms to collect data.

From the suggested coding methods, I find a possible alignment with Descriptive. Since I am not an experience coder; I have multiple types of data (transcripts and workshop group discussions); this method enables me to create codes by topic by asking a simple question like "What is this about?" Descriptive coding supported the inductive content analysis by creating a list of codes as they emerged in the evaluation. Coding methods may help determine the effectiveness of Action Research Theory that aims to improve the practice of ISA advocacy.

The next step was to pilot a sample of the data with the coding methods to ensure I was not forcing the method to the data.

Procedure for Content Evaluation

Having prepared the transcripts and other available text, I began evaluating each text section looking for meanings related to the research questions and the entries in the codebook. As the text evaluation is in progress, I included my interpretation notes on the right hand side of the sheet.

1. Selected and read text section. I interpreted the meaning of the participant's comments. What were they communicating? Make notes on the right hand corner of the transcript.

2. As action research had the purpose of increase learning, I also looked for evidence of learning within the sections of the transcripts and make notes.

3. I evaluated the text selection against the codebook (begin with the first codebook entry and repeat the process with each entry in the codebook).

Each response was evaluated for common themes, which serve as categories, starting with the variables of interest, *ISA advocacy, ISA awareness*, *challenges* and *constraints*, and *commitments*. Did the text selection relate to any of the codes, if yes, identify which code, and interpret the text meaning?

4. If the selected text did not yield a codebook relationship, and I discovered a new code, I made a note on the transcript and add and entry to the codebook. During the inductive analysis, additional topics were discovered as related to attitudes, behaviors, perception, knowledge, and change.

The data sample would be an expression of motivation (category) in the participant's own words. For example, the ISA topic does not apply to the work environment, or the document was too long or takes up too much employee time.

As new code categories emerged, a constant comparative method, Leedy and Ormrod (2009), (category changes, shifts, expansions, and merges) was used to backtrack, and applicable information is added as needed. Saturation was achieved once the emergence of new codes is greatly reduced (over 50%). I used this coding template for new entries, adopted from Saldana (2013). Unlike the pre- existing codes, these emerge from the data, not the literature. In an attempt to support the coding decision, I also include as a step to write memos to document the reflections on the new code.

Code:

Sources: (citation table)

Description:

Example or finding

The guiding questions for the analytic memo, listed in Figure 3.9, are not applicable to all codes, but for consistency, I decided to make it a step to include, even if the question was not applicable.

Figure 3.9: List the Guiding Questions Adopted from Saldana (2013)

1. Reflect and write about how you personally relate to the participants or phenomena.

   Format: [Personal Relationship to the Study: my comments and reflections]

2. Reflect and write about how my study's research questions:

   Research Question 1: What do members of middle management know about information security risk awareness?

   Format: [Research Question 1: my comments and reflections]

   Research Question 2: What are members of middle management currently doing about advocacy of information security awareness?

   Format: [Research Question 2: my comments and reflections]

   Research question 3: Have members of middle management identified any factors that affect their or peer managers' ISA *advocacy behavior*?

   Format: [Research Question 3: my comments and reflections]

   Research Question 4: Do Action Research workshops have a measurable impact on positive ISA behaviors among Middle Managers who participate?

   Format: [Research Question 4: my comments and reflections]

3. Reflect and write about my code choices and their operational definition

   Format: [Code Definition: 'lack of time'+ my comments and reflections]

4. Reflect and write about emergent patterns, categories, themes

   Format: [Emergent patterns, categories, themes: "Dependence on IT" + my comments and reflections]

5. Reflect and write about possible networks (connections between codes)

   Format: [Networks: "Dependence on IT" - "lack of knowledge" +my comments and reflections]

6. Reflect and write about the relationships between codes and theories.

   Format: [Theory: Lippitt's +my comments and reflections]

   Format: [Theory: Action Research as a Theory +my comments and reflections]

7. Reflect and write about problems with the study

   Format: [Problem: not enough time during workshop +my comments and reflections]

   Format: [Problem: problem +my comments and reflections]

8. Reflect and write about any personal or ethical dilemmas with the study

   Format: [Ethics: What can I or should I contribute during group discussions +my comments and reflections]

9. Reflect and write about future directions for the study

Format: [Future Directions: future study + my comments and reflections]

10. Reflect and write about the analytic memos generated thus far

Format: [Meta Memo: + my comments and reflections]

11. Reflect and write about the final report

Format: [Final Report: x should be highlighted in the report + my comments and reflections]

The scheme and coding test were accomplished by soliciting peer feedback, which comes from a peer doctoral student or a peer information security professional willing to give an independent opinion. A member check, meaning review by respondents, was not advisable due to the limited amount of time the managers have to participate in the study and the concern that they would "re-write" their history, changing the pre-test knowledge to match their current *ISA knowledge*.

Coding Categories and the Codebook

The codebook included a definition of each category, an example from the text analyzed, and a counterexample. An initial codebook is based on literature. I define and label the codes listed in table 3.16 based on the common attributes found to describe the motivation. The codebook is categorized into broader groups as the themes emerge.

Table 3.16: Codebook for Content Analysis

Categories	Codes	Definitions	Example/ Counter Example	Sources

Level of *Awareness Knowledge*	High level of *awareness knowledge*	Expressions describing a high level of *awareness knowledge*.	Example:
			I changed the default password on my personal device.
			Counter example:
			When the browser screen looks in a certain way, it should be safe to use.
				Deyhle (2002);
				Mejias (2012);
				Siponen (2000)

	Neutral level of *awareness knowledge*	Expressions describing a neutral or adequate level of *awareness knowledge*.	Example: I heard smart phone apps could have security viruses; can you talk about that? Counter example: I never considered a virus came from the app I downloaded from the app store.	Dutta & Roy (2008); McLean(1992) ; Stephanou, A (2008)
	Low level of *awareness knowledge*	Expressions describing a low level of *awareness knowledge*.	Example: All large companies have good security. Counter example: You should look for the lock on the browser when deciding to use an online service	Furnell, Gennatou & Dowland (2002); Dutta & Roy (2008)

Advocacy Behavior	Advocacy benefits	A manager's perspective on benefits of being an active advocate of ISA.	Example:
			I advocate to protect our company reputation.
			Counter example:
			If you share, people think you are a know it all.
				Choi et al., (2008);
				Grojean, et al. (2004);
				Katsikas (2000);
				McLean(1992)
				Rokeach (1968)

	Advocacy past activities	Advocacy activities occurring as a past practice.	Example: We used to think it was unsafe to use the hotel business centers. Counter example: There is nothing we can do about data breaches, except not use the Internet.	Katsikas(2000)

	Advocacy present activities	Advocacy activities occurring as a current practice.	Example: Share email management best practices. Counter example: I received a phishing alert but did not forward it.	Iversen, Mathiassen & Nielsen (2004)

	Suggested activities	Ideas to improve a challenge with the objective to increase advocacy activities.	Example:
			Share ISA with peers.
			Counter example:
			ISA is the IT groups responsibility
				Desman (2003)
				Denzin & Lincoln (2011);
				McLean (1992);
				Siponen (2000)

Challenges and constraints	Irrelevant	Participants' responses used words inferring that the ISA content was not shared because it had no relevance to the employee's job function.	Example: ISA is not my job. Counter example: ISA is the IT groups responsibility	Baskerville & Myers (2004)
	Complex	Participants' responses used words inferring that the ISA content was not shared because the material was too technical or complex.	Example: Managers have different levels of understanding. Counter example: The awareness presentation was easy to understand.	Furnell, Gennatou & Dowland (2002) McLean(1992)
	Length	Participants' responses used words inferring that the ISA content was not shared because the tasks will take too long for the employees to perform.	Example: I do not have time to sit in a learning session about ISA. Counter example: I forward the email notifications to my peers.	Furnell, Gennatou & Dowland (2002)

	Lack of Time	Participants' responses used words inferring that they personally do not have time to manage ISA advocacy responsibilities	Example: I have too many responsibilities already. Counter example: I trust IT has this covered.	Furnell, Gennatou & Dowland (2002)
	Other challenges	Experiences that make it a challenge to advocate for ISA	Example: I never got guidance to share ISA. Counter example: The company asked you to share information.	Leach (2003)
Commitments	Plan for action	Advocacy activities the participant feels they can accomplish	Example: Be more diligent about training and awareness. Counter example: IT should add security topics to the newsletter.	Furnell, Gennatou & Dowland (2002); McLean(1992) ; Siponen (2000) Stanleigh (2008) Thomas (1990)

Demographic Analysis Procedure

This procedure included descriptive information about the participant demographics. The data helps understand who the participants are by describing their position at the organization. The demographics include:

- The age ranges of the management groups
- Responses provided by gender
- The percentage of managers who's job function is IT related

- The industry participating in the workshop
- The participants length of management experience
- The participant's length of employment with the present organization

The codebook, table 3.17, specifies the variables for the spreadsheet, the valid codes for data entry, and the type of data analysis targeted for each variable. The gender measurement is taken by workshop observation by counting the number of women and men attending the workshops.

Table 3.17: Demographics Questionnaire Codebook

Question	Coding Method	Values	Data Analysis	Interpretation of data
How many years have you been in a management position in your overall work experience?	Self-Coded by respondent	Numeric values 00-75 92 – left blank, by respondent (find and cite the average expectancy of work years)	Descriptive Statistics	Identify relationships (differences and similarities) between the overall work experience and the constructs in this study.
How many years have you been a manager at this institution?	Self-Coded by respondent	Numeric values 00-75 92 – Question not answered, left blank, by respondent	Descriptive Statistics	Identify relationships (differences and similarities) between the tenure at the organization and the major variables in this study

Select the closest number to your age range (circle only one):	Select one answer from choices provided	20 - Representing the age range from 20 to 29 30 - Representing the age range from 30 to 39 40 - Representing the age range from 40 to 49 50 - Representing the age range from 50 to 59 60 – Representing the age range from 60 to 69 Other: A numeric Self-Coded entry for other, numeric value, representing the age range of the respondent 91 – Respondent chose to not disclose	Descriptive Statistics	Identify relationships (differences and similarities) between the respondent age range and the major variables in this study:
Please select the closest match to your management level	Select one answer from choices provided	10 representing the Executive Management level. 20 representing the Non- Executive Management level. 30 representing the Non-Management level. 40 representing the IT Security Related Manager level. 92 – Question not answered, left blank, by respondent	Data inclusion validation	Application - Participant validation of management level for data inclusion in the study. If the level of management is not Non - Executive Management level the data will be excluded.

What is your industry?	Self-Coded by respondent	15 – Finance 25 – Education 35 –Community 45 – Manufacturing 55, 65, 74 – use to assign other unexpected industry Self-Coded by respondent. 92 – Question not answered, left blank, by respondent	Descriptive Statistics	Identify relationships (differences and similarities) between the respondent's industry and the major variables in this study.
Is your job function IT related	Select one answer from choices provided	3 - Representing the option YES, I work in IT or have IT related responsibilities. 6 - Representing the option NO, I don't work in IT or have IT related responsibilities 92 – Question not answered, left blank, by respondent	Descriptive Statistics	Identify relationships (differences and similarities) between the respondent's job function related (or not) to IT and the major variables in this study

Pre and Post Questionnaires

The use of scales during the pre and post-test questionnaires provided an opportunity to measure changes in self-assessed behaviors and attitudes of data collected. Upon observation of the data, I noticed missing entries or blank responses. The pre-test questionnaire contained more instances of blank responses for some questions compared to the post-test. Two possible interpretations to the missing data are, first, the participants begin the workshop without knowing or fully understanding what to expect. Second, the participants left the question blank as a reflection of neutrality, which might be the case after the exposure to the workshop during the post-test. In order to include and manage the cases with missing data, I chose to impute values based upon logical rules, Gelman and Hill (2006). My data strategy for the missing values included recording the data as blanks, and counting the blanks as a neutral response in the descriptive statistics. I used a logical rule that said my assumption is based on the nature of how the rest of the data looked. It is logical to assume that, when faced with a continuous scale from 1-7 of agree-disagree, with 4 as a neutral value, a non-answer can mean only two things: a) the individual could not place themselves on the scale because they did not know exactly how they felt, or b) they did not understand the question, so they chose to bypass it. In either case, it is logical to treat their non-response as a neutral one because it is the neutral category that is there to catch those who feel ambivalent about whether they agree or disagree. In this instance, those who do not answer the question simply have not committed to the fact that they are neutral, but it is logical to assume that this means, for the purpose of my study, that they are definitely not in categories 1-3 or 5-7, which would be the more radical areas of feeling. By placing them in the same category as those who actually committed to neutrality, they are grouped according to this logical assumption, which in the case of agree-disagree.

Descriptive statistics was used to analyze the data and identify the impact of the workshop on the manager's perspective, attitude, and behavior. In the Likert scale data presentation, I use the ratio of the participants' selection using percent (%) and I round up to the next the whole value, e.g. 2.62 was rounded to 3%.

I used the Wilcoxon Signed Rank Test (Zaiontz, 2014) which is a non-parametric variant of a paired t test, to measure the significance, meaning the difference between the arithmetic mean of the pre-test and post-test questionnaire responses. This method is consistently used in a repeatable format to show rigor in my data analysis. The steps at glance include:

a. Define Null and Alternative Hypothesis

H0 –there is no difference between data samples

H1 – there is a difference between data samples

b. State Alpha (0.05)

c. Calculate Test Statistic

The difference between data set 1 and 2. (data set 1 – data set 2 = difference)

Rank the results (differences) in order from smallest to largest

Calculate Positive R = Add (the sum) all the scores for the positive ranks.

Calculate Negative R = Add (the sum) all the score for the negative ranks.

Find T, the smallest of R+ and R-.

n is the number of observations.

Use T and n to calculate z

d. State Decision Rule (z distribution)

Find Critical Z or critical value in the table: http://www.real-statistics.com/statistics-tables/wilcoxon-signed-ranks-table/ If the Z calculated is less than the Z score or greater than Z calculated, reject the null hypothesis. For details on instructions followed, please see http://www.real-statistics.com/non-parametric-tests/wilcoxon-signed-ranks-test/.

Use case example, when measuring the participant's response in level of *awareness knowledge,* the pre-test questionnaire included the following statement; *I have a high awareness level of Information Security*. In the post-test, the participants are asked: *I have a high awareness level of Information Security knowledge as a result of attending this workshop.* In both cases, participants were instructed to assign a value of agreement with that statement from a scale from one to seven. From the data gathered in the pre and post-test, the T- Test compared the means of the two groups to determine if there was a significant difference in *awareness knowledge* between the pre and post-test questionnaire.

As mentioned earlier, each participants' set of assessments make up the unit of analysis. Although each workshop may have served as a unit of analysis, the samples may have been too small, statistically insignificant, and I ran the risk of disclosing the identity of my participants through case descriptions and the use of sample comments. The total numbers of participants from all workshops are included in the statistical data analysis. Most questions in the pre-test are compared with its counterpart on the post-test and the data is analyzed to measure improvements is favor of ISA advocacy as a result of the AR workshop. Table 3.18 shows the pre-test questionnaire Codebook, table 3.16 shows the post-test questionnaire Codebook.

Table 3.18: Pre-Test Questionnaire Codebook

Question	Coding Method	Values	Data Analysis	Interpretation of data
I have a high awareness level of Information Security.	Likert Scale	All Likert scales coded as: 1. Strongly disagree 2. Moderately disagree 3. Mildly disagree 4. Agree and disagree equally 5. Mildly agree 6. Moderately agree 7. Strongly agree 92 .Question not answered, left blank, by respondent	Statistics T-Test	Knowledge Level To measure differences between the level of Awareness (knowledge) prior and after the Action Research workshop.

Question	Coding Method	Values	Data Analysis	Interpretation of data
Describe the sources you use to learn about information security awareness (ISA) while at this organization. You may select the most appropriate, one or more from the following list, or add your own comments.	Multiple choice	1 -I search for bulletins published on the company intranet. 2 - I learn from my colleagues and peers. 3 - I attend ISA presentations and events. 4 - I watch company-posted webinars and videos. 5 - I receive information security awareness e-mails. 6 - I ask my local information security officers when I need information. 7 - I am not aware of the resources available to learn about ISA. 8 - I research ISA independently from external resources like the Internet. 9 - Please elaborate on any other sources you use to learn about information security awareness	Descriptive Statistics (Frequency)	To measure the most frequent sources of ISA use to learn about information security. To measure the impact on learning strategies as a result of the workshop.
The ISA content provided is in a language easy to understand.	Likert Scale	As above: 1 through 7 and 92.		Challenges and Constraints
The VIDEO ISA content provided is in the learning format I prefer.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-TEST	To measure differences between the learning formats preferences prior and after the Action Research workshop.
The TEXT ISA content provided is in the learning format I prefer.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-TEST	To measure differences between the learning formats preferences prior and after the Action Research workshop.

Question	Coding Method	Values	Data Analysis	Interpretation of data
The POWERPOINT presentation ISA content provided is in the learning format I prefer.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-TEST	To measure differences between the learning formats preferences prior and after the Action Research workshop.
The ISA content provided is just right in length	Likert Scale	As above: 1 through 7 and 92.	Statistics T-TEST Descriptive statistics	Challenges and Constraints
The ISA content provided is easy to find.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-TEST Descriptive statistics	Challenges and Constraints
I am comfortable and fluent with topics related to information security.	Likert Scale	As above: 1 through 7 and 92.		Learning comfort Knowledge Level
I know only what is applicable to my immediate work environment.	Likert Scale	As above: 1 through 7 and 92.		Learning comfort Knowledge Level
I need to learn more about information security.	Likert Scale	As above: 1 through 7 and 92.		Learning comfort Knowledge Level
I don't have many opportunities to advocate for information security awareness.	Likert Scale	As above: 1 through 7 and 92.		Advocacy
I think I should be involved as an ISA advocate, but have not done it before.	Likert Scale	As above: 1 through 7 and 92.		Advocacy
When I do receive ISA material, I always share it with my employees.	Likert Scale	As above: 1 through 7 and 92.		Advocacy
I have the resources available to contribute to ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.		Challenges and Constraints
I don't have the time available to contribute to ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.		Challenges and Constraints

Question	Coding Method	Values	Data Analysis	Interpretation of data
Describe your ISA *advocacy behaviors* experienced in the past few weeks. You may select the most appropriate, one or more from the following list, or add your own comments.	Multiple Choice	1- I forwarded an ISA informational bulletin to my employees or peers 2- I announced in my staff meeting an ISA event or presentation and encouraged attendance 3- I invited the information security department to present ISA in my all hands meeting or departmental meetings. 4- I shared an ISA news article I read or found on the Internet. 5- I forwarded an email update with my comments regarding an industry incident. 6- I talked about policies or regulations with my staff or peers. 7- I remind my staff to comply with clean desk or other security practices.		Advocacy

Table 3.19: Post-Test Questionnaire

Question	Coding Method	Values	Data Analysis	Interpretation of data
My level of ISA knowledge has increased as a result of attending this workshop.	Likert Scales	As above: 1 through 7 and 92.	Statistics T-TEST	Knowledge Level To measure differences between the level of Awareness (knowledge) prior and after the Action Research workshop.
I have a high awareness level of Information Security knowledge as a result of attending this workshop.	Likert Scales	As above: 1 through 7 and 92.	Statistics T-TEST	Knowledge Level To measure differences between the level of Awareness (knowledge) prior and after the Action Research workshop.
In your opinion, should a manager be part of raising ISA consciousness?	Likert Scales	As above: 1 through 7 and 92.	Descriptive Statistics	To measure the impact on levels of advocacy attitude as a result of the Action Research workshop.

Question	Coding Method	Values	Data Analysis	Interpretation of data
Describe any new plans to learn about information security awareness (ISA) provided by your organization. You may select the most appropriate, one or more from the following list, or add your own comments.	Multiple Choice	1- I will search for bulletins published on the company intranet. 2- I will attend ISA presentations and events. 3- I will watch company-posted webinars and videos. 4- I will sign up for information security awareness e-mails. 5-I will ask my local information security officers for more information. 6- I will ask my colleagues and peers for more information. 7- I will learn about the resources available to learn about ISA. 8- I research ISA independently from external resources like the Internet. 9- Please elaborate on any new plans to learn about information security awareness	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.
I would like to receive ISA content in a language easy to understand.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.
I would like to receive ISA content in VIDEO format.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.
I would like to receive ISA content in TEXT format.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.
I would like to receive ISA content in POWERPOINT presentation format.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop
I would like to receive ISA content that is just right in length.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.
I would like to receive ISA content that is easy to find.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on learning strategies as a result of the workshop.

Question	Coding Method	Values	Data Analysis	Interpretation of data
The ISA presentation did not affect my motivation or engagement ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.	Statistics T-Test	To measure the impact on advocacy motivation as a result of the workshop.
The ISA presentation motivated me to begin engaging in ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.		To measure the impact on advocacy motivation as a result of the workshop.
ISA presentation motivated me to increase my engagement in ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.		To measure the impact on advocacy motivation as a result of the workshop.
The ISA presentation motivated me to continue in my current high level of engagement in ISA advocacy.	Likert Scale	As above: 1 through 7 and 92.	Descriptive Statistics	To measure the impact on advocacy motivation as a result of the workshop.
Describe your desired comfort level related to information security knowledge. You may select the most appropriate, one or more from the following list, or add your own comments.	Multiple choice	1- I am already constantly learning about topics related to information security. 2- I need more training; I know only what is applicable to my immediate work environment. 3- I need to learn more, I don't know much about information security. 9- Please elaborate on your desired comfort level related to information security knowledge		Learning comfort Knowledge Level
Based on the commitment to action exercise, please list at two to five Information Security advocacy activities that YOU plan to engage in during the coming days or weeks.	Open ended	For each entry assign a number starting with 1 and incrementing by 1. For each repeated use of words from a previous entry, use the same code assigned.	Descriptive Statistics	To measure similarities in advocacy behavior commitments
Find opportunities to advocate for information security awareness.	Likert Scales	As above: 1 through 7 and 92.		To measure the impact on advocacy behaviors as a result of the workshop.
Get involved as an ISA advocate, just do it!	Likert Scales	As above: 1 through 7 and 92.		To measure the impact on advocacy behaviors as a result of the workshop.

Question	Coding Method	Values	Data Analysis	Interpretation of data
Subscribe to ISA material source and consistently share it with my employees.	Likert Scales	As above: 1 through 7 and 92.		To measure the impact on advocacy behaviors as a result of the workshop.
Obtain the resources available to contribute to ISA advocacy.	Likert Scales	As above: 1 through 7 and 92.		To measure the impact on advocacy behaviors as a result of the workshop.
Dedicate some time to contribute to ISA advocacy.	Likert Scales	As above: 1 through 7 and 92.		To measure the impact on advocacy behaviors as a result of the workshop.
Describe your ISA advocacy planned behaviors for the next few weeks.	Multiple choice	1- I will forward an ISA informational bulletin to my employees or peers 2- I will announce in my staff meeting an ISA event or presentation and encouraged attendance 3- I will invite the information security department to present ISA in my all hands meeting or departmental meetings. 4- I will share an ISA news article I read or found on the Internet. 5- I will talk about policies or regulations with my staff or peers. 9- Please elaborate on your ISA advocacy planned behaviors for the next few weeks		
Please describe what have you learned new about security concerns and the need for information security awareness and advocacy?	Open Ended	For each entry assign a number starting with 1 and incrementing by 1. For each repeated use of words from a previous entry, use the same code assigned.		To measure the impact on *awareness knowledge* and advocacy behaviors as a result of the workshop.

Trustworthiness of Data and Findings

Generating results and interpretations included thoroughly testing the working propositions and, in some cases, adjusting them. Validation emerged through the data patterns from the testing. "Validity is when an instrument measures what it has been designed to measure" (Thomas, 1990, p. 74). My instruments included a description of the intended concept studied for each questionnaire section. For example, see figure 3.10 below, in my pre and post-test survey, I included a description of the construct I measure before the question. In the example below the words in italic represent the construct measured, followed by the pre/post-test question:

Figure 3.10 Example of Intent of the Questions

Description of the Intent of the Questions
Current comfort level related to Information Security learning The following refers to the comfort level related to Information Security learning. Please select the box of a single score from 1 to 7, 1 means you strongly disagree with the statement and 7 means you strongly agree with the statement. How much do you agree with the following statement? I am comfortable and fluent with topics related to information security.

More importantly, validation of the working proposition must be consistent for each case tested. The researcher compares the analysis conclusions against the existing literature to find alignment as well as contradictions, and evaluate to find and include opposing points of view.

In their study, Kaarst-Brown and Guzman raised concerns about "capturing (i.e., representing) the lived experience using text in general" (2008, p. 4). Given the qualitative direction taken for this research, it is certainly a point of view to question as the instruments are developed in detail. In the assessments, I consistently addressed the question to the participants in language that directed the query to their personal experience. For example, the question: *If you currently advocate for information security awareness in your company, what are the two reasons you do it?* This question specifically asked about the participant's experience in the matter. This detailed measurement strengthens the objectivity of the researcher and bias.

Consistency in documented data evaluation and measurement prevented bias, since it leveraged a consistent procedure for all the data. This approach strengthened the construct validity, reliability and integration for qualitative studies (Leedy and Ormrod (2009), Denzin and Lincoln (2011), Rudestam and Newton (2007)). It is in alignment with my pragmatic approach, and intention of documenting the known reality to use as data to transform learning and practices.

The workshop dry run validated the viability of the AR workshop design to influence the participants in favor of *advocacy behavior*. At the end of the workshop dry run, my reviewer gained insights and ideas of ISA advocacy activities that were within her control to perform. She commented, "Going through this exercise has given me ideas about security advocacy that I didn't have before". This supported the workshop a measurable impact on positive ISA behaviors among managers who participate. In a secondary dry run to validate the design, my reviewer expressed a concept learned during the workshop. Specifically, "I just realized how my personal information can be at risk even though I do not use (social media) Facebook."

With the inclusion of peer review, consistent measurement, content analysis protocols, and development of constructs, I also followed guidelines for accomplishing reliability as described by (McNiff and Whitehead, 2006).

Pretesting: I performed peer reviews of the instruments and the ISA presentation with colleagues and critical friends to ensure the language and the questions were clear and formatted in a way that they addressed the intended construct.

Internal consistency: I documented and performed the procedures in a repeatable and consistent manner. In addition, to strengthen the structure of the findings, I evaluated and presented the data analysis from the perspective of the instruments as it was administered to the participants, and in the order of the research constructs evaluated. Finally, during the discussions chapter, I address the data analysis from the research questions point of view.

Equivalent forms: The instrument design consisted of several parts including a survey and the action research action exercise. (See Appendix: 4, 6 and 7). The survey data was measured consistently using descriptive and inferential statistics and the workshop group discussions were measured consistently using descriptive content analysis.

Test–retest: The instruments and procedures were documented step-by-step in a repeatable fashion.

Summary

This chapter outlined the action research approach, including the process, instrument development, and procedures for data collection and data analysis, and validation of efforts.

An Action Research workshop is the setting for activities leading toward learning, self-reflection of knowledge, and activities to gather suggestions to increase advocacy. The workshop itself contributed to information security and awareness learning. It is the topic to which the activities are applied. The self-assessment activity evokes reflection on the manager's opinion towards ISA knowledge and their need to learn more. The group discussion promotes dialogue on personal attitudes, content attributes, and other factor that may be interpreted as an influencing motivator towards sharing awareness with peers and employees. *Commitments* to change come from the ideas and suggested actions that these managers are willing to do to advocate security awareness.

The data analysis is a combination of an inductive and deductive approach. Dialogue, recommendation, feedback, and comments are analyzed with the techniques to explore the managers' perspectives on attitudes, perceptions, *behaviors*, *challenges*, *knowledge*, and change.

In chapter 4, I introduce the data findings, the interpretation of the data analysis, and lessons learned. The accumulation of the data and analysis serve as the foundation for recommendations to promote improvements in practice. Any organization can benefit from the research by applying the lessons learned through the research and promoting the ISA advocacy positive influences across the company.

Chapter 4: Data Analysis

This findings chapter is dedicated to the analysis and interpretation of data collected during the Action Research workshops. Each component of the design is examined separately to show the findings of the particular instruments. I used the pre-test and post-test questionnaire data to represent a measurement of the constructs awareness knowledge, advocacy behavior, challenges, and commitments through descriptive and inferential statistics. I used the content analysis of the action research group discussion to gain a deeper understanding of the participants' point of view of ISA advocacy and awareness knowledge. The email follow-ups measured the long-term effect on learning, improvements in practice, and as a measurement of the construct commitment through content analysis.

In the data interpretation section of this chapter, I evaluate and interpret the data by constructs. I chose a mixed-method approach for this study. A blend of qualitative and quantitative methods used during an Action Research workshop helped gain rich data to reveal perceptions, level of knowledge, and advocacy experiences. The first instrument administered was a pre-test questionnaire to measure ISA advocacy experiences and security awareness knowledge before beginning the workshop. This measurement provided data on existing knowledge and a recount of advocacy experienced prior to the workshop. Since it was a self-assessment, the questionnaire helped to eliminate the researchers influence and/or bias.

Descriptive statistics and content analysis were applied to the data to formulate an interpretation. Using descriptive statistics, I present the means for the individual questions as scores representing disagreement, neutrality, or agreement. Scores representing disagreement are from 1 to 3, while scores representing agree and disagree equally are 4; scores representing agreement are from 5 to 7. (The pre-test was also used to gather the participants' demographic data, which I shared in chapter 3.)

The workshop included an information security awareness presentation of industry data breaches. This presentation served to set the context of the workshop and to expose the group to information security awareness facts. Using content analysis of the transcribed recordings of the workshops, I present quotes from participants' comments about their reactions to the ISA artifacts presented to them.

Following the research design, the next instrument was an action research "action exercise", similar to a focus group. The group responded to semi-structured questions with dialogue and idea exchange, exploring ISA advocacy behaviors, challenges, and commitments to ISA advocacy. This exercise gave the participants a voice and a chance to express their reality based on their personal experiences, attitudes towards ISA, knowledge, and advocacy. This exercise also gave the participants an opportunity to commit to ISA advocacy and improvements in security behavior best practices.

After the group discussion, I administered a post-test questionnaire to measure planned ISA advocacy and security awareness knowledge gained as an effect of the workshop participation. This measurement additionally captured the immediate impact of the workshop and its effectiveness to increase learning. I used descriptive content analysis, descriptive and inferential statistics to analyze the data.

In order to measure the long-term effect of the action research, I used an email follow-up as the instrument to receive participants' feedback on ISA advocacy experiences and increase in awareness knowledge after three (3) and six (6) weeks of the workshop. The email follow-up is self-administered and had no time restrictions. The email follow-up also served as a way to eliminate the effect of researcher bias as the response on behalf of the participants was voluntary.

The variables in the study were derived from the literature and described in detailed in chapter 2. The findings are presented here in four (4) sections: awareness knowledge (Section 1), advocacy behavior (Section 2), challenges (Section 3), and commitments (change, attitudes, and values) (Section 4). The last section, 4 also represents the data findings on the final research question, supporting the effectiveness of action research as a method to increase learning and bring change into practice. For each one of these sections, I include which data supported each variable by their instrument component as listed in table format, labeled Data Analysis Findings. This includes the content analysis of the ISA presentation, the pre-test and post-test questionnaire descriptive and inferential statistics survey results, findings from the action research action exercise, and findings from the email follow-up.

Data Findings by Design Instrument

Pre-Test Questionnaire Summarized Responses

The pre-test questionnaire was administered right before the Action Research workshop. The questionnaire attempted to measure the constructs awareness knowledge, advocacy behavior, challenges, and commitments prior to experiencing the workshop. The pre-test questionnaire summary includes the results of each question in the order as it appeared in the survey. The descriptive statistics are included directly below or with the data comparisons to the post-test responses. The table 4.1 Summary of the Pre-Test Questionnaire Items shows a baseline of the participants' self-reflected perception of awareness knowledge, advocacy behavior, and challenges; followed by a brief description narrative. The participants' selection is represented in percentage, followed by the individual counts of the Likert scales in parenthesis.

Table 4.1: Summary of Pre-test Questionnaire Items (N=38)

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
7a	Awareness Knowledge	I have a high awareness level of Information Security.	3.9	45% (2,4,11)			21% (8,1)	34% (5,8,0)		
9a	Awareness Knowledge	The ISA content provided is in a language easy to understand.	3.4	29% (5,2,4)			45% (13,4)	26% (4,3,3)		
9b	Awareness Knowledge	The VIDEO ISA content provided is in the learning format I prefer.	3.7	18% (4,0,3)			66% (18,7)	16% (4,2,0)		
9c	Awareness Knowledge	The TEXT ISA content provided is in the learning format I prefer.	3.8	18% (4,0,3)			66% (16,9)	16% (2,3,1)		
9d	Awareness Knowledge	The POWERPOINT presentation ISA content provided is in the learning format I prefer.	3.9	13% (3,0,2)			71% (18 ,9)	16% (3,2,1)		
9e	Awareness Knowledge	The ISA content provided is just right in length.	3.7	21% (4,1,3)			65% (18 ,7)	14% (1,3,1)		
9f	Awareness Knowledge	The ISA content provided is easy to find.	3.6	26% (4,1,5)			63% (17,7)	11% (2,1,1)		

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
10a	Awareness Knowledge	I am comfortable and fluent with topics related to information security.	3.8	45% (2,7,7)			18% (4,3)	42% (11,2,2)		
10b	Awareness Knowledge	I only know what is applicable to my work environment.	4.1	32% (1,5,6)			24% (5,4)	44% (10,7,0)		
10c	Awareness Knowledge	I need to learn more about information security.	5.9	0% (0,0,0)			21% (4,4)	79% (7,11,12)		
11a	Challenge	I don’t have many opportunities to advocate for information security awareness.	4.1	21% (3,2,3)			32% (10,2)	47% (6,11,1)		
11b	Challenge	I think I should be involved as an ISA advocate, but have not done it before.	3.9	26% (3,1,6)			48% (16,2)	26% (6,4,0)		
11c	Advocacy Behavior	When I do receive ISA material, I always share it with my employees.	4.0	28% (2,4,5)			40% (12,3)	32% (5,5,2)		
11d	Challenge	I have the resources available to contribute to ISA advocacy.	3.3	44% (6,7,4)			32% (9,3)	24% (6,2,1)		
11e	Challenge	I don’t have the time available to contribute to ISA advocacy.	4.0	32% (3,3,6)			31% (9,3)	37% (9,3,2)		

Prior to the workshop, I asked the participants to self-assess their level of awareness (item 7a). The results show almost half of the participants, forty-five percent (45%), reported not having a high awareness level of information security prior to experiencing the workshop. Meanwhile, thirteen (13) participants or thirty-four percent (34%) had a positive self-assessment of awareness level. The neutral and blank responses account for twenty-four percent (24%). None of the participants selected he or she had a high awareness level.

Item 8, in the pre-test questionnaire prompt the participant to describe the sources used to *learn* about information security awareness (ISA) while at their organization. The responses listed below show a heavy reliance on colleagues and peers with fifty-eight percent (58%), followed by ISA emails with thirty-four percent (34%). Furthermore, thirty-four percent (34%) were not aware of the resources available to them for learning about ISA.

- 21% searched for bulletins published on the company intranet.
- 58% learned from my colleagues and peers.
- 05% attended ISA presentations and events.
- 11% watched company-posted webinars and videos.
- 34% received information security awareness e-mails.
- 15% asked my local information security officers when I need information.
- 34% were not aware of the resources available to learn about ISA.
- 13% researched ISA independently from external resources like the Internet.

In items 9a through 9f, participants reflected on their preferred learning formats. At this point of the workshop, responses are heavily represented by neutrality, which I interpreted as managers not having an opinion due to lack of context, or not having considered the value of language as part of their prior experiences. I found the highest number of blanks or non-responses in this set of pre-test question (9a-9f). The non-responses (blanks) range from 1 to 9 instances throughout the preferred learning format responses (see table 4.1). I combined the blank responses to the Agree and Disagree Equally as I interpret this as neutrality or not having an opinion on the subject. Under the option for ‘other’ in question 9g, several participants wrote in comments suggesting lack of *awareness knowledge* or awareness training. These were the statements used to express lack of awareness training on information security:

- *“Unaware of any content”*
- *“Not aware of ISA training at my facility”*
- *“I am not aware of my company providing ISA content”*

Item 10a through 10c measured the participants’ perceived fluency and comfort level related to Information Security topics. The responses to question 10a show forty-five percent (45%) of the participants reflected disagreement that they were fluent and comfortable, while forty-two percent (42%) reported agreement to some fluency with information security topics. Only eleven percent (11%) of the responses was neutral, leaving three (3) participants who left the entry blank. The neutral and blank responses account for eighteen percent (18%) of the responses.

On question 10b, thirty-five percent (35%) of the population expressed disagreement with the statement “*I only know what is applicable to my immediate work environment*”, while fifty percent (50%) expressed agreement, fifteen percent (15%) were neutral, and four (4) participants did not respond to the question. The neutral and blank responses account for twenty-four (24%) of the responses.

Despite the self-reported knowledge and comfort with information security topics, including those outside their immediate work environment, on question 10c, no one disagreed outright with the need to learn more about information security. On the contrary, eighty-eight percent (88%) were in agreement with the increased need to learn about information security.

Only twelve percent (12%) were neutral on the question, which could again be related to their higher or lower level of awareness knowledge. Four (4) participants did not respond to the question. The neutral and blank responses account for twenty-one (21%) of the responses. There were no additional comments provided by the respondents.

Item 11a through 11d measured prior experiences and opportunities for sharing ISA with the manager's employees or peers, eliciting data about both *challenges* and existing *advocacy behavior*. In these responses, the managers' shared opportunities, perceptions, and resources that they felt influenced their motivation to advocate for ISA.

In item 11a, almost half of the population forty-seven percent (47%) expressed agreement with the statement that they do not have many opportunities to advocate for ISA, while twenty-one percent (21%) disagreed. This perceived lack of opportunity may be a challenge to ISA advocacy. A little over a quarter, twenty-six percent (26%), of the respondents were neutral (Agree and Disagree Equally). Five percent (5%) of the responses were left blank, which could mean they did not have an opinion due to lack of context at this time of the workshop, (pre-test), or the question did not relate to their experiences. The neutral and blank responses account for thirty-one (31%) of the responses. The mean (4.4) is reflective of neutrality towards the statement, *I don't have many opportunities to advocate for information security awareness.* This suggests that at the point of the pre-test questionnaire, given their non-IT status, these participants may not have considered that there was an expectation that they should advocate for information security awareness.

In item 11b, twenty-six percent (26%) disagreed with the statement *I think I should be involved as an ISA advocate, but have not done it before*. The wording of the question leads to two potential interpretations, as there is the possibility that these twenty-six percent (26%) do not think they should be involved in ISA advocacy, or, that they believe they should be involved, but disagree because they have not done so before. Forty-two percent (42%) were neutral on this subject, while five percent (5%) did not respond. The neutral and blank responses account for forty-seven (47%) of the responses. The mean (3.9) is reflective of neutrality towards the statement *I think I should be involved as an ISA advocate, but have not done it before.* This suggests that during the pre-test questionnaire the participants did not understand the expectation that they should be involved as an ISA advocate.

In item 11c, twenty-eight percent (28%) responded they do not always share when they do receive ISA material, while slightly more respondents at thirty-two percent (32%) do share ISA material. Almost a third of the participants, thirty-two percent (32%), had a neutral response, and eight percent (8%) did not respond to this question at all. The neutral and blank responses account for forty (40%) of the responses. The mean (4.0) is reflective of neutrality towards the statement: *When I do receive ISA material, I always share it with my employees. This* is perhaps less important than the finding that almost one third *did* engage in advocacy behaviors though information sharing *prior* to the Action Research workshop, and another third who *sometimes* shared and sometimes did not.

In item 11d, forty-five percent (45%) responded with disagreement to the statement showing resource availability as a challenge to ISA advocacy. While twenty-four percent (24%) responded in agreement with the availability of resources to contribute to ISA advocacy, twenty-four percent (24%) responded with Agree and Disagree Equally, and eight percent (8%) did not provide a response. The neutral and blank responses account for thirty-two (32%) of the responses. The mean (3.3) is reflective of disagreement towards the statement: *I have the resources available to contribute to ISA advocacy*. This suggests that during the pre-test questionnaire, the majority of participants did not know if they had the resources to contribute to ISA advocacy.

In item 11e, thirty-two percent (32%) of responses disagreed they lacked time for ISA advocacy, however, thirty-seven percent (37%) of participants agreed that lack of time constrained their *advocacy behavior*. Twenty-three percent (23%) of the respondents were neutral, and eight percent (8%) did not respond to the question. The neutral and blank responses account for thirty-one percent (31%) of the responses. Roughly, 1/3 of the responses agree, 1/3 of the responses disagree, and 1/3 did not have a response. The greater number of all responses were in agreement supporting of lack of time to contribute to *advocacy behaviors*. No additional comments were added by the respondents to this topic. For this question, the mean (4.0) is reflective of the split opinions towards the statement: *I don't have the time available to contribute to ISA advocacy*. As will be noted later, some of the reason for this split was because of differences in understanding what ISA advocacy involved.

Item 12 in the pre-test questionnaire prompts the participant to select from a list, or describe in their own words their ISA *advocacy behaviors* in the weeks prior to the Action Research workshop. Responses to the listed *advocacy behaviors* were as follows:

- 8% forwarded bulletins
- 5% announced event opportunities
- 16 % shared articles
- 11% forwarded an email
- 18% talked about policies
- 5 % reminded staff of a best practice.

The data supported that managers had some prior experiences they could recognize from the list of *advocacy behaviors* provided. This suggests that at the time of the pre-test questionnaire the participants may not have recognized the behaviors examples of ISA advocacy, but did recall engaging in these activities.

Action Research "Action Exercise"

This portion of the workshop followed the Information Security Awareness presentation. In this step of the design, the participants discussed their responses to the questions in a group setting with the goal of exchanging ideas and learning from each other's experiences and contributions. Several participants approach the discussion as an opportunity to address concerns they had about specific security circumstances, looking for ways to make better online behavioral choices. For example, a common concern was not knowing when it was safe to click on a link when using a service or product. Another concern expressed was not knowing when to trust online messages that prompt for an upgrade on their computer software. The core of the issue is the lack of knowledge regarding how to differentiate between an authentic link upgrade message, and that of a malicious link upgrade message. By voicing their concern to the group, they began a dialogue with their peers about how to address the issue. This served as an opportunity for the peer group to share *awareness knowledge*, best practices, and ideas for strategies to adopt while using online services and ISA advocacy.

I analyzed the recording transcripts from each workshop using descriptive coding. I evaluated the dialogue that was generated through the semi-structured questions, looking for patterns and meanings related to the AR "action exercise". At the end of each question discussion, I listed on the whiteboard the participant's contributions provided during the exercise. I grouped all the findings looking for similarities and differences.

The first question asked managers to identify what they perceived as the benefits of being active advocates for information security awareness and behavior at their firm. Several participants related the ISA advocacy benefits to “the responsibilities one should assume in a management position”. Managers are responsible for employees, and as such, they related ISA advocacy benefits to a sense of duty that they should have towards their employees. One participant viewed sharing awareness as “a responsibility”, while another associated advocacy with “accountability towards the staff”. Another notable comment was about “maintaining the employees trust”. I summarize the benefits of being active advocates for ISA as follows:

- Awareness for accountability
- Positions of responsibility
- Accountability towards staff
- Employee trust

In the same discussion, there were over a dozen instances of the topic related to the protection of company information. The participants described it in several ways including, “preventing data loss”, “protecting intellectual property”, and “securing trade secrets and company information”. Participants also considered the need for “information protection at a personal and customer level”. They varied in their description of what information or artifacts warranted protection. While some participants used the word “information”, others were specific to “trade secrets”, “financial information”, “intellectual property”, “proprietary software”, and “company records”. Understanding different types of data and the association of its value to either business or one’s personal security is an opportunity for awareness education.

An increased level of personal awareness was identified as a means to learn, create consciousness, and to share the knowledge with others. The participants described the benefit as a way to help themselves and others. In addition to having knowledge, participants viewed this as a way to drive action in the form of help, protection, instruction, prevention, warnings, learning, and understanding. As noted by the numbers, some of these were unique statements, while others had multiple respondents with the same comments.

- “I want employees to be aware of the risks to their personal security”
- “It helps others learn”
- “Protect employees personal information (2)”
- “To have an overall awareness of IS”
- “Provide means to allow for sharing of information security”
- “Employees will have understanding of IS that currently don’t have”
- “Help warn and instruct others through communications (4)”
- “To raise awareness and consciousness”
- “Drives home the need for caution”
- “Stay knowledgeable on current information and trends (2)”
- “Knowing who to share or not share information with”
- “Help staff minimize their exposure of information (3)”
- “An opportunity to hold security Q & A during staff meetings”
- “Extend awareness throughout population including at home”
- “To set some basic guidance to follow”

After the detailed analysis of each workshop transcription, the next step was to consolidate the findings and group them to find similarities. Each of the following tables represents the consolidated list of responses from the action research action exercise (ARAE) questions 2 through 5.

In ARAEQ2, I asked the managers, *if you currently advocate for information security awareness in your company, what are two reasons you do it? If you feel that you are not currently a strong advocate for information security awareness, what are two reasons for this or that hold you back?* Table 4.2 show the contributions to the ARAE question 2, listing reasons to benefit or dissuade ISA advocacy.

Table 4.2: Consolidated Reasons to Advocate and Not Advocate for ISA

Reasons for ISA Advocacy Provided by Management Groups	Encourages or Deters	Supporting Literature
To better understand an online threat.	Encourages	Siponen (2001)
An honest attitude	Deters	Furnell, Gennatou & Dowland (2002) Loch et al. (1992)
The company's IT group provides all the protection necessary (3)	Deters	Loch et al. (1992)
Lack of appreciation, comment are not always welcome	Deters	Grojean, et al. (2004)
To keep people informed by sharing best practices with peers	Encourages	Grojean, et al. (2004)
Lack of time (2)	Deters	Furnell, Gennatou & Dowland (2002)
Advocate for ISA is to maintain a good company reputation.	Encourages	Grojean, et al. (2004)
Lack of consistent educational updates to maintain the *awareness knowledge* (3)	Deters	Furnell, Gennatou & Dowland (2002)
The company asks you to share security information.	Encourages	Grojean, et al. (2004)
Not my role (2)	Deters	Leach (2003) Grojean, et al. (2004)
Managers do not have the understanding or level of consciousness (13)	Deters	Furnell, Gennatou & Dowland (2002)
There has never been a word or guidance on the topic.	Deters	Leach (2003)
We share to help others protect their personal information (4)	Encourages	Grojean, et al. (2004)

In ARAEQ3, I asked the managers to write on the *flipchart, white board or comment area, four or five Information Security Advocacy activities and best practices that your group presently engages in which you feel promote, share, and direct the attention of your employees* *or peers to ISA learning*. Table 4.3 shows the contributions to the ARAE question 3, listing ISA advocacy activities.

Table 4.3: Consolidated List of Information Security Advocacy Activities

Advocacy Experiences	Supporting Literature	Best Practice to Promote Behavior
Talk to peers (2)	Grojean, et al. (2004)	Receive company notifications about phishing emails (3)
Send security alerts to the team (2)	McLean 1992	Use company approved devices
Obtain informational feeds from industry portals (2)	McLean 1992	Password management best practices (6)
Quarterly newsletter with security tips and best practices	McLean 1992	Change the default settings on your home router
Collaborative exchange with industry peers	Grojean, et al. (2004)	Change file name on the password file and encrypt the file
Have policies for employee to follow	Grojean, et al. (2004) Furnell, Gennatou & Dowland (2002)	Have a designated credit card for online purchase

In ARAEQ4, I asked the managers to write on the *flipchart, white board, or comment area, the challenges or constraints you presently experience that you feel makes it harder for you to engage in information security advocacy behavior*. Table 4.4 shows the contributions to the ARAE question 4, listing a consolidated list of ISA advocacy challenges.

Table 4.4: Consolidated List of Information Security Advocacy Challenges

ISA Advocacy Challenges	Supporting Literature
Lack of knowledge (4)	Leach (2003) Furnell, Gennatou & Dowland (2002)
Too many passwords is complicated (3)	Leach (2003) Furnell, Gennatou & Dowland (2002)
You do not want to seem overly concern	Siponen (2001)
If you think you know it all, people will not listen.	Grojean et al. (2004)
Different levels of awareness and knowledge	Furnell, Gennatou & Dowland (2002)
We are not asking	Not mentioned in prior literature
Addressing concerns is not a priority	Furnell, Gennatou & Dowland (2002) McLean (1992)
We do not want to bring up the subject, because things will be lock even more cannot do the job.	Leach (2003)
Difficulties of remaining up to date (2)	Furnell, Gennatou & Dowland (2002)
IT does not give guidance	Leach (2003) Grojean, et al. (2004)
Must use company provided laptop for access and they are very restrictive.	Leach (2003)
Trust in IT, false sense of security (5)	Loch et al. (1992)
Lack of education or training (3)	Furnell, Gennatou & Dowland (2002)
Not relevant to my work (3)	Siponen (2001)

In ARAEQ5, I asked the managers, *Are there ways that you could overcome or remove these? Is there support that the company could provide to help you overcome them?* Table 4.5 shows the contributions to the ARAE question 5, listing ways to overcome the challenges they identified dissuading ISA advocacy.

Table 4.5: Consolidated List of Ways to Overcome Challenges

Suggested ways to overcome challenges	Supporting Literature
Provide training updates in reoccurring timeline.	Furnell, Gennatou & Dowland(2002)
Hold AR awareness sessions.	McLean (1992)
Provide webinars	McLean (1992)
Be more diligent through training and awareness	Katsikas (2000)
Clarify awareness advocacy expectations (top down).	Grojean, et al. (2004)
Meet with IS department for updates discuss user experience.	McLean (1992)
ISA- Help people understand cost of breach, indirect impact, reputation	McLean (1992)
IT Newsletter should have security topics	McLean (1992)
Better understanding of the different types of security.	McLean (1992)
Take responsibility to investigate if something does not look right	Leach (2003)
Visible postings in the lunch area.	Leach (2003)
Use internal network for regular reminders about ISA	McLean (1992)
Promote awareness of policies	McLean (1992)
Amplification of policies with explanation of reasons behind policies.	McLean (1992)

Suggested ways to overcome challenges	Supporting Literature
Mandatory training that is engaging and interactive.	Katsikas (2000)
Start teaching the clients ISA	Katsikas (2000)

Individual *Commitment* to ISA Advocacy Behavior

The last step of the ARAE was to set individual goals for accomplishable ISA activities. The participants were asked to look over the discussion points and ideas exchanged and list the ISA activities they thought they would be willing to accomplish going forward. Participants wrote their plans on individual *commitment* sheets. The responses were tabulated by individual workshops, with repeated responses consolidated and then grouped by common themes.

Similar to the responses in ARAEQ3, when I asked the participants for ISA advocacy *commitments*, the results varied between two categories, “activities promoting ISA” and “security best practice improvements”. Every group submitted activities under both categories, supporting the need to learn more about the topics before reaching a comfort level to share the information.

The list below represents the consolidation of *commitments* towards ISA advocacy activities. Their responses suggest they have an understanding of action driven change that is necessary to increase the awareness of information security. It is also suggestive of the need for learning as much as the goal to share with others and is reflective of the response to the presentation. The items on the lists are action driven tasks that are simple to do and accomplishable.

Consolidated ISA advocacy *commitment* activities

- “Talk to family about risk of security breach and tips to minimize the risk”

- "Emphasize important of ISA to my employees"
- "Provide tools to emphasize ISA"
- "Promote others to also learn and commit to ISA"
- "Collectively learn more about ISA"
- "Get more connected with IT for ISA updates"
- "To engage in more ISA group activities"
- "Promote company ISA sessions"
- "Share ISA at a personal level"
- "Get presentation from industry related sites"
- "Create Google account for breach news and pass them to employees"
- "Have regular ISA conversations at team meetings"
- "Communicating of best practices and strategies for ISA"
- "Communicate breaches in a clear way"
- "Talk to employees about what we are doing today"
- "More research awareness of threat"

The list below represents the consolidation of *commitments* to ISA best practices provided by the management groups during the Action Research workshops. Their responses suggest they have common themes where online behaviors can improve. This can also serve as topics of ISA they can start promoting as they learn. Most of the themes are concentrated around the management of passwords, email accounts, online shopping accounts, and devices.

- User ID and Password Management:
  - "Use complex password"
  - "Not sharing sign-in and password"
  - "Change all my passwords to be unique"
  - "Make sure I don't use the same passwords for all my sign in"
  - "Use different passwords for different service"

- Device Management:
  - "Not use personal devices for company business"
  - "Read the agreement when downloading an Smartphone app"

- Email Management:
    - “Limit use of email from vendors”
    - “Use unique email accounts for the different online services”
    - “Close inactive email accounts”
    -
- Online Accounts Management:
    - “Actively monitor online account activities”
    - “Constantly monitor my financial accounts’
    - “Use a credit card for online shopping”
    - “Use PayPal for online shopping”
    - “Linked my PayPal account to a separate checking account”
    - “Do not give your personal information to any store”
    - “Erase credit card number from online stores”
    - “Set up bill pay. Do not allow access to your bank account”
    - “Check your online account statements often”
- Information Management:
    - “Limit my social media posts”
    - “Have a strategy to know what to do in case of a breach”
    - “Be suspicious; don’t assume your information is not compromised”
    - “Don’t give out the same information for every online account”
    - “Use a strategy for banking financial and non-financial”

Post-Test Questionnaire Summarized Responses

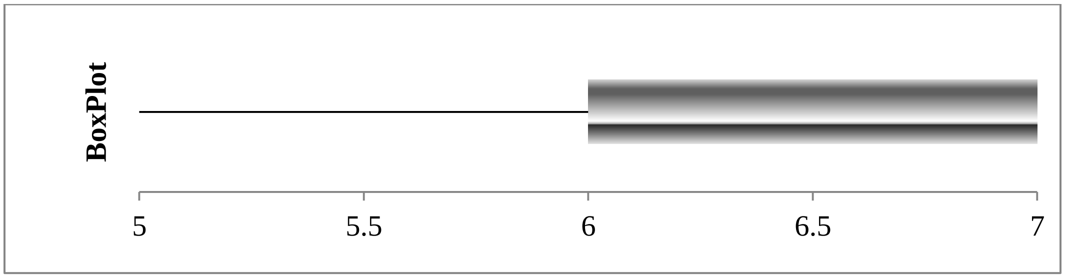
The post-test questionnaire was administered right after the Action Research workshop. The data reflects the immediate impact of the workshop on the constructs *awareness knowledge, advocacy behavior, commitments* and *challenges*.

The table 4.6 summarizes the instrument items measuring the level of information security *awareness knowledge*. The participants’ selection is represented in percentage, followed by the individual counts of the Likert scales in parenthesis.

In item 1a, most respondents were in agreement with the statement, *my level of ISA knowledge has increased as a result of attending this workshop.* Thirty-two percent (32%)

strongly agreed, Fifty percent (50%) moderately agreed, and thirteen percent (13%) mildly agreed. Two (2) participants, representing five percent (5%), did not answer the question. None of the participants disagreed with the statement, clearly supporting that the Action Research workshop increased their learning about information security awareness. The mean (6.1), shown in the box plot (figure 4.1), is reflective of the strong and almost unanimous agreement. The box plot supports the response distribution with a minimal score of five (5) and the maximum score of seven (7).

Figure 4.1 Box Plot Showing Increase in ISA Knowledge



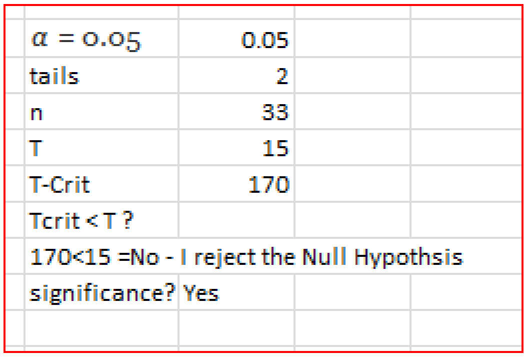
In item 1b, respondents agreed to the statement, *I have a high awareness level of Information Security knowledge as a result of attending this workshop*. Eighteen percent (18 %) strongly agree, forty-two percent (42%) moderately agree, and thirty-two percent (32%) mildly agree. Three (3) participants, representing eight percent (8%), did not answer the question. The neutral and blank responses account for eight percent (8%) of the responses.

I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 7a with the post-test item 1b, to show if the workshop improved the participants' level of *awareness knowledge*.

H0 – There is no significant difference between the pre-test and post-test awareness level of Information Security knowledge.

H1- There is a significant difference in awareness level of Information Security knowledge as a result of attending this workshop.

Figure 4.2: Non-Parametric T-Test for Awareness Knowledge



$\alpha = 0.05$	0.05
tails	2
n	33
T	15
T-Crit	170
Tcrit < T ?	
170<15 =No - I reject the Null Hypothsis	
significance?	Yes

Since T-critical (170) is not less than T (15), I reject the null hypothesis, and accept the alternative H1. Prior to the pre-test, the participants may not have questioned their individual ISA level of knowledge. The pre-test responses show a mix of agreement and disagreement leaning slightly towards disagreement with having a high level of *awareness knowledge*. The post-test data, however, is clustered around agreement of an increase of ISA knowledge, suggesting the immediate impact of the workshop. The T-Test supports the impact on learning by showing there is a significant difference ($p < 0.05$) in awareness level of information security knowledge between the pre-test and post-test responses. This suggests an increase of *awareness knowledge*.

When answering the item 1c, in your opinion, should a manager be part of raising ISA consciousness? Ninety-two percent (92%) of the respondents answered in a positive were towards *advocacy behavior*. That is, forty-seven (47%) strongly agree, thirty-two percent (32%) moderately agree and thirteen percent (13%) mildly agree. One participant, Agree and Disagree Equally, while two participants did not answer the question. The neutral and blank responses account for eight percent (8%) of the responses. The sample set is not a comparison between the pre-test and post-test. The question is specific to the effect of the workshop on the construct awareness advocacy.

Table 4.6: Summary of Items Related to ISA Knowledge (N=38)

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
1a	Awareness Knowledge	My level of ISA knowledge has increased as a result of attending this workshop.	6.1	0% (0,0,0)			5% (0,2)	95% (12,16,7)		
1b	Awareness Knowledge	I have a high awareness level of Information Security knowledge as a result of attending this workshop.	5.7	0% (0,0,0)			8% (0,3)	92% (12,16,7)		
1c	Awareness Knowledge	In your opinion, should a manager be part of raising ISA consciousness?	5.5	0% (0,0,0)			8% (1,2)	92% (5,12,18)		

Item	Statistical Inference
1a	The clustering of the data suggests the Action Research workshop had an impact on the participant's learning of the topic.
1b	The T-Test result supports there is a significant difference ($p < 0.05$) in awareness level of Information Security knowledge as a result of attending this workshop.
1c	The clustering of the data suggests the Action Research workshop influenced the respondents' opinions enough to drive change on the practice of raising ISA consciousness as a result of the workshop.

In item2, the participants were given a list of learning sources and sample learning behaviors to describe any new plans to learn about information security awareness (ISA). In this statement, the sources of ISA content impact the *awareness knowledge* construct by exploring the actual and planned learning activities. I compared the difference between responses in the pre-test item 8, where the statements are existing behavior, as in actual activities and the post-test item 2, where the statement are desired behavior in learning activities.

In analyzing the participant selection of sources, *learning from colleagues and friends*, and *receiving emails* were the most selected learning activities of information between pre and post-test. During the workshop, participants learned activities they can do to learn more about information security. In each of these cases, there was an increase in the selection of learning activities, suggesting that prior to the workshop they had not engaged. Given the new awareness, they are willing to consider.

- Bulletins published on the company intranet increased by sixteen percent (16%)
- Learn from my colleagues and peers decreased by eight percent (8%)
- Attend ISA presentations and events increased by thirty-nine percent (39%)
- Watch company-posted webinars and videos increased by twenty-one percent (21%)
- Receive ISA e-mails decreased by eight percent (8%)
- Ask my local information security officers when I need information increased by sixteen percent (16%)
- Research ISA independently from external resources like the Internet increased by thirteen percent (13%)

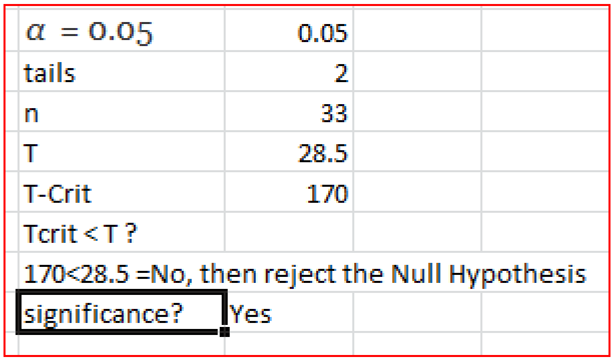
The number of respondents that were not aware of the resources available to learn about ISA changed from thirty-four percent (34%) in the pre-test, to thirty-eight percent (38%) in the post-test, suggesting there is a group of participants that are still challenged with learning activities as it may apply to their company. In the post-test there is a decline for in the selection *learn from colleagues and peers*, suggesting that after the workshop participants have a better understanding of learning activities available to them and don't have to lean heavily on their peers.

In items 3a through 3f, participants used Likert scales to measure the preferences in the ISA content format and content attributes of future awareness learning opportunities. The table 4.7 shows a summary of the ISA format related questions, the construct related to the question and the responses to the instrument items. Following the table is the narrative describing my interpretation to the responses.

Table 4.7: Summary of ISA Format Related Questions (N=38)

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
3a	Awareness Knowledge	I would like to receive ISA content in a language easy to understand.	5.8	3% (0,0,1)			13% (2,3)	84% (5,11,16)		
3b	Awareness Knowledge	The VIDEO ISA content provided is in the learning format I prefer.	5.4	5% (0,1,1)			29% (8,3)	66% (8,7,10)		
3c	Awareness Knowledge	The TEXT ISA content provided is in the learning format I prefer.	5.0	8% (2,0,1)			24% (4,5)	68% (10,12,4)		

3d	Awareness Knowledge	The POWERPOINT presentation ISA content provided is in the learning format I prefer.	5.2	8% (0,1,1)	16% (7,3)	68% (9,13,4)
3e	Awareness Knowledge	The ISA content provided is just right in length.	6.0	3% (0,0,1)	18% (2,5)	84% (5,12,15)
3f	Awareness Knowledge	The ISA content provided is easy to find.	6.2	3% (0,0,1)	13% (2,3)	84% (2,11,19)

Item	**Descriptive Statistics or Inference**
3a	The clustering of the data, mean =5.81, suggests the Action Research workshop had an impact on the participants' desired preference in ISA content. I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9a with the post-test item 3a. H0 – There is no significant difference between the pre-test and post-test preferred format is in a language easy to understand. H1- There is a significant between the pre-test and post-test preferred format is in a language easy to understand.  α = 0.05 0.05 tails 2 n 33 T 28.5 T-Crit 170 Tcrit < T ? 170<28.5 =No, then reject the Null Hypothesis significance? Yes The T-Test support there is a significant difference in means (p > 0.05) between the pre-test and post-test preferred format of the attribute "language easy to understand".

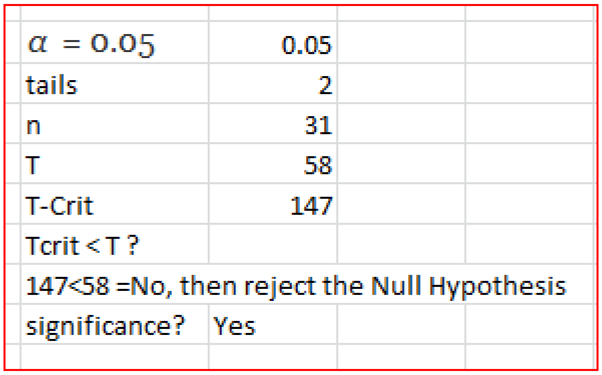
3b

The clustering of the data, mean =5.40, suggests the Action Research workshop had an impact on the participants' desired preference in ISA content.

I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9b with the post-test item 3b.

H0 – There is no significant difference between the pre-test and post-test responses on the ISA content preferred in video format.

H1- There is a significant between the pre-test and post-test responses preferred on the ISA content preferred in video format.



α = 0.05	0.05		
tails	2		
n	31		
T	58		
T-Crit	147		
Tcrit < T ?			
147<58 =No, then reject the Null Hypothesis			
significance?	Yes		

The T-Test supports there is a significant difference ($p < 0.05$) between the pre-test and post-test means for the preference of ISA content in video format.

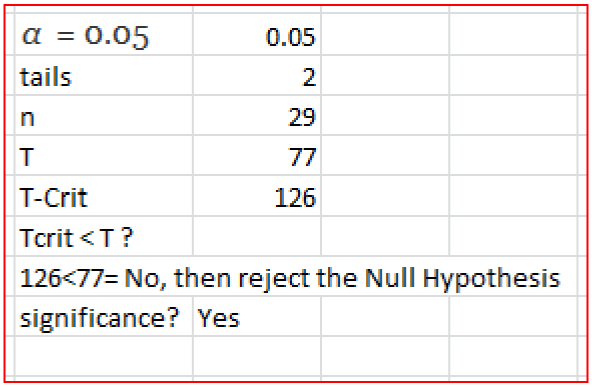
3c

The clustering of the data, mean =5.08, suggests the Action Research workshop had an impact on the participants' desired preference in ISA content.

I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9c with the post-test item 3c.

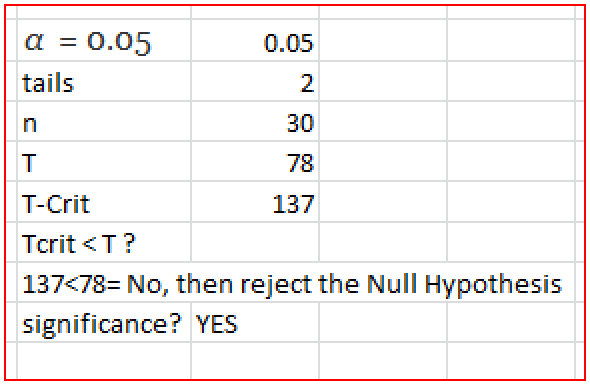
H0 – There is no significant difference between the pre-test and post-test responses on the ISA content preferred in text format.

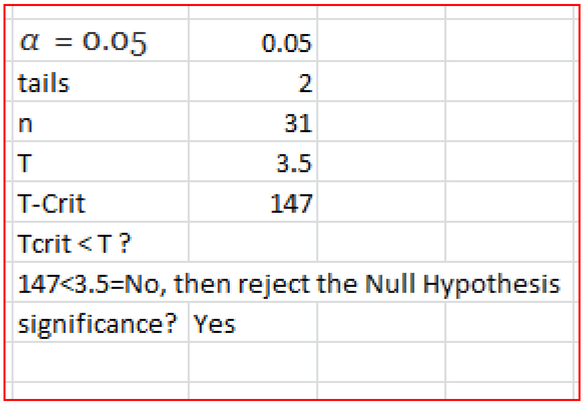
H1- There is a significant between the pre-test and post-test responses preferred on the ISA content preferred in text format.

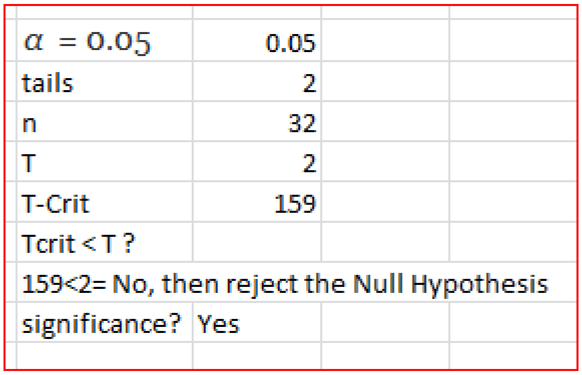


α = 0.05	0.05
tails	2
n	29
T	77
T-Crit	126
Tcrit < T ?	
126<77= No, then reject the Null Hypothesis	
significance?	Yes

The T-Test supports there is a level of significance ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content in text format.

<table>
<tr>
<td>3d</td>
<td>
<p>The clustering of the data, mean =5.25, suggests the Action Research workshop had an impact on the participants' desired preference in ISA content.</p>
<p>I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9d with the post-test item 3d.</p>
<p>H0 – There is no significant difference between the pre-test and post-test responses on the ISA content preferred in power point format.</p>
<p>H1- There is a significant between the pre-test and post-test responses preferred on the ISA content preferred in power point format.</p>

<table>
<tr><td>α = 0.05</td><td>0.05</td></tr>
<tr><td>tails</td><td>2</td></tr>
<tr><td>n</td><td>30</td></tr>
<tr><td>T</td><td>78</td></tr>
<tr><td>T-Crit</td><td>137</td></tr>
<tr><td>Tcrit < T ?</td><td></td></tr>
<tr><td colspan="2">137<78= No, then reject the Null Hypothesis</td></tr>
<tr><td>significance?</td><td>YES</td></tr>
</table>
<p>The T-Test supports there is a level of significance of (p < 0.05) between the pre-test and post-test responses preferred on the ISA content preferred in PowerPoint format.</p>
</td>
</tr>
</table>

<table>
<tr>
<td>3e</td>
<td>
<p>The clustering of the data, mean =6, suggests the Action Research workshop had an impact on the participants’ desired preference in ISA content.</p>
<p>I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9e with the post-test item 3e.</p>
<p>H0 – There is no significant difference between the pre-test and post-test responses on the ISA content preferred on length.</p>
<p>H1- There is a significant between the pre-test and post-test responses preferred on the ISA content preferred on length.</p>

<table>
<tr><td>α = 0.05</td><td>0.05</td></tr>
<tr><td>tails</td><td>2</td></tr>
<tr><td>n</td><td>31</td></tr>
<tr><td>T</td><td>3.5</td></tr>
<tr><td>T-Crit</td><td>147</td></tr>
<tr><td>Tcrit < T ?</td><td></td></tr>
<tr><td colspan="2">147<3.5=No, then reject the Null Hypothesis</td></tr>
<tr><td>significance?</td><td>Yes</td></tr>
</table>
<p>The T-Test supports there is a level of significance of (p < 0.05) between the pre-test and post-test responses preferred on the ISA content attribute on “just the right length”.</p>
</td>
</tr>
</table>

<table>
<tr>
<td>3f</td>
<td>
<p>The clustering of the data, mean =6.28, suggests the Action Research workshop had an impact on the participants' desired preference in ISA content.</p>
<p>I performed a two-tailed Wilcoxon Signed-Ranks Test for Paired Samples with α = .05 to test the following null hypothesis. The hypothesis below compares the results from the statements from the pre-test item 9e with the post-test item 3e.</p>
<p>H0 – There is no significant difference between the pre-test and post-test responses on the ISA content that is easy to find.</p>
<p>H1- There is a significant between the pre-test and post-test responses preferred on the ISA content that is easy to find.</p>

<table>
<tr><td>α = 0.05</td><td>0.05</td></tr>
<tr><td>tails</td><td>2</td></tr>
<tr><td>n</td><td>32</td></tr>
<tr><td>T</td><td>2</td></tr>
<tr><td>T-Crit</td><td>159</td></tr>
<tr><td>Tcrit &lt; T ?</td><td></td></tr>
<tr><td colspan="2">159&lt;2= No, then reject the Null Hypothesis</td></tr>
<tr><td>significance?</td><td>Yes</td></tr>
</table>
<p>The T-Test supports there is a level of significance of ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content that is "easy to find".</p>
</td>
</tr>
</table>

The responses to the question 3a reveal the preference in format for receiving awareness information in the future. In general, most respondents *would like to receive content in a language that is easy to understand.* There were no responses strongly or moderately disagreeing with the statement, however, one participant, indicative of three percent (3%), mildly disagree. Two (2) respondents, representing five percent (5%), agree and disagree equally with the statement. The majority of the participants, eighty-four percent (84%), responded in agreement with the format preference favoring content in a language easy to understand. Within this group, forty-two percent (42%) strongly agree, twenty-nine percent (29%) moderately agree and thirteen percent (13%) mildly agree. Eight percent (8%) did not respond, with the neutral and blank responses account for thirteen percent (13%) of the responses.

When I compare the ISA content format preferences in the pre-test (item 9a), the level of disagreement to receiving content that is easy to understand is higher in the post-test (item 3a) only three percent (3%) mildly disagree and five percent (5%) remain neutral. The pre-test shows a lower level of agreement while most respondents increased in agreement with the statement in the post-test, which represents a desired experience. The mean (5.8) is reflective of the agreement to the statement indicating a desired preference in ISA content format. Compared to the mean (3.5) in the pre-test, it also suggests that the participants began to recognize the value of the format of the ISA content. During the evaluation of language easy to understand, the participants experience prior to the workshop was limited. Once they experienced an awareness session, they were able to opine on the simplicity of the language. After the workshop the participants know what attributes to look for, the participants had this attribute to consider for future learning.

Continuing the analysis of the preference in format for receiving awareness information in the future is the item 3b, video ISA content as a preferred learning format. During the pre-test eighteen percent (18%) responded with complete or partial disagreement compared to five percent (5%) in the post-test, representing a thirteen percent (-13%) decrease on the level of disagreement. Another noticeable difference is the decrease of Agree and Disagree Equally by ten percent (-10%).

Sixty-six percent (66%) of participants responded with complete or partial agreement compared to the pre-test. Eight percent (8%) strongly agree, twenty-six percent (26%) moderately agree and eighteen percent (18%) mildly agree. The number of responses left blank decreased by ten percent (-10%) from eighteen percent (18%) to eight percent (8%), or three (3) respondents. The neutral and blank responses account for twenty-nine percent (29%) of the responses. The T-Test supports there is a level of significance of ($p < 0.05$) between the pre-test and post-test means for the preference for ISA content preferred in video format. The arithmetic mean for the responses to the post-test is 5.4. The mean is reflective of the agreement to the statement indicating a desired preference in ISA content format. The data suggest that during the initial evaluation of the ISA content format the participants experience prior to the workshop was limited. Once they experienced an awareness session, they were able to opine on the attributes of the content format.

The next analysis of the preference in format for receiving awareness information in the future is the item 3c, TEXT ISA content as a preferred learning format. In the pre-test eighteen (18%) responded with complete or partial disagreement compared to eight percent (8%) in the post-test, representing a ten percent (-10%) decrease on the level of disagreement. Another noticeable different is the decrease of Agree and Disagree Equally by twelve percent (-12%).

Sixty-eight percent (68%) of participants responded with complete or partial agreement compared to the pre-test. Eleven percent (11%) strongly agrees, thirty-two percent (32%) moderately agree and twenty-six percent (26%) mildly agree. The number of responses left blank decreased by five percent (-5%) from eighteen (18%) to thirteen percent (13%) or five (5) respondents. The neutral and blank responses account for twenty-four percent (24%) of the responses.

The T-Test supports there is a level of significance ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content preferred in text format. The data suggest that during the initial evaluation of the ISA content format the participants experience prior to the workshop was limited. Once they experienced an awareness session, they were able to opine on the attributes of the content format. After the workshop the participants know what attributes to look for, the participants had new knowledge to consider for future learning.

Following the text format, is item 3d, the analysis for receiving awareness information in the future in PowerPoint. In the pre-test thirteen percent (13%) responded with complete or partial disagreement compared to eight percent (8%) in the post-test, representing a five percent (-5%) decrease on the level of disagreement. Another noticeable difference is the decrease of Agree and Disagree Equally by fourteen percent (-14%).

Sixty-eight percent (68%) of participants responded with complete or partial agreement compared to the pre-test. Eleven percent (11%) strongly agrees, thirty-four percent (34%) moderately agree and twenty-four percent (24%) mildly agree. The number of responses left blank decreased by ten percent (-10%) from eighteen (18%) to eight percent (8%). The neutral and blank responses account for sixteen percent (16%) of the responses.

The T-Test suggests there is a level of significance ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content preferred in PowerPoint format. The arithmetic mean for the responses to the post-test is 5.2. The mean is reflective of the agreement to the statement indicating a desired preference in ISA content format. The clustering of the data suggests the Action Research workshop had an impact on the participants' desired preference in ISA content. The data suggest that during the initial evaluation of the ISA content format the participants experience prior to the workshop (mean=3.9) was limited. Once they experienced an awareness session, they were able to opine on the attributes of the content format.

I found similar results when the length of the ISA content was the attribute analyzed. In post-test item 3e, participants' assessed the length attribute preference for receiving awareness information in the future. In the pre-test twenty-one percent (21%) responded with complete or partial disagreement compared to three percent (3%) in the post-test, representing an eighteen percent (-18%) decrease on the level of disagreement. Another noticeable different is the decrease of Agree and Disagree Equally by forty-two percent (-42%).

Eighty-four percent (84%) of participants responded with complete or partial agreement compared to the pre-test. Thirty-four percent (34%) strongly agree, thirty-two percent (32%) moderately agree and thirteen percent (13%) mildly agree. The number of responses left blank decreased by five percent (-5%) from eighteen (18%) to thirteen percent (13%) or five (5) respondents. The neutral and blank responses account for eighteen percent (18%) of the responses.

The T-Test supports there is a level of significance of ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content attribute on “just the right length”. The mean of the post-test is reflective of the agreement to the statement indicating a desired preference in ISA content format. This clustering of the data suggests the Action Research workshop did have an impact on the participants’ desired preference in ISA content. My interpretation is that during the initial evaluation of the ISA content format the participants experience prior to the workshop was limited. Once they experienced an awareness session, they were able to opine on the attributes of the content format. After the workshop the participants know what attributes to look for, the participants had new knowledge to consider for future learning.

In item 3f, the ease to find ISA content is analyzed as part of the preferred format for receiving awareness information in the future. In the pre-test twenty-six percent (26%) responded with complete or partial disagreement compared to three percent (3%) in the post-test, representing a twenty-three percent (-23%) decrease on the level of disagreement. Another noticeable different is the decrease of Agree and Disagree Equally by forty percent (-40%).

Eighty-four percent (84%) of participants responded with complete or partial agreement compared to the pre-test. Fifty percent (50%) strongly agree, twenty-nine percent (29%) moderately agree and five percent (5%) mildly agree. The number of responses left blank decreased by ten percent (-10%) from eighteen (18%) to eight percent (8%) or three (3) respondents. The neutral and blank responses account for thirteen percent (13%) of the responses.

The T-Test supports there is a level of significance of ($p < 0.05$) between the pre-test and post-test responses preferred on the ISA content that is “easy to find”. The clustering of the post-test data (mean=6.2), suggests the Action Research workshop had an impact on the participants’ desired preference in ISA content. The data suggest that during the initial evaluation of the ISA content format the participants experience prior to the workshop was limited. Once they experienced an awareness session, they were able to opine on the attributes of the content format. After the workshop the participants know what attributes to look for, the participants had new knowledge to consider for future learning.

Items 4a through 4d measured the workshop effect on the participants’ motivation to engage in ISA advocacy after the ISA presentation. The table 4.8 summarizes the instrument items 4a through 4d, including the participants’ responses affecting the motivation to engage in *advocacy behavior.*

Table 4.8: Summary of Motivation Related Questions (N=38)

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
4a	Motivation to Engage in ISA Advocacy	The ISA presentation did not affect my motivation or engagement ISA advocacy.	2.17	79% (13,12,5)			13% (2,3)	8% (2,1,0)		
4b	Motivation to Engage in ISA Advocacy	The ISA presentation motivated me to begin engaging in ISA advocacy.	5.68	0% (0,0,0)			18% (3,4)	82% (11,13,7)		
4c	Motivation to Engage in ISA Advocacy	ISA presentation motivated me to increase my engagement in ISA advocacy.	5.51	3% (1,0,0)			16% (3,3)	81% (14,9,8)		
4d	Motivation to Engage in ISA Advocacy	The ISA presentation motivated me to continue in my current high level of engagement in ISA advocacy.	4.65	8% (0,1,2)			50% (16,3)	42% (10,1,5)		

Item	Descriptive Statistics or Inference
4a	The mean (2.1) is reflective of disagreement to the statement suggesting positive effect on motivation or engagement to ISA advocacy.
4b	The mean (5.6) is reflective of the agreement to the statement suggesting a positive effect on motivation or engagement in favor of ISA advocacy.
4c	The mean (5.5) is reflective of the agreement to the statement suggesting a positive effect on motivation or engagement in favor of ISA advocacy.
4d	The mean (4.6) is reflective of neutrality suggesting a neutral or unchanged effect on motivation or engagement in favor of ISA advocacy.

Item 4a surveys the participants on the effect of the ISA presentation had on their motivation or *advocacy behavior* engagement. The question measures the immediate results after the workshop. When asked, *The ISA presentation did not affect my motivation or engagement ISA advocacy*, the majority of the respondents disagreed. The arithmetic mean for the responses to the post-test is 2.1, which is reflective of disagreement to the statement. The clustering of the data suggests disagreement to the statement indicating an effect on *motivation or advocacy behavior* engagement.

Seventy-nine percent (79%) of participants responded with complete or partial disagreement. Thirty-four percent (34%) strongly disagree, thirty-two percent (32%) moderately disagree, and thirteen percent (13%) mildly disagree. Five percent (5%) of the respondents Agree and Disagree Equally.

Eight percent (8%) of participants agreed completely or partially. No participants strongly agreed, but three percent (3%) moderately agreed and five percent (5%) mildly disagreed. Eight percent (8%) of the respondents left the question unanswered. The neutral and blank responses account for thirteen percent (13%) of the responses.

In item 4b, *The ISA presentation motivated me to begin engaging in ISA advocacy;* no participants responded with complete or partial disagreement. Eight percent (8%) of the respondents Agree and Disagree Equally. Eighty-two percent (82%) of participants were of complete or partial agreement. Eighteen percent (18%) strongly agree, thirty-four percent (34%) moderately agree and twenty-nine percent (29%) mildly disagree. Eleven percent (11%) of the respondents left the question unanswered. Four respondents or ten percent (10%) left the questions unanswered. The neutral and blank responses account for eighteen percent (18%) of the responses.

The survey Likert scale values were from one (1) to seven (7), one meaning strongly disagrees and seven meaning strongly agree. The arithmetic mean for the responses to the post-test is 5.6. The mean is reflective of the agreement to the statement indicating a positive effect on *motivation or advocacy behavior* engagement.

In item 4c, *the ISA presentation motivated me to increase my engagement in ISA advocacy*. Three percent (3%) of the participants responded with complete or partial disagreement. Three percent (3%) strongly disagree, but no participants moderately disagree or mildly disagree. Eight percent (8%) of the respondents Agree and Disagree Equally.

Eighty-one percent (81%) responded in agreement, of which twenty-one percent (21%) strongly agree, twenty-four percent (24%) moderately agree and thirty-seven percent (37%) mildly disagree. Eight percent (8%) of the respondents left the question unanswered. The neutral and blank responses account for sixteen percent (16%) of the responses.

The mean (5.1) is reflective of the agreement to the statement indicating *a positive effect on motivation or engagement in favor of ISA advocacy*.

In item 4d, *the ISA presentation motivated me to continue in my current high level of engagement in ISA advocacy*. Eight percent (8%) of the participants responded with complete or partial disagreement. No participants strongly disagree, but three percent (3%) moderately disagree and five percent (5%) mildly disagree. Forty-two percent (42%) of the respondents Agree and Disagree Equally.

Thirteen percent (13%) strongly agree, three percent (3%) moderately agree and twenty-six percent (26%) mildly disagree. Eight percent (8%) of the respondents left the question unanswered. The neutral and blank responses account for fifty percent (50%) of the responses.

The arithmetic mean for the responses to the post-test is 4.6. The mean is reflective of neutrality to the statement indicating *a neutral effect on motivation or engagement in favor of ISA advocacy*. This clustering of the data suggests the Action Research workshop had *a neutral effect on motivation or advocacy behavior engagement.* The data also suggest no change, which could mean the participants may have not previously considered their engagement in ISA advocacy as high.

In item 5, the participants were asked to *describe [*their*] desired comfort level related to information security knowledge*. The participants shared the following comfort levels for learning influencing the variable *awareness knowledge*.

3%	are already constantly learning about topics related to information security.
45%	need more training; they know only what is applicable to my immediate work environment.
55%	need to learn more, they don't know much about information security.

Only three percent (3%) responded with a self-assessment reflective of constant learning. Forty-five percent (45%) respondents need more training, as they only know what is applicable to their immediate work. Fifty-five percent (55%) need to learn more, as they don't know much about information security.

One respondent contributed the following comment when asked to elaborate on your desired comfort level related to information security knowledge. This supports action research is an effective tool to drive action driven change and improvements in practice.

"I have my head in the sand. I need to wake up."

The question post-test Q5 has similarities and differences to the pre-test question 10. They are similar in that they both refer to the comfort level related to Information Security learning. The difference between the pre-test Q10 and post-test Q5 responses is in that the pre-test statement measures responses using Likert scales, while the post-test statement measures responses using multiple choice. For the analysis, I counted the selections from the post-test multiple choice and compared to the number of responses that agree or disagree with the corresponding portion of the pre-test questionnaire.

While they questions are not a one for one match, the data contributes to a deeper understanding of the participants level of knowledge. The table 4.9 lists the questions and responses evaluated for this purpose.

Table 4.9: Similarities Between Comfort Level Assessments

Pre-Test Question 10	Post-Test Question 5
Pre-Test Q10a – Likert Scales I am comfortable and fluent with topics related to information security	Post-Test Q5a – Multiple Choice I am already constantly learning about topics related to information security
15 respondents expressed agreement.	3 respondents selected this choice
Pre-Test Q10b – Likert Scales I know only what is applicable to my immediate work environment.	Post-Test Q5b – Multiple Choice I need more training; I know only what is applicable to my immediate work environment.
17 respondents expressed agreement.	17 respondents selected this choice
Pre-Test Q10c – Likert Scales I need to learn more about information security.	Post-Test Q5c – Multiple Choice I need to learn more, I don’t know much about information security.
30 respondents expressed agreement	21 respondents selected this choice

Comfort level assessment similarities between the pre-test Q10a – post-test Q5a:

While in the pre-test fifteen (15) of the thirty-five (35), respondents expressed agreement with the comfort and fluency with topics of information security. The poste-test shows three (3) of the thirty-five (35) respondents that are already constantly learning about it. Three participants expressed continuous learning even though fifteen (15) respondents express existing comfort and fluency with topics of information security. These responses suggest there is a gap in continuous learning information security topics.

Comfort level assessment similarities between the pre-test Q10b– post-test Q5b:

While in the pre-test seventeen (17) of the thirty-four (34) respondents expressed they know only what is applicable to the immediate work environment. The post-test show seventeen (17) or the thirty-four (34) respondents expressed the need for more training, as they only know what is applicable to their immediate work environment. There is no change with the participants identifying with the need for more training beyond the knowledge that is applicable to their immediate work environment.

Comfort level assessment similarities between the pre-test Q10c– post-test Q5c:

In the pre-test, fifteen (15) of the thirty-five (35) respondents expressed agreement with the need to learn more about information security. The poste-test, however, shows twenty-one (21) of the thirty-five (35) respondents identified with the need to learn more, [as they] do not know much about information security. The post-test statement is not associated with the knowledge related to the work environment; it is open ended to all information security knowledge. More participants expressed the need to learn more during the pre-test than the post-test.

Item 6 is based on the *commitment* to action; the participants were asked to list two (2) to five (5) Information Security advocacy activities that [they] planned to engage in during the coming days or weeks. The following are the information security topics expressed in the post-test questionnaire grouped by major topics like email, credit card, passwords, sharing ISA, learning ISA, online account management, general information management, and general preventive activities. Although the participants were asked for advocacy experiences, they included activities that are security best practices. This suggests the participants are not clear about the differences between learning activities and advocacy activities. The data also suggest an increase in learning, as many of the responses were topics discussed during the workshop. The advocacy experiences contribute to action driven changes that can improve in the practice of information security advocacy.

- Encourage leaders to do ISA presentations in their town halls.
- Encourage the team to learn more, and think about their awareness.
- Find better connected with our IT team
- Share ISA with staff, peers and friends
- Share best practices with staff
- Email ISA articles to team

In item 7, the participants shared their level of agreement with experiences they need to overcome in order to accomplish their committed activities. They were presented a list of activities, item 7a through 7e, to which they described how much they agreed or disagreed with the experiences using a Likert scale. The table 4.10 is a summary of advocacy challenges to overcome followed by the narrative of the data interpretation.

Table 4.10: Summary of Advocacy Challenges to Overcome (N=38)

Item	Construct	Question	Arithmetic Mean	Strongly Disagree	Moderately Disagree	Mildly Disagree	Agree and Disagree Equally	Mildly Agree	Moderately Agree	Strongly Agree
				(1)	(2)	(3)	(4)	(5)	(6)	(7)
7a	Challenge and Advocacy Behavior	Find opportunities to advocate for information security awareness.	5	9% (1,1,1)			31% (8,4)	60% (11,7,5)		
7b	Challenge and Advocacy Behavior	Get involved as an ISA advocate, just do it!	5.1	3% (0,0,1)			36% (10,4)	61% (10,9,4)		
7c	Challenge and Advocacy Behavior	Subscribe to ISA material source and consistently share it with my employees.	4.9	9 % (1,1,1)			36% (10,4)	55% (7,10,4)		
7d	Challenge and Advocacy Behavior	Obtain the resources available to contribute to ISA advocacy.	4.9	6% (1,1,0)			42% (12,4)	52% (7,8,5)		
7e	Challenge and Advocacy Behavior	Dedicate some time to contribute to ISA advocacy.	5.4	3% (0,1,0)			21% (5,3)	76% (13,10,6)		

Item	Descriptive Statistics or Inference
7a	The mean (5) is reflective of the agreement to the statement suggesting a positive effect to finding opportunities to advocate for information security awareness. The data suggest support for action driven change in favor of ISA advocacy.
7b	The mean (5.14) is reflective of the agreement to the statement indicating a positive effect on the need to get involved as an ISA advocate.
7c	The mean (4.97) is reflective of the agreement to the statement indicating a neutral effect to subscribe to ISA material source and consistently share it with their employees. The neutral effect means for some participants, their need to subscribe to ISA material source and consistently share it with employees remains unchanged.
7d	The mean (4.97) is reflective of the agreement to the statement indicating a neutral to positive effect to obtain the resources available to contribute to ISA advocacy.
7e	The mean is reflective of the agreement to the statement indicating a positive effect to dedicate some time to contribute to ISA advocacy.

Interpretation for item 7a: Find opportunities to advocate for information security awareness.

Most participants agreed to the need to overcome the challenge of finding opportunities to advocate for information security awareness. Nine percent (9%) of the participants responded with complete or partial disagreement. Three percent (3%) strongly disagree, three percent (3%) moderately disagree, and three percent (3%) mildly disagree. Twenty-one percent (21%) of the respondents Agree and Disagree Equally. Thirteen percent (13%) strongly agree, eighteen percent (18%) moderately agree and twenty-nine percent (29%) mildly disagree. Ten percent (10%) of the respondents left the question unanswered. The neutral and blank responses account for twenty-one percent (21%) of the responses.

The arithmetic mean for the responses to the post-test is 5.0. The mean is reflective of the agreement to the statement indicating a positive effect to finding opportunities to advocate for information security awareness. The data suggest support for action driven change in favor of ISA advocacy.

Interpretation for item 7b: Get involved as an ISA advocate; just do it!

Most participants are neutral or agree they need to get involved as an ISA advocate. Three percent (3%) of the participants responded with complete or partial disagreement. None of the participants strongly or moderately disagrees and three percent (3%) mildly disagree. Twenty-six percent (26%) of the respondents Agree and Disagree Equally. Eleven percent (11%) strongly agrees, twenty-four percent (24%) moderately agree and twenty-six percent (26%) mildly agree. Ten percent (10%) of the respondents left the question unanswered. The neutral and blank responses account for thirty-six percent (36%) of the responses. The arithmetic mean for the responses to the post-test is 5.14. The mean is reflective of the agreement to the statement indicating a positive effect on the need to get involved as an ISA advocate.

Interpretation for item 7c: Subscribe to ISA material source and consistently share it with my employees.

Most participants agree they need to subscribe to ISA material source and consistently share it with my employees. Nine percent (9%) of the participants responded with complete or partial disagreement. Three percent (3%) of the participants strongly disagree, three percent (3%) moderately disagree, and three percent (3%) mildly disagree. Twenty-six percent (26%) of the respondents Agree and Disagree Equally. Eleven percent (11%) strongly agrees, twenty-six percent (26%) moderately agree and eighteen percent (18%) mildly disagree. Ten percent (10%) of the respondents left the question unanswered. The neutral and blank responses account for thirty-six percent (36%) of the responses.

The arithmetic mean for the responses to the post-test is 4.9. The mean is reflective of the agreement to the statement indicating a neutral to positive effect to subscribe to ISA material source and consistently share it with their employees. The neutral to positive effect means for some participants, their need to subscribe to ISA material source and consistently share it with employees remains unchanged.

Interpretation for item 7d: Obtain the resources available to contribute to ISA advocacy.

Most participants agree they need to overcome the challenge to obtain the resources available to contribute to ISA advocacy. Six percent (6%) of the participants responded with complete or partial disagreement. Three percent (3%) of the participants strongly disagree, three percent (3%) moderately disagree, and none of the participants mildly disagrees. Thirty-two percent (32%) of the respondents Agree and Disagree Equally. Fifty-two percent (52%) responded with agreement, of which, thirteen percent (13%) strongly agree, twenty-one percent (21%) moderately agree and eighteen percent (18%) mildly disagree. Ten percent (10%) of the respondents left the question unanswered. The neutral and blank responses account for forty-two percent (42%) of the responses.

The arithmetic mean for the responses to the post-test is 4.9. The mean is reflective of the agreement to the statement indicating a neutral to positive effect to obtain the resources available to contribute to ISA advocacy. For thirty-two percent (32%) of the participant, the behavior of obtaining the resources available to contribute to ISA advocacy remains unchanged while for fifty-two percent (52%) of the participant there is a positive effect towards action driven change to improve the practice of information security awareness advocacy.

Interpretation for item 7e: *Dedicate some time to contribute to ISA advocacy*.

Most participants agree they need to overcome the challenge to dedicate some time to contribute to ISA advocacy. Three percent (3%) of the participants responded with complete or partial disagreement. None of the participants strongly disagrees, three percent (3%) moderately disagree, and none of the participants mildly disagrees. Thirteen percent (13%) of the respondents Agree and Disagree Equally. Seventy-six percent (76%) responded with agreement, of which, sixteen percent (16%) strongly agree, twenty-six percent (26%) moderately agree and thirty-four (34%) mildly disagree. Eight percent (8%) of the respondents left the question unanswered. The neutral and blank responses account for twenty-one percent (21%) of the responses.

The arithmetic mean for the responses to the post-test is 5.4. The mean is reflective of the agreement to the statement indicating a positive effect to dedicate some time to contribute to ISA advocacy.

In item 8, the participants were asked to describe their ISA advocacy planned behaviors for the next few weeks. The participants selection show an increase on ISA advocacy planned behaviors, suggesting increase in learning about *advocacy behaviors* which could have a positive effect to drive action driven change in the practice of advocating for information security.

39% will forward an ISA informational bulletin to my employees or peers.
16% will announce in their staff meeting an ISA event or presentation and encouraged attendance.
11% will invite the information security department to present ISA in my all hands meeting or departmental meetings.
42% will share an ISA news article read or found on the Internet.
42% will forward an email update with their comments regarding an industry incident.
3% will talk about policies or regulations with my staff or peers.

In table 4.11, I compared to the pre-test where the participants were asked about existing activities, the post-test questionnaire asked about desired behavior. The differences mark new knowledge in *advocacy behaviors* learned during the workshop that the participants could accomplish. The post-test responses show an increase in most of the *advocacy behaviors* include noticeable increases except for talking about policies or regulations with staff members. The data suggest an increase in learning about *advocacy behaviors*, which could have a positive effect to drive action driven change in the practice of advocating for information security.

Table 4.11: Comparisons of Advocacy Behavior Assessments

Advocacy Behavior	Pre-Test Item 12 % responses	Post-Test Item 8 % responses
Forward an ISA informational bulletin to my employees or peers.	8%	39%
Announce in my staff meeting an ISA event or presentation and encouraged attendance.	5%	16%
Invite the information security department to present ISA in my all hands meeting or departmental meetings.	0%	11%
Share an ISA news article I read or found on the Internet.	16%	42%
Forward an email update with my comments regarding an industry incident.	11%	42%
Talk about policies or regulations with my staff or peers.	18%	3%

Item 9, describes new learning about security concerns and the need for information security awareness and advocacy. The participants shared their perspectives on their *current comfort level related to learning.* Of the twelve (12) current learning contributions, I categorized the comments into four groups.

- Best practices to manage digital footprints.
- Online threat awareness
- The value of ISA advocacy
- General appreciation of ISA

These contributions supports action research is an effective approach to increase learning.

The Follow-up Email Analysis

The data analysis approach for the email follow-up was to evaluate the responses with the content analysis procedures described in chapter 3. For each organization, I sent the email follow-up three (3) weeks after the workshop and repeated the procedure again six (6) weeks after the workshop. The intention in this step in the design is to determine behavioral changes and knowledge retention resulting from the Action Research workshop lessons learned. The data is qualitative, presented as an email response with a list of advocacy activities, and secure behavior best practices. From the data, I evaluate the residual knowledge and awareness retention; data on behavior changes in relation to *commitment*. The response rate was is generally low. Of the population (N=38) the response rates are identified by workshops, time interval, and gender in table 4.12.

Table 4.12: Email Respondents by Workshop, Time Interval and Gender

Workshop site code	Response rate - 3 week Follow-up	Male	Female	Response rate – 6 week Follow-up	Male	Female
Workshop 1CC	0 respondents	0	0	1 respondent	0	1
Workshop SL1	0 respondents	0	0	3 respondents	2	1
Workshop PR1	0 respondents	0	0	0 respondents	0	0
Workshop SL2	12 respondents	9	3	3 respondents	0	3

I received twelve (12) email responses from the three (3) weeks email request and seven (7) responses from the six (6) weeks email request. A total of nine (9) males and three (3) females responded to the three (3) weeks email follow-up compared to the latter where only two (2) males and five (5) females replied to the email request. That is a thirty-one percent (31.5 %) response rate for the three (3) week email request and an eighteen percent (18.4%) response rate for the six (6) week email request, showing a response rate drop of thirteen percent (-13.1%).

The first question asked the participants for a recount of advocacy activities they engaged in since the workshop: *Based on the commitment to the action exercise, please list at two to five Information Security advocacy activities that YOU have engage in the last few weeks*. The responses included specific instances of shared ISA advocacy with peers, employees, family members, and friends. The experience included shared guidance on security best practices and shared information security awareness similar to the workshop presentation. Furthermore, the recount of activities included personal behavioral changes in topics we discussed at the workshop. These responses suggest the Action Research workshop had a positive effect on improvements is learning and improvements in practice. Below are the coded responses to the emails received during the email inquiry.

These are the grouped responses received from the three (3) week email follow-up.

Advocacy Activities:

- “Shared ISA presentation from the workshop with peers”.
- ” Spoke to direct reports about the security best practices” (2).
- “Spoke to parents and friends about the different examples to protect personal information”.
- “I have not engaged in any ISA activities”.

Improvements in best practices:

- Changes in password management
- Changes in online account management

- Changes in email account management
- Changes in information management.

These are the grouped responses received from the six (6) week email follow-up.

Advocacy Activities:

- “Spoke to family members about best practices on password management”.
- “Informed my parents about the risk of clicking on videos.”
- “Informed all my family about the risk of disclosing personal information on their e-mail”.
- “Talked to my daughter-in-law about information disclosed in social media”.
- “Discussed with family and friends about online account management”.
- “Talked about strategy of using different passwords for different activities with my wife”.
- “Reviewed with my daughter’s a social media strategy to increase privacy”.
- “I have not engaged in any ISA activities”.

Best Practices:

- Read about information security on company intranet.
- Online purchases behavioral changes three (3).
- Install virus scan software for my personal computer.
- Changes in password management (5).
- Changes in email management.
- Created a strategy for storage of multiple set of credentials (2).
- Changes in online account management (2).
- Changes in information management (3).
- I changed the product defaults settings on my wireless router at home.

The second question on the email follow-up was a multiple-choice question: *Describe any new or continued approaches since the ISA workshop to learning about information security* *awareness (ISA).* This question had the respondents differentiate if the learning approach was new or a continued behavior. The table 4.13 list the summary of learning approaches received.

Table 4.13: Summary of Learning Approaches.

New	Continued	3 weeks	6 weeks	Approaches to learning about ISA since the workshop
3	5	3	5	I search for bulletins published on the company intranet.
1	1	1	1	I currently attend ISA presentations and events.
				I watch company-posted webinars and videos.
5		2	3	I sign up for information security awareness e-mails.
2	4	3	3	I ask my local information security officers for more information.
2	3	2	3	I ask my peers or colleagues about ISA.
3	6	2	7	I learn about ISA independently from external resources like the Internet.

The data suggests improvements in practice by the participants who have adopted new approaches in leaning since the workshop. Most choices had instances of adopting a new approach. The most noticeable improvement in a learning approach was signing up for information security awareness emails. This suggests the participants learned of a new source for ISA learning.

Most choices also had continued learning behaviors, except for *I sign up for security awareness emails.* This suggests the participants knew about most learning approaches choices. The lack of respondents watching company posted webinar suggest there are no videos or webinars available at the particular organizations. I asked the participants to expand on their selections with comments, the following are examples provided:

"I looked on-line for information about ISA. The intent was to familiarize myself in ways in which security breaches have been done in the past. And get tips on how to prevent such occurrences in the future."

"I get on the internet and read information on Security Awareness. This is something that even though I have been doing this before, I think I started to do it a little more than before."

"I was speaking with my husband about the password he had setup for viewing his online banking and viewing any other internet site, to make sure there is some complexity by using some characters and numbers. "

"I had a short discussion with some people on the storage of passwords and not choosing a password because it is easy to remember, because it would be easy for hackers to get into."

"Downloaded all passwords on a thumb drive & put into my safe @ home."

Both email follow ups generated similar advocacy experiences and changes in best practice behavior. ISA advocacy was shared with peers, employees, family, and friends. The ISA advocacy topics shared were subjects discussed in the workshops. The best practice behaviors recounted were also topics discussed in the workshops. This supports action research is an effective tool to increase learning and motivate improvement in the security best practices as well as the practice of advocating for ISA.

Data Interpretation Sections by Construct

Section 1: Awareness Knowledge

I searched the data analysis for evidence supporting the variable *awareness knowledge* in the working proposition 1: Rich feedback on self-reflective levels of knowledge in information security awareness indicates managers are sufficiently exposed to ISA content. **The analysis of the data measuring awareness knowledge includes the findings listed in table 4.14.**

Table 4.14: Data Analysis Findings for *Awareness Knowledge*

Instrument Analysis	Data Analyzed	Awareness Knowledge	Supporting Literature
Pre-Test Questionnaire	List instrument items measuring *awareness knowledge*	See descriptive statistics summary below	Leach 2003
Content Analysis of the ISA Presentation Recording	Coded recordings generated data supporting level of *awareness knowledge*	High Level Neutral Level Low Level	Dutta & Roy, 2008
Action Research Action Exercise	Group responses to ARAE questions	Reflections of improvements in learning	Katsikas (2000)
Post-Test Questionnaire	List instrument items measuring *awareness knowledge*	See descriptive and inferential statistics summary below	McNiff and Whitehead (2006)
Email Follow-up	New or continued approaches to learning	Improvements in learning and improvements of best practices	McNiff and Whitehead (2006)

Pre-Test Questionnaire

The pre-test questionnaire items in the table 4:14, Items Measuring *Awareness Knowledge*, below yielded a self-assessed state of *awareness knowledge*, learning format preferences, and comfort level in learning ISA prior to the Action Research workshop. The measurement was taken to show the participants point of view on ISA knowledge before being exposed to an information security awareness presentation.

Prior to the workshop the participants disagreed with having a high level of *awareness knowledge* (mean=3.92). The scores representing the preference in content learning formats consistently represented disagreement with means between 3.47 and 3.96. These suggest that prior to the workshop participants had not considered the different content formats available as it relates to their learning preferences.

Table 4.15: Items Measuring Awareness Knowledge

Item	Construct	Question	Mean
7	Awareness Knowledge	I have a high awareness level of Information Security.	3.92
9a.	Preferred learning format	The ISA content provided is in a language easy to understand.	3.47
9b.	Preferred learning format	The VIDEO ISA content provided is in the learning format I prefer.	3.77
9c.	Preferred learning format	The TEXT ISA content provided is in the learning format I prefer.	3.86
9d.	Preferred learning format	The POWERPOINT presentation ISA content provided is in the learning format I prefer.	3.96
9e.	Preferred learning format	The ISA content provided is just right in length.	3.77
9f.	Preferred learning format	The ISA content provided is easy to find.	3.61
10a	Learning comfort level	I am comfortable and fluent with topics related to information security.	3.82
10b	Learning comfort level	I only know what is applicable to my work environment.	4.14
10c	Learning comfort level	I need to learn more about information security.	5.91

Scores representing their self-assessed learning comfort level reflected disagreement on the present state of comfort with topics related to information security in general (mean 3.82). When the comfort level self-reflection was directed to their specific work environment, the participants were neutral (mean=4.14). The participants agreed in the need to learn more about information security (mean=5.91). The data suggest that prior to the Action Research workshop the participants recounted not having a high level of *awareness knowledge*, discomfort in the topics of information security and expressed the need to learn more.

When asked about the learning sources for ISA, in pre-test Question 8, participants described existing practices indicative of reliance on peers and colleagues as a common source for ISA with fifty-eight percent (58%). Still, there is evidence participants knew about sources to find information. The most common sources of ISA were from on their company's Intranet, twenty-one percent (21%), and in email notifications, thirty-four percent (34%), that they received. The least common learning sources were ISA events and presentations with five percent (5%) and webinars or videos with eleven percent (11%) of the responses. To my surprise, only fifteen percent (15%) reached out to their local information security offices when they needed information while thirteen percent (13%) researched independently from external resources like the Internet. Furthermore, thirty-four percent (34%) were not aware of the resources available to learn about ISA. The data from pre-test item 8 again suggest the participants of this study are insufficiently exposed to information security awareness content prior to the Action Research workshop.

Leach (2003) addresses factors affecting employee security behaviors, the importance of information security awareness, and organizational recommendations to improve the security posture. The data yielded consistently lower scores than neutral for self-evaluation regarding their state of *awareness knowledge*, learning format preferences, and comfort level in learning ISA prior to the Action Research workshop. According to Leach, *the user experience* and *what they see* (Leach, 2003, p. 686) are two factors affecting end-user decisions on acceptable and unacceptable behavior. The Pre-test questionnaire responses to their ISA learning preferences and existing knowledge supports these factors and suggest the managers are not sufficiently exposed to information security awareness content. Table 4.16 shows the characteristics supportive of the literature.

Table 4.16: Characteristics Supporting Leach (2003)

Key Themes from the Literature	Level of Awareness Knowledge	Finding
Leach 2003 suggests developing the user's knowledge in security will aid in the development of a security aware work force, which will support better secure behavior decision making.	My study data findings yielded consistently lower scores than neutral for self-evaluation regarding their state of *awareness knowledge*, learning format preferences, and comfort level in learning ISA prior to the Action Research workshop.	The lower and neutral scores on *awareness knowledge* are indicative of the need for more ISA exposure.

Content Analysis of the ISA Presentation Recording

The content analysis yielded findings under the level of awareness category. There were twenty-five (25) participant expressions analyzed from the recording transcriptions, of which ten (10), representing were contributions to sharing knowledge about security awareness.

Each contribution was coded into one of three (3) levels of *awareness knowledge*: low, neutral and high. Of the group feedback, six (6) comments provided accurate guidance in security behavior best practices. Accurate feedback suggests a high level of *awareness* *knowledge* compared to the peer participants, represented by twenty-four percent (24%) of the twenty-five (25) total comments. The (4) four comments that only provided partial information or those comments that benefitted from a discussion for clarification were coded as neutral level of *awareness knowledge*, represented by sixteen percent (16%). The remaining sixteen (16) comments were inquiries soliciting guidance to a best practice or the use of a product or tool, suggesting a low level of *awareness knowledge* with sixty percent (60%) compared to their peer participants. The table 4.17 lists the findings for the level of knowledge codes as they relate to the artifact presentation recordings.

Table 4.17: Codes from the Transcribed Data Recordings

Categories	Codes	Definitions	Response Percent (N=25)	Findings
Level of Awareness Knowledge	High level of awareness knowledge	Expressions describing a high level of awareness knowledge.	24%	*Engaged Participation* *Peer expresses their disbelief* *Use humor to validate the point* *Protection from incidents by using a credit card for purchase* *Shares Guidance* *Recollection of memory,*
	Neutral level of awareness knowledge	Expressions describing a neutral or adequate level of awareness knowledge.	16%	*Assumptions about behaviors* *Recalls a security concern* *Relate workshop to recent incident* *Trying to understand the incident at a deeper level*

	Low level of awareness knowledge	Expressions describing a low level of awareness knowledge.	60%	*Seeks Guidance* *False sense of safety based on popularity or size of a retailer* *Reaction to severity of the problem*

The following table (4.18) shows the characteristics specific to the content analysis of the ISA presentation recordings as they relate to the level of *awareness knowledge*.

Table 4.18: Characteristics specific to the analysis of the ISA Presentation

Key Themes from the Literature	Level of Awareness Knowledge	Finding
Exposing the end users to security incidents raises the awareness to the need for security knowledge. In contrast, the lack of ISA can lead to a security dismissive attitude that has the potential to lead to security breaches. Dutta and Roy (2008)	My data findings included high or rich ISA feedback is an indication that some managers are sufficiently exposed to ISA content.	Some participants demonstrated knowledge of ISA by contributing rich feedback to the ISA presentation.
	Neutral or Partial understanding of risk is not reflective or an indication that managers are sufficiently exposed to ISA content.	Some participants demonstrated partial knowledge of ISA by recounting experiences that indicated a partial understanding of ISA.
	Low understanding of ISA indicates managers are not sufficiently exposed to ISA content.	During the ISA presentation, some mangers expressed a lack of understanding of the topics discussed.

The findings from the content analysis (Table 4.18: Characteristics specific to Content Analysis of the ISA Presentation Recording and Level of *Awareness Knowledge*) suggest the participants of this study were insufficiently exposed to information security awareness content.

This finding raises a concern, as well as presents an opportunity for organizations, as Dutta and Roy (2008) found that more user exposure to awareness and training increases their ability to understand risk and the value of data and information security transactions.

Action Research Action Exercise

During the action research action exercise, data was gathered through a group discussion exchanging ideas on reasons, activities, benefits, and *challenges* to advocate for ISA. Question 3 of the action research exercise explores advocacy activities and advocacy best practices. Among the responses were secure behaviors the groups presently engaged that are not ISA advocacy activities. Similarly, during the action research individual *commitments* to ISA advocacy, respondents committed to a mix of advocacy activities and security best practices.

The recounts of secure behaviors suggest the respondents were expressing *awareness knowledge* from the perspective of security best practices and not from an ISA advocacy point of view. The group responded with foundational security best practices including password management, email management, online accounts management, and best practices regarding online shopping. The data suggest the managers had at least a base *awareness knowledge* foundation, supporting Katsikas (2000), see table 4.19, but can benefit from a broader exposure.

Table 4.19: Characteristics Supporting Katsikas (2000)

Key Themes from the Literature	Level of Awareness Knowledge	Finding
Katsikas (2000) found additional manager training is needed in different security domains.	My study data suggest the managers had at least base *awareness knowledge* and need more ISA exposure.	Participants in my study recounted basic best practices activities reflecting base level knowledge. There is a need for more ISA exposure.

Post-Test Questionnaire

The post-test results reflect the immediate impact of the Action Research workshop on *awareness knowledge*, learning format preferences, and comfort level in learning ISA. The descriptive statistics of the responses to questions 1a, 1b and 1c affecting the learning comfort levels are reflective of agreement with means between 5.51 and 6.19. The data supports that participants gained ISA knowledge during the workshop (see Table 4.20). The T-Test comparing the pre-test item 7 and post-test item 1b, level of *awareness knowledge*, supports there is a significant difference in awareness level of Information Security knowledge as a result of attending this workshop. Furthermore, the participants agree that managers should be a part of raising ISA consciousness.

Table 4.20 Summary of Post-Test Results Items 1a through 1c

Item	Construct	Question	Mean
1a	Learning comfort level	My level of ISA knowledge has increased as a result of attending this workshop.	6.19
1b	Learning comfort level	I have a high awareness level of Information Security knowledge as a result of attending this workshop.	5.71
1c	Learning comfort level	In your opinion, should a manager be part of raising ISA consciousness?	5.51

Item	Statistical Inference
1a	The clustering of the data suggests the Action Research workshop had an impact on the participant’s learning of the topic.
1b	The T-Test result (*p*<0.05), supports there is a significant difference in awareness level of Information Security knowledge as a result of attending this workshop.
1c	The clustering of the data suggests the Action Research workshop affected the respondents’ opinions enough to drive change on the practice of raising ISA consciousness as a result of the workshop.

In contrast to pre-test item 8, in post-test item 2 the participants reevaluated the sources of ISA content as a consideration to plan ISA learning. I analyzed the actual and planned learning activities after the workshop. While the dependency on colleagues and peers decreased, *other sources of ISA learning increased*. Given the same list of activities as consideration for learning sources, the activities such as researching ISA independently from external resources like the Internet, searching for bulletins published on the company intranet, attending ISA presentations and events, watching company-posted webinars and videos, and asking local information security officers when they needed information all increased. The data suggest the Action Research workshop expanded their *awareness knowledge* relative to the sources of ISA content available to them.

Similarly, I compared the ISA "content format preferences" between the pre-test items 9a through 9f with the desired preference for future learning in post-test items 3a through 3f. The data suggest the Action Research workshop expanded their awareness of formats in which to find information that is available for them to learn about ISA. Consistently through the comparison, the scores are reflective of agreement about desired formats, with means ranging from 5.08 to 6.29. The attributes of content that is "easy to find" and "the right length" scored the highest, suggesting the participants need ISA content that is hard to find or too long is not helpful. The clustering of the data suggests that the Action Research workshop had an impact on the participants' desired preference in ISA content attributes. Furthermore, the T-Test comparing the means consistently supports there is a significant difference between the pre-test and post-test preferred formats, making desired format a significant attribute to increase *awareness knowledge*.

In post-test item 5, the participants expressed the ISA comfort levels with information security topics by consistently pointing out the need to learn more. Only three percent (3%) responded they are already constantly learning about topics related to information security. In contrast, forty-five percent (45%) responded they need more training, as they know only what is applicable to their immediate work environment, and fifty-five percent (55%) responded they needed to learn more, as they do not know much about information security. The data suggest that more the Action Research workshop increased these managers awareness of how little they knew, but brought about a comfort (familiarity) with the information security topic that will lead to increases in their *awareness knowledge*.

In addition to planned *advocacy behaviors*, the post-test item 6, yielded data related to behaviors in security best practices. The responses suggest some participants integrated their understanding of practices related to security behavior with ISA advocacy. While it was not the intent to confuse ISA advocacy and security best practices, the data did suggest increase learning of *awareness knowledge*, as the responses were reflective of security best practices including email management, password management, online accounts management, and general protection of information. These topics are foundational knowledge for online users to protect their personal information. The data supports action research is an effective tool to increase learning.

Similarly, in post-test item 9, when the participants' recounted what they have learned new about security concerns, the need for information security awareness and advocacy, the responses were reflective of increased learning through the workshop. Among the themes expressed by the respondents was the recognition for security behaviors necessary to manage digital footprints, a grasp on online threat awareness, an increase value of ISA advocacy, and a general appreciation of information security awareness. The data supports action research as an effective tool to increase learning and to improve in practice.

McNiff and Whitehead (2006) describe one of the functions of action research is to improve learning. The post-test data analysis results supports the workshop positively influenced the participants' security learning.

Email Follow-Up

Similar to the action research "action exercise" results, during the email follow up the participants were asked to recount advocacy activities they engaged in both three (3) weeks and six (6) weeks of the workshop. Consistently, respondents continue to include security behaviors when describing their new ISA advocacy experiences. While the responses were not all advocacy experiences, the email follow-ups reflected an increase in information security awareness. The following are the summarized improvements in secure behavior practice, these themes were the topics presented in the workshop, suggesting an increase in *awareness knowledge* from the information learned in the workshop. The improvements in practice responses three and six weeks after the workshop are:

Improvements in best practices:

- Changes in password management
- Changes in online account management
- Changes in email account management
- Changes in information management.

The second question in the email follow up asked the participants about new or continued approaches to learning information security awareness. As mentioned in earlier, the data suggest improvements in practice by the participants who have adopted new approaches in leaning since the workshop. Most choices had instances of adoption of a new approach, the most noticeable improvement being that many participants signed up for information security awareness emails. This suggests the participants learned of a new source for ISA learning resulting from their participation in the Action Research ISA workshop. Most choices also had continued learning behaviors, except for *I sign up for security awareness emails.* This suggests the participants knew about most learning approaches choices. It could also suggest participants found the list an accomplishable and easy path to learning ISA.

Again, the data findings support the action research as a method to improve learning presented by McNiff and Whitehead (2006). The email follow up data analysis supports that the Action Research workshop was an effective tool to improve awareness learning.

Section 2: ISA Advocacy Behavior

I searched the data analysis for evidence supporting the variable *advocacy behavior* in the working proposition 2: *Self-reflection of present advocacy behavior projects positive attitudes and increases motivation to propose and take action toward sharing ISA with employees and peers.* The analysis of the data measuring ISA Advocacy includes the findings in table 4.21.

Table 4.21: Data Analysis Findings for ISA Advocacy

Instrument Analysis	Findings	ISA Advocacy	Literature
Pre-Test Questionnaire	List instrument items measuring ISA advocacy	Experiences advocating for ISA prior to the workshop.	Grojean et al.(2004),
Content analysis of the ISA presentation recording	Recordings generated data supporting ISA Advocacy	Self-reflected and observed behaviors	Desman (2003)

Instrument Analysis	Findings	ISA Advocacy	Literature
Action Research Action Exercise	Advocacy Activities	Experiences advocating for ISA after the ISA presentation.	Grojean et al. (2004) Siponen (2001) McLean (1992) Leach (2003)
Post-Test Questionnaire	List instrument items measuring ISA advocacy	N/A	N/A
Email Follow Up	Post workshop ISA activities	Experiences advocating for ISA after the workshop	Desman (2003)

Pre-Test Questionnaire

The pre-test questionnaire items yielded a self-assessed current state of experience with *advocacy behavior* prior to the Action Research workshop. The measurement was taken to show the participants' point of view and experience with ISA advocacy before being exposed to an information security awareness presentation. On pre-test item 11, participants self-reflected on the opportunities available to advocate, their thoughts towards engaging in advocacy, their experiences advocating, the availability of resources, and time for advocacy. The table 4.22 is the summary of their prior experiences sharing ISA with peers or employees, with the arithmetic means for the participants' self-reflection. In general, the means for the individual questions are indicative of scores representing disagreement and neutrality. Before the Action Research workshop, participants expressed neutrality on "opportunities available" (mean=4.41), "existing experiences sharing ISA" (mean=4.05), and "time available to share" (mean=4.00). Concerning their thoughts about advocating and "having the resources available for advocacy", the participants expressed disagreement trending neutral with means of 3.91 and 3.34 respectively. The data suggest that at the time of the pre-test questionnaire the participants did not recognized what was meant by the term ISA advocacy and did not have enough information to opine on opportunities, resources, existing experiences or time available to engage on the matter. It was reasonable to assume that without knowledge that there is an activity called *advocacy behavior* that the response would be neutral.

Table 4.22: Summary of Experiences Sharing ISA with Peers or Employees

Item	Question	Mean
11a	I don’t have many opportunities to advocate for information security awareness.	4.41
11b	I think I should be involved as an ISA advocate, but have not done it before.	3.91
11c	When I do receive ISA material, I always share it with my employees.	4.05
11d	I have the resources available to contribute to ISA advocacy.	3.34
11e	I don’t have the time available to contribute to ISA advocacy.	4:00

When presented with examples of *advocacy behaviors*, the data suggest that while they recognize familiar activities like forwarding an email, at the time of the pre-test, they did not realize these activities were associated with “advocating for ISA”. When asked to select from a variety of experiences representing ISA *advocacy behaviors* in pre-test Question 12, responses included forwarded bulletins with eight percent (8%), announced event opportunities with five percent (5%), shared articles with sixteen percent (16 %), forwarded an email with eleven percent (11%), talked about policies with eighteen percent (18%), and reminded staff of a best practice with five percent (5 %). Grojean et al. (2004) apply mechanisms used by the different levels of management to channel the priority of ethics. My study extends the use of the mechanisms, and finds the advocacy behaviors in pre-test questions 12 are useful ways of conveying an ISA message, these examples support the “value based leadership” and “setting the example" mechanisms presented by Grojean et al. (2004). The scores indicative of low experiences sharing ISA and the lack of association of activities to ISA advocacy, are reflective of opportunities for improvements in favor of an ISA advocacy climate.

Content Analysis of the ISA Presentation Recording

As the ISA presentation took place, I encouraged the participants to contribute examples of sharing information security awareness. The content analysis yielded findings under the ISA Advocacy category from the coded recordings of the ISA presentation. Self-reflected and observed behaviors included eagerness to share knowledge, recalling stories based on existing experiences, and correcting a peer's false assumption through humor. The self-reflected and observed behaviors in table 4.23 indicate that basic *advocacy behaviors* do happen. The interpretation is that there is opportunity for improvement in practice with guidance and by setting expectations. As the workshop facilitator, I encouraged comments and dialogue on the topic of advocacy behavior. Desman (2003) proposes speaking ISA in a language the audience understands, and setting expectations on taking actions, in this case towards ISA advocacy, is for the benefit of the company. In alignment with Desman guidance, my workshop shared an ISA presentation in a language that was easy to follow and encouraged participation with sharing ISA experiences. The data findings yielded examples of lessons learned from lectures and anecdotal lessons from a past security concern. Although the examples were few in numbers, these examples set the tone of advocacy behaviors for all participants to learn.

Table 4.23: Findings for ISA Advocacy

Category	Code	Definition	Analysis Instrument	Findings
Advocacy Behavior	Advocacy benefits	A manager's perspective on benefits of being an active advocate of ISA.	ARAE Q2	Values leading to behaviors in favor of ISA advocacy. Climates reflective of sharing through peer-to-peer communication. To better understand an online threat. An honest attitude. Effort appreciation.
	Advocacy past activities	Advocacy activities occurring as a past practice.	Relating the artifact to the recordings	Recollection of memory. A story learnt from a lecture. Anecdotal lesson from past security concern.
	Advocacy present activities	Advocacy activities occurring as a current practice.	ARAE Q3	Talk to peers Send securities alerts to the team Obtain informational feeds from industry portals Quarterly newsletter with security tips and best practices Collaborative exchange with industry peers. Have policies for employee to follow.

Action Research Action Exercise

At this point of the workshop progression, participants have completed the pre-test questionnaire and have seen the awareness presentation. The expected outcome was that after the workshop experience they should be able to recognize activities that are reflective of ISA advocacy. During the action research action exercise (ARAE), data gathered through a group discussion included an exchange of ideas on reasons, benefits, and *challenges* to advocate for ISA.

During the ARAEQ2, the workshop data gave me insight on how ISA is done in the different organizations. For those middle managers practicing ISA advocacy, their environment's climate is reflective of sharing through peer-to-peer communication. Manager's share information to keep people informed of best practices, they share to help others protect their personal information, and they share as the company has guided them to do so. These actions suggest there is value for information, understanding of threats, and concern for good company reputation. These personal and organizational values have bearing in the peer-to-peer communication behavior. Although Grojean et al. (2004) were referring to ethics in their study, I am suggesting the use of multiple levels of values that influence ethics in organizational behavior also affects ISA advocacy.

A reason to engage in ISA advocacy was to understand an online threat at a deeper level. Siponen (2001), found in his study the need for all Internet users, even at a personal level, to be aware and understand basic security threats. In my study, the participants identified the same need as a reason to advocate for ISA, supporting Siponen's (2001) study. This acknowledges there is value to understand ISA and it implies that is a reason why people share, promote, or direct the attention of this topic to others.

The question ARAE 3 was an inquiry of present ISA advocacy experiences to engage the participants to recount their advocacy activities. Most workshop participants contributed activities reflective of secure behavior and best practices, not *advocacy behavior*. Their contributions to best practices were reflected under *awareness knowledge*.

A small group of managers contributed ISA advocacy experiences reflective of sharing information listed in table 4.24, Advocacy Experiences. The most common activities among participants were sending secure alerts to the team and having policies to follow. Managers recounted sending security alert emails when they were made aware of the notification, which, according to McLean are "common promotional methods" used to share awareness (1992, p. 186). My study does not leverage the marketing lens to promote ISA but the participants did identify with sharing ISA content through some of the tools identified in McLean (1992).

Managers also shared the ability to talk to peers and employees about policies when they were made available to follow. The data suggest that when managers have been provided with the resources like the email notification and policies, they are able to convey the message to others which is indicative of "value-based leadership" (Grojean et al. 2004), and serves as evidence that contributes to advocacy of information security.

The least common ISA activities came from participants that are managers in regulated environments by standards and government mandates. The data suggest the small number of ISA activities is reflective of the small number of participants that worked in such environments. The data also suggest the experiences described involved an active approach to the obtaining relevant ISA. The participants sought out information security exchanges with other industry peers and signed up to industry feeds like informational portals. These activities are less passive, more involved in the practice of seeking and sharing ISA.

Although participants identified having policies for employees to follow as an experience of advocacy, the comments were part of a discussion where participants acknowledge the existing policies for online shopping were not always followed. This is contrary to the guidance of (Grojean et al., 2004) mechanisms for sending messages to influence employees. Not only are these managers are not always setting an example, but also there seems to be a gap in their organization's ISA culture. Hence, both, setting the example and ensuring security awareness is an ongoing factor in the organization are only partially supported.

Table 4.24: Advocacy Experiences

Advocacy Experiences	Supporting Literature
Talk to peers	(Grojean et al., 2004).
Send securities alerts to the team	McLean 1992
Obtain informational feeds from industry portals	McLean 1992
Quarterly newsletter with security tips and best practices	McLean 1992
Collaborative exchange with industry peers.	Not mentioned in prior literature
Have policies for employee to follow	Grojean et al., (2004) Furnell, Gennatou, & Dowland, (2002)

Post-Test Questionnaire

The Post-Test questionnaire did not include items addressing present advocacy activities. This instrument does not contribute data supporting the variable ISA advocacy.

Email Follow-Up

The email follow up served to measure the longer-term effectiveness of the security awareness advocacy after the workshop. While one respondent did not change their *advocacy behavior*, others did. The responses are supportive of behavioral change in response to setting the expectation for advocacy. Advocacy activities included:

- "Shared ISA presentation from the workshop with peers".

- “Spoke to direct reports about the security best practices”.
- “Spoke to parents and friends about the different examples to protect personal information”.
- “One participant has not engaged in any ISA activities”.

During the workshop, I shared the importance security awareness and encouraged the participants to share ISA. Most of those that responded to the email follow up did take action, supporting (Desman, 2003) guidelines to set the expectations for action, in this case the action of sharing ISA. The actions recounted by the participants in the email follow-ups were reflective of the topics discussed during the workshop. This suggests they understood the content presented importance of security awareness and took action by sharing it with others.

Section 3: Challenges and Constraints

I searched the data analysis for evidence supporting the variable *challenges* and *constraints* in the working proposition 3: *Discovery of organizational and personal attitudes and motivations enabling or hindering ISA advocacy provides the organization with recommendations for changes to increase the ability to practice advocacy behavior*. The analysis of the data measuring *Challenges and Constraints* includes the findings listed in table 4.25.

Table 4.25: Data Analysis Findings for Challenges and Constraints

Instrument Analysis	Findings	Challenges and Constraints	Literature
Pre-Test Questionnaire	List instrument items	Opportunities, lack of time and involvement.	Furnell, Gennatou, & Dowland, (2002)
Content analysis of the ISA presentation recording	Recordings did not generate data supporting challenges.	N/A	N/A
Action Research Action Exercise	ARAE Q2 ARAE Q4 ARAE Q5	Factors dissuading behaviors in favor of ISA advocacy. Challenges identified Overcoming challenges	Siponen (2001) McLean (1992) Furnell, Gennatou, & Dowland, (2002) Leach (2003)
Post-Test Questionnaire	List instrument items	Opportunities, lack of time and involvement.	Furnell, Gennatou, & Dowland, 2002 McLean (1992)
Email Follow Ups	Email responses	N/A	N/A

Pre-Test Questionnaire

The pre-test questionnaire measured through a survey the constructs *awareness knowledge*, *advocacy behavior*, *commitments* and *challenges* prior to experiencing the workshop. The following are the pre-test questions items focusing on identifying *challenges and constraints* affecting a manager's ability or willingness to advocate for ISA. The participants were asked to evaluate the opportunities (item 11a), resource availability (item 11d), and time (item 11e) as a reason for preventing them from ISA advocacy. Table 4.26 lists the detailed questions. Prior to experiencing the ISA workshop, the participants had a neutral self-reflection to the opportunities available to advocate (mean=4.41). The participants disagree with having resources available to advocate (mean=3.34); and they were neutral about having time available to advocate. Furnell, Gennatou, & Dowland (2002) found workload prioritization conflicts, unwillingness, and inability to focus on security factors leading to users' dismissal of risk considerations. In my study, the low scores reflective of opportunities, time, and resources to advocate for ISA support are supportive of Furnell, Gennatou, & Dowland (2002).

Table 4.26: Pre-Test ISA Advocacy Challenges

Item	Question	Mean
11a	I don't have many opportunities to advocate for information security awareness.	4.41
11d	I have the resources available to contribute to ISA advocacy.	3.34
11e	I don't have the time available to contribute to ISA advocacy.	4.00

Content Analysis of the ISA Presentation Recording

As the ISA presentation took place, I encouraged the participants to ask comments and questions. The content analysis did not yield findings under the *Challenges and Constraints* category from the coded recordings of the ISA presentation.

Action Research Action Exercise

The group discussion yielded rich feedback on *challenges and constraints* hindering ISA advocacy. The dialogue seemed the most fruitful method to gain a deeper understanding.

During the ARAEQ2, I found examples of factors that dissuaded ISA advocacy. Unexpectedly, I found honesty a value that dissuaded ISA *advocacy behavior*. The manager shared the perception of having an honest attitude and expecting everyone else to operate with the same credence. Similarly, Loch et al. (1992) reported in their study a finding described as the belief that employees acted in good faith and would not intentionally cause harm to their place of employment. The belief of an honest attitude affected the behavior of sharing ISA through inaction, suggesting the manager was "dismissive of risk" (Furnell, Gennatou & Dowland, 2002, p. 353). The person did not see the threat to security in his environment as a concern because people are honest and do not behave in a negative way.

Similarly, I found appreciation, or the lack of, has an effect of ISA behavior. In this finding, the manager did not share ISA, as he did not feel the effort was appreciated by others. This is an example where the personal value for appreciation influenced the behavior that dissuaded ISA advocacy. The finding supports Grojean et al., (2004, p. 225) "behavior will be shaped by those practices that are encouraged and rewarded by the organization's leaders, giving rise to new norms of behavior." The finding suggests the lack of appreciation for sharing information will not encourage a climate of ISA advocacy.

I also found managers do not have the understanding of security awareness topics; this constraint was identified by Furnell, Gennatou, and Dowland, 2002 as one of the "problems with promoting security awareness" (2002, p. 352). This finding is not saying these managers don't have value for information, understanding of threats, and concern for good company reputation. I am suggesting they just don't have enough exposure to security awareness to understand the value of ISA to influence their behavior to motivate sharing ISA.

During the ARAEQ4, the participants discussed *challenges* and *constraints* that made ISA *advocacy behavior* harder to accomplish. Siponen (2001) equates one of the characteristics of security awareness to health issues. He describes people not acting upon security awareness concerns until there is a problem. I found during the exploration of *challenges* a participant did not want to seem overly concern and that perception kept him from engaging in ISA *advocacy behaviors*. Similar to Siponen's dimension of security awareness where "it seems to be that security awareness may be difficult to internalize properly in the sense that it may be often regarded in the same way as a matter of health; nothing is done as long as nothing goes wrong" (2001, p. 26). The data suggest the participant is not internalizing the need for ISA advocacy, as there seems to be no issue to address.

Other *constraints* to the promotion of security awareness identified by the participants and supported by Furnell, Gennatou, & Dowland, 2002, include the lack of ability or reluctance to prioritizing security concerns, due to other business issues being a higher priority. Similarly, McLean (1992) refers to the prioritization *challenges* as conflicts in stimuli; both supported by my data findings.

Furnell, Gennatou, & Dowland also identifies the constraint of the lack of awareness training, in some cases due to "lack of financial resources" (2002, p. 353). Prioritization conflicts and lack of training *constraints* are reflective of organizational factors that affect mid-level managers from receiving the necessary support for ISA advocacy. These organizational factors also contribute to the difficulties of remaining up to date with security information, contributing to participants having different levels of awareness and knowledge. Both, *constraints* were also identified by the participants as a challenge hindering ISA advocacy. The data suggest the need for continual management support in order for security awareness and advocacy to be an ongoing part of the organizations processes.

Furthermore, with support, managers may find relief to the "difficulties in complying" which according to Leach, is a "factor influence end-user decisions to practice" the expected secure behavior (2003, p. 689). Participants identified other types of factors contributing to the difficulty in compliance, including the complexity of the topic and lack of security *awareness knowledge*. Complexity of the topic relates to security awareness practices that are considered complicated, from the participants point of view, like maintaining too many user credentials. The data suggest that the perception of security awareness as complex and difficult to comply make it harder for participants to practice advocacy.

Knowledge was discussed earlier in this chapter in the section dedicated to the variable *awareness knowledge*. However, a related challenge to *awareness knowledge* was identified as lack of guidance. The participants are not given the proper guidance to practice *advocacy behavior*.

A notable challenge to sharing information security with others is the perception of relevance (Siponen, 2001, p. 28). Participants identified information security advocacy as not relevant to their work. Lack of relevance and guidance are *challenges* that need to be addressed as the data suggest participants' need more guidance to make an informed decision regarding ISA advocacy.

During the ARAEQ5, the participants discussed ways to overcome the *challenges* and *constraints* that made ISA *advocacy behavior* harder to accomplish. A recommended solution towards overcoming *challenges* was identified by the participants, as awareness advocacy expectations should come from the top down. Grojean and colleagues suggests climates are formed as the organizational leadership influences perception. This is an opportunity for the managers to foster organizational climates using their influence in favor of ISA advocacy, assuming the proper expectations are set from the top of the organizational structure.

During the discussions to discover ways to overcome *challenges* to ISA advocacy, a participant suggested sharing the financial cost, indirect impact of a data breach and the social impact against the reputation of the organization would motivate the adoption of ISA advocacy. Similarly, feedback from a different participant suggested the organizations should better explain the policies to include an explanation of the reasons behind it. In other words, in addition to telling what the policy is, also tell why the policy is implemented. This supports introducing or leveraging a behavioral program as a guide to promote adoption of ISA *advocacy behavior*. As participants proposed ways to overcome *challenges*, they mentioned elements that support McLean's (1992) attributes for creating ISA campaigns. Suggestions included, the experienced awareness session during the workshop, leveraging webinars, newsletters, and network messaging to share ISA. These are all examples of a campaign delivery of "instruction, advice, or warning" (p. 188) called campaign "points of delivery messages" (p. 188). Additional elements backing McLean's (1992) attributes for creating campaigns were strong themes, found in the feedback to overcome *challenges* to ISA advocacy. Some examples included a better understanding of the different types of breaches and the promotion of policies. The data supports McLean's (1992) marketing practices to condition middle management to share and support ISA advocacy.

Post-Test Questionnaire

The following are the post-test questions items focusing on identifying *challenges and constraints* affecting a manager's ability or willingness to advocate for ISA. The participants were asked to evaluate the opportunities, thoughts about involvement, need for an information source, resource availability, and time as a challenge they need to overcome in order to advocate for ISA.

In item 7a, most participants agree (mean =5), they need to overcome the challenge of finding opportunities to advocate for information security awareness. For item 7b, the (mean= 5.14) is reflective of the agreement indicating a positive effect on the need to get involved as an

ISA advocate. Item 7c, the (mean=4.97) is reflective of the neutrality indicating no effect to subscribe to ISA material source and consistently share it with their employees. Item 7d, is reflective of the neutrality (mean=4.97), indicating a no effect to obtain the resources available to contribute to ISA advocacy. Item 7e is reflective of agreement with (mean = 5.4), indicating the need to dedicate some time to contribute to ISA advocacy.

In summary, participants agree they need to find opportunities, get involved, and make time for ISA advocacy. Participants were neutral to details such as subscribing to a source of information or resources availability. The data suggest participants gained consciousness about the importance of information security awareness and recognize gaps they need to overcome in order to advocate. As identified earlier in this section, the gaps of lack of time, involvements and opportunities as *constraints* supports prioritization conflicts identified by Furnell, Gennatou, & Dowland (2002), and conflicts of stimuli identified by McLean (1992).

Email Follow-Up

The email follow-ups data analysis was accomplished using content analysis describing the long-term effect to learning, to practice improvement, and as a measurement of the construct *commitment*. This instrument did not contribute ISA advocacy *constraints* and *challenges*.

Section 4: *Commitments*

I searched the data analysis for evidence supporting the variable *commitments* in the working proposition 4: *An Action Research workshop contributes to participants learning, and to improvements to practice through participants contributions to increase ISA advocacy*. The analysis of the data measuring *Commitments* includes the findings listed in table 4.27.

Table 4.27: Data Analysis Findings for *Commitments*

Instrument Analysis	Findings	Commitments	Literature
Pre-Test Questionnaire	List instrument items	N/A	N/A
Content analysis of the ISA presentation recording	Recordings generated data supporting	Reactions to the ISA presentation.	Not matched to the literature
Action Research Action Exercise	ARAE	Individual Commitments to ISA	Grojean et al.(2004), Katsikas (2000), Falkenberg & Herremans, (1995)
Post-Test Questionnaire	List instrument items	Items measuring commitment	Siponen (2001)
Email Follow Up	Advocacy Activities Best Practices	Responses from emails follow up	(McNiff & Whitehead, 2006)

Pre-Test Questionnaire

The pre-test questionnaire measured through a survey the constructs *awareness knowledge*, *advocacy behavior,* and *challenges* prior to experiencing the workshop. The survey did not yield findings under the *commitments* category.

Content Analysis of the Presentation

During the ISA presentation, I found participants expressed reactions that may contribute to motivations towards future *advocacy behavior commitments*. The following are the findings with a brief description.

- The lack of awareness knowledge. There was a moment in the presentation when the participant realized what they did not know.
- Fear based on the lack of knowledge. There was a moment in the presentation when the participant expressed worry because of what they did not know.

- Perceived helplessness. There was a moment in the presentation when the participant expressed resignation to not benefitting from online services because of the existence of threats.
- Validation of trust. There was a moment in the presentation when the participant realized the need for more guidance to manage the information they leave online.

These reactions are evidence some participants recognized and understood the need for knowledge and guidance for action driven change. The Action Research workshop presentation was the catalyst to a realization of need for improvements in practice and additional knowledge. I am not suggesting that at this particular moment, the participants are committed to ISA advocacy but I am suggesting the realization of the importance of information security is a precursor to *commitment* to ISA advocacy.

Action Research Action Exercise

At this point of the workshop progression, participants have completed the pre-test questionnaire and have seen the awareness presentation. During the group discussions, the participants have given reasons to advocate for ISA (AEARQ2), examples of ISA advocacy activities they have participated in (ARAEQ3), identified *constraints* hindering their support for advocacy activities (ARAEQ4) and ways to overcome the limitations (ARAEQ5). The next step in the workshop was to ask for their *commitments* to serve as an ISA advocate. The expected outcome was that after the workshop experience they should understand why ISA and its advocacy are important to them personally and to their organizations. After learning about advocacy activities and considering their limits, the participants should also understand what is being asked of them when this call to action occurs. The call to action is for participants to commit to accomplishable ISA activities that promote, share, and direct the attention of their employees or peers to ISA learning. This part of the exercise was done individually, and then discussed as a group. The expected outcome of the group discussions is that participants can learn from each other through verbal exchange of ideas. The consolidate list of *commitments* from the data analysis chapter shows participants willingness to advocate after the workshop.

Consolidated ISA advocacy *commitment* activities

- “Talk to family about risk of security breach and tips to minimize the risk”
- “Emphasize important of ISA to my employees”
- “Provide tools to emphasize ISA”
- “Promote others to also learn and commit to ISA”
- “Collectively learn more about ISA”
- “Get more connected with IT for ISA updates”
- “To engage in more ISA group activities”
- “Promote company ISA sessions”
- “Share ISA at a personal level”
- “Get presentation from industry related sites”
- “Create Google account for breach news and pass them to employees”
- “Have regular ISA conversations at team meetings”
- “Communicating of best practices and strategies for ISA”
- “Communicate breaches in a clear way”
- “Talk to employees about what we are doing today”
- “More research awareness of threat”

The individual items on the lists are action driven tasks that are simple to do and most individuals should be able to perform. Although the workshop benefited them by increasing their knowledge and increasing the understanding, they also gained the perspective of the importance of ISA and its advocacy. The list is reflective of the participants' recognition of the need for ISA and a response to the call to action, supporting Katsikas (2000) description of awareness, detailed earlier in the literature review. The response to the call to action also speaks to their understanding as a leader or "dominant role model" (Falkenberg & Herremans, 1995, p. 139) in sharing the awareness of information security by communicating, learning and stressing its importance.

As management emphasizes the importance of learning and sharing ISA, they are effectively encouraging an ISA climate, supporting Grojean, et al. (2004). The *commitment* list above suggests the implementation of value-based leadership to communicate and deliver on the *commitment* in favor of ISA advocacy.

Post-Test Questionnaire

The following are the post-test questions items focusing on identifying *commitment* to ISA advocacy. The participants were asked to evaluate the motivations towards advocacy, new plans to learn about information security awareness, and the effect on motivation to advocate, new plans to engage in advocacy activities as a result from the Action Research workshop.

I included post-test question 2 to this section as it pertains to *commitments* to learning. The participants were asked to describe any new plans to learn about information security awareness (ISA) provided by their organization. The increases in new plans to learn ISA suggest the Action Research workshop is an effective tool to improve the practice of *advocacy behaviors*. They are as follow:

- Bulletins published on the company intranet increased by 16%
- Learn from my colleagues and peers decreased by 8%
- Attend ISA presentations and events increased by 39%
- Watch company-posted webinars and videos increased by 21%
- Receive ISA e-mails decreased by 8%
- Ask my local information security officers when I need information increased by 16%
- Research ISA independently from external resources like the Internet increased by 13%

Relating to motivation, participants responded to the statements as follows:

(4a) *The ISA presentation did not affect my motivation or engagement ISA advocacy.* Indicating a positive effect on motivation or engagement in favor of ISA advocacy with a mean =2.17.

(4b) The ISA presentation motivated me to begin engaging in ISA advocacy. Indicating a positive effect on motivation or engagement in favor of ISA advocacy with a mean=5.68.

(4c) ISA presentation motivated me to increase my engagement in ISA advocacy. Indicating a positive effect on motivation or engagement in favor of ISA advocacy with a mean=5.51.

(4d) The ISA presentation motivated me to continue in my current high level of engagement in ISA advocacy. Suggesting a neutral or unchanged effect on motivation towards ISA advocacy with a mean=4.65. I interpret the participants were neutral about the words

reflecting continuity they did not have. Specifically the use of the words *current high level of engagement* was not an existing behavior prior to the workshop.

The responses to post question 4a, 4b, and 4c suggest the Action Research workshop is an effective tool to improve the practice of *advocacy behaviors*. The following summarizes the *commitments* to ISA advocacy expressed by the participants in the Post-Test Question 6. These plans suggest the Action Research workshop is an effective tool to improve the practice of *advocacy behaviors*.

- "Encourage leaders to do all staff presentation".
- "Encourage the team to learn more, and think about their awareness".
- "Find better connected with our IT team".
- "Share ISA with staff, peers and friends".
- "Share best practices with staff".
- "Email ISA articles to team".

In post-test question 8, the participants were asked to describe their ISA advocacy planned behaviors for the next few weeks after the workshop. The participants' selections show an increase on ISA advocacy planned behaviors, suggesting increase in learning about *advocacy behaviors* and a positive effect motivating action driven change in the practice of advocating for information security. I interpret the intended behaviors as a form of *commitment* to ISA advocacy.

39% will forward an ISA informational bulletin to my employees or peers.

16% will announce in their staff meeting an ISA event or presentation and encouraged attendance.

11% will invite the information security department to present ISA in my all hands meeting or departmental meetings.

42% will share an ISA news article read or found on the Internet.

42% will forward an email update with their comments regarding an industry incident.

3% will talk about policies or regulations with my staff or peers.

In post-test question 9, the participants were asked to describe what they learned new about security concerns and the need for information security awareness and advocacy. The participants shared their perspectives on their *current comfort level related to learning.* In their own words, they expressed an increased understanding for ISA, learning and advocacy, which I interpret are necessary as a pre cursor to *commitment*.

Their main contributions are categorized into four groups.

- Best practices to manage digital footprints.
- Online threat awareness
- The value of ISA advocacy
- General appreciation of ISA

Through the workshops, the participants received ISA, and used the information learned to commit to future ISA advocacy behaviors, supporting Siponen (2001), by enabling the participants to reach a state in which they can share ISA. These contributions supports action research is an effective approach to increase learning, and the practice of advocacy for information security. The new level of understanding positions the participants to share the awareness of information security.

Email Follow-Up

The email follow-ups are the data supporting participants follow through with their expressed *commitments*. There was a thirty-one percent (31.5 %) response rate for the three (3) weeks email request and an eighteen percent (18.4%) response rate for the six (6) weeks email request. The first question asked the participants to recount advocacy activities they have engaged in since the workshop. Most participants recounted activities consistent with the *commitments* expressed in the workshop. The communicated with peers, family and employees about security best practices they learned from the workshop. Some examples of best practices include password, email, and online accounts management activities that help protect personal information online. Furthermore, one participant's feedback was no advocacy activities. The responses suggest the participants shared what they learned from the workshop and actioned their *commitments* with the information they had. The data suggest management will share what they know.

The second question in the email follow up was related to actions towards new learning. I received a total of nineteen (19) email follow-up responses. The participants were presented with a multiple choice list of learning activities, their responses showed if a new learning activity was adopted or an existing learning activity was continued. From the list of learning activities like sign up for information security awareness e-mails, or ask peers for awareness information, nineteen (19) selections were towards continued behavior and sixteen (16) selections to the multiple choices were towards new behaviors. The data is evidence the participants continued with a behavior that increased their learning, as well as began new behaviors toward learning. The data also suggest they learned from the workshop alternatives to learning source.

Sharing what they learned, adopting new security behaviors are indicative to action research as an effective tool to increase learning and motivating improvements to practice, which are benefits of the action research theory as shared by McNiff & Whitehead (2006).

Summary

This chapter is focused on the analysis and interpretation of the data collected during the Action Research workshops. The use of mix methods applied for the data analysis was content analysis, descriptive and inferential statistics. There are several parts to the data analysis, they include:

- The pre-test and post-test questionnaire data analysis yielded descriptive and inferential statistics supporting the variables measured to address the study research question.
- Analyzing the data from the action exercise group discussion using descriptive content analysis yielded codes supporting constructs found in the literature review.
- The email follow-ups data analysis was accomplished using content analysis describing the long-term effect to learning, to practice improvement, and as a measurement of the construct *commitment*.

The key lessons learned from the research contribute to the overall body of knowledge in the information security awareness discipline as follow. Key finding 1: the feedback on self-reflective levels of knowledge in information security awareness indicated managers are not sufficiently exposed to ISA content. Key finding 2: the self-reflection on *advocacy behaviors* projected positive attitudes and increased motivation to propose and take actions toward sharing

ISA with employees and peers. Key finding 3: the main *challenges* discovered show that managers need more guidance, increase *awareness knowledge*, organizational support, and the creation of a climate that supports *advocacy behaviors*. Key finding 4: the Action Research workshop contributed to participants learning, and to improvements to information security practice through participants' new behaviors to increase ISA advocacy. Participants reported they learned and used the ISA topics discussed during the workshop with their friends, family, peers, and employees after the workshop.

The data findings section presents the data in the order and by the instrument used during workshop, while the data interpretation by construct organizes the data according to the variable it represents and the interpretation of the data impact on the construct. In Chapter 5, I discuss further my data analysis findings, and explore the limitations of the study as well as opportunities for future research.

Chapter 5: Discussions

As I mentioned earlier in the study, information security is a technical discipline that needs to be socialized. Creating security awareness that has an influence on people's lives can arise from drawing their attention to specific situations what are often intangible threats.

> *"We live in a society that depends on IT and IS. The proliferation of IT into every aspect of everyday life is no more a trend, but a fact. Under these circumstances any individual must at least have basic knowledge of issues related to the security of information systems" (Katsikas, 2000, p. 134).*

The Action Research workshop was one way of bringing managers attention to security incidents like disclosure of data. Through the ISA presentation a small sample of industry related security breaches were shown to describe the frequency of data disclosures, the magnitude, the type of breach and the severity of the incidents. The gaps in security that led towards the disclosure of information varied for each company. The individual businesses are responsible for taking corrective action. In the meantime, individually, people have the choice to act responsibly to protect their personal information by reducing the type of data and amount of data they leave online. As employees of any organization, we also should act to improve the protection of business information by adopting secure behaviors. This study found that by sharing the awareness of information security, we could effectively socialize the concern and share the knowledge for others to take action towards their own data protection. This helps them take action towards socializing information security more widely in the enterprise.

The research question findings reflect an opportunity to recognize the need for ISA and then developing a strategy for dispersing the information to peers and employees. In 2002, the Organisation for Economic Co-Operation and Development (OECD) revised the established Guidelines for the Security of Information Systems and Networks: Towards a Culture of

Security. The guidelines stress the importance of developing a culture of security, which includes raising awareness about risk and promoting information sharing, in public and private organizations, applicable everyone interacting with information systems and networks. My recommendation follows these foundational guidelines and extends them with organizational and public recommendation to practical steps aimed to foster a climate in favor of ISA advocacy

1. *Prioritize the importance of ISA – help in understanding that ISA and its advocacy is important to everyone at a business and personal level.*
2. *Obtain or extend learning – These are the activities that involved obtaining the awareness information necessary to share. Some examples include reaching out to the IT group, the industry forums, or public distributions for artifacts.*
3. *Plan ISA activities – The list of advocacy behaviors measured in the study suggest that advocacy activities can be simple to accomplish. Once a manager has obtained the ISA artifacts or tools, the next step is to share it. This can be accomplished by directly supplying the recipients or making the information available at a central location.*

    a. Furnish guidance – to share information that will help the recipient understand online behaviors that can help prevent disclosure of personal and company information.

    b. Make available tools – to share tools that aid in protecting information.

The most common task identified was the simplest tasks, to communicate. It is accomplished by talking, setting up email distributions, sharing, engaging in activities, and promoting information. Through the discussions of the research questions 1 through 4, we will see various examples where the participants communicate the information they know, ISA activities they have engaged in, and the challenges they identify as a constraint to sharing ISA.

RQ1: What do members of middle management know about information security awareness? This research question is measured with the variable Awareness Knowledge.

As part of the Action Research workshop managers recounted their experiences sharing information on information security, defined as ISA advocacy in this research. They also self-evaluated their levels of knowledge regarding information security awareness. The data suggest prior to the workshop the participants are insufficiently exposed to ISA and had a low level of awareness knowledge. Once the workshop concluded, the participants expressed an increase in awareness knowledge and a desire to learn more. The workshop itself was one "exposure" to an Information Security Awareness learning experience.

Before I shared the awareness of information security with the managers, the self-assessment yielded their views on their current level of knowledge, comfort level related to information security learning, ISA content format and attribute preferences, learning sources and their comfort level related to information security learning. The key findings are that the participants recounted not having a high level of ISA knowledge, which is supported by the descriptive statistics reflecting participants' low scores on questions regarding their awareness knowledge. They expressed discomfort in the topics of ISA, which was further supported by the descriptive statistics reflecting low scores on questions relating to their comfort and fluency of topics related to ISA in general. The questions relating to the self-assessed security awareness knowledge applicable to their employment indicated a slightly more positive neutral score. In regards to their preferences related to the content format and attributes, which is the material they would use to learn more about information security and information security advocacy, the means of the data ranged from 3.61 and 3.96, suggesting a low to neutral value for content preferences. The consistent low to neutral scores in the pre-test results is suggestive of the possibility the managers were not sufficiently exposed to ISA content. Furthermore, the participants expressed agreement on the need to learn more ISA.

During the ISA presentation, the participants' contributions to sharing knowledge and asking questions varied widely between expressions describing high twenty-four percent (24%), neutral sixteen percent (16%) and low sixty percent (60%) levels of prior ISA knowledge. The lack of contributions to share knowledge compared to the ISA inquiries also suggests the participants are insufficiently exposed to ISA. These findings support new opportunities to effectively increase the level of awareness about information security, among middle managers. The presentation followed by the opportunity to discuss the content of the presentation was an example of effectively socializing the awareness of information security.

Similarly, in the post-test item 3a through 3f, the participants reevaluated the available learning formats previously presented in the pre-test item 9a through 9f. The content formats included video, PowerPoint presentations, and text. Other format considerations included attributes like content that is easy to find, right in length and in a language that is easy to understand. The T-Test comparing the pre-test and post-test arithmetic means for each question, supports there is a significant difference in preferred learning formats and content attributes. In addition, supporting my interpretation, are the comments written in by the participants included statements used to express lack of awareness training on information security:

- "Unaware of any content"
- "Not aware of ISA training at my facility"
- "I am not aware of my company providing ISA content"

The majority of participants expressed the need to learn more ISA in post-test item 5. Forty-five percent (45%) responded that they need more training, as they “know only what is applicable to my immediate work environment”, and fifty-five (55%) responded they need to learn more, as they do not know much about information security at all. Only three (3%) expressed they are already are constantly learning about topics related to information security. The data supports the need for more systematic exposure to information security awareness in order to increase the awareness knowledge among managers.

In summary, as it pertains to awareness knowledge, the thesis study finds that feedback on self-reflective levels of knowledge in information security awareness indicates managers are not sufficiently exposed to ISA content. The ISA presentation within an Action Research workshop was an example of ISA exposure that helped participants put the subject of ISA into a relevant professional context, and self-evaluates their own level of security awareness knowledge regarding information security concerns. The pre-test survey served as an effective baseline, resulting in neutral feedback and low scores for their generally limited ISA insights.

RQ2: What are members of middle management currently doing about advocacy of information security awareness? This research question is measured with the variable Advocacy (behavior).

In chapter 4, the data interpretation section 2 shows managers participating in the research were not cognizant of the term ‘advocacy behaviors’ prior to the workshop. However, they had behaved in ways reflective of sharing awareness of information security. There is a measurable difference between the experiences considered *advocacy behaviors* in the participants’ pre-test survey, the comments analyzed from the awareness presentation, the workshop discussions, the post-test survey, and email follow-ups. The data suggest after the workshop they had a better understanding and sensitivity, and recounted some of their own advocacy behavior experiences.

The pre-test survey included two items related to the variable *advocacy behavior*. The pre-test item 11b and 11c, asked about current experiences advocating for ISA among peers and employees. They expressed disagreement trending neutral to the thoughts that they should be involved, but lacked the experience in item 11b, (mean=3.91). They reflected neutrality (mean=4.05) to always sharing ISA when they do receive the material in item 11c, (e.g. Sharing ISA emails).

The next question, pre-test item 12, showed the participants a list of activities that constitute part of advocacy behaviors. The responses indicate they did engage in the behaviors, even though they were not aware that the experiences were considered advocacy behaviors. The activities were normal activities related to communicating and sharing information. However, as it was referring to ISA advocacy, the same activities are meant to convey ISA related messages. The data shows eight percent (8%) forwarded ISA bulletins, five percent(5%) announced ISA event opportunities, sixteen percent(16%) shared ISA articles, eleven percent(11%) forwarded an ISA email, and eighteen percent(18%) talked about security policies and five percent(5%) reminded staff of a security best practice. This is surprisingly low.

The comments analyzed from the awareness presentation yielded themes under the variable *advocacy behavior* category. During the awareness presentation, the participants expressed a limited number of examples of *advocacy behaviors* by anecdotal recounts based on past experiences, and contributed to each other’s conversations with humor to clear an incorrect assumption. These examples are evidence of where participants conveyed ISA through communications. The limited number of contribution is indicative of opportunities for improvement in the practice of ISA advocacy by managers.

The workshop discussion analyses conducted for this thesis study yielded some findings of common themes under the variable *advocacy behavior* category. In environments where peer-to-peer communications was part of their organizational climate, the participants shared *awareness knowledge* by forwarding email notifications they received regarding security alerts. When information about policies was made available, managers talked to peers and employees about them. These *advocacy behaviors* are evidence of managers sharing *awareness knowledge* when the information was made available to them.

Another example of *advocacy behavior* came from a group of managers whom worked in a regulated environment. Their behavior described an active approach to obtaining *awareness knowledge* from industry related data feeds to share with peers and employees. Sharing was also accomplished by peer-to-peer communication through sending emails and talking. In addition, this group included awareness knowledge in their quarterly newsletter and collaborated with industry peers non-sensitive security best practices. These behaviors are evidence that some groups take a more proactive approach to advocacy behaviors by actively seeking *awareness knowledge* to share.

The email follow-up responses yielded data contributing to the *advocacy behavior* category. One of the participants' responded as not engaging in advocacy behavior, furthermore, the workshop did not change his/her current advocacy behavior. In this case, the Action Research workshop did not improve the practice of ISA advocacy.

Other email follow-up respondents did recount experiences in sharing the awareness of information security. Behaviors included peer-to-peer communications with family members and communications with employees and peers. The data included examples of experiences including, a manager shared the ISA presentation PowerPoint presented at the workshop with peers. Other managers spoke to their direct reports about security best practices. Another manager spoke to parents and friends about different methods to protect personal information. These examples are indicative that the participants understood the importance of ISA and chose to share the *awareness knowledge* they had with others. It is also an indication that the Action Research workshop had a positive impact towards improving the practice of sharing information security awareness.

In Summary, the self-reflection of advocacy behaviors projected positive attitudes and increased motivation to propose and take actions toward sharing ISA with employees and peers.

Prior to the Action Research workshop, the participants described having a neutral to low engagement in current advocacy practices, partially due to what I interpreted as the lack of understanding of the expectation of advocacy tasks. Although they did not understand what constituted taking actions towards advocacy, they did describe some activities that were common peer-to-peer communications about security concerns. Similar findings from the analysis of the comments from the awareness presentation support a low level of pre-workshop engagement in advocacy behaviors. Most comments during discussions were inquiries to knowledge, compared to suggesting ways for sharing ISA. Although low in number of suggestions, the data shows some advocacy behavior did occur.

The action research action exercise also supports advocacy behavior occurred when the information was available to share. Sharing information through peer-to-peer communication like forwarding an email was the most prevalent method of sharing. This is, as I interpret the data, part of a manager’s sense of duty. Although the data suggest the engagements in *advocacy* *behaviors* were low, findings support managers sharing *awareness knowledge* when the information was made available to them.

The email follow-up responses support my interpretation that managers shared ISA when it was made available to them. Although one respondent reported no change in their behavior, the vast majority recounted sharing the security themes presented in the workshop with family, friends, peers, and employees.

In general, manager's view of performing advocacy behaviors as it was presented in the workshop was not negative. My interpretation is based on the evidence showing they do share information when it is available to them.

RQ3: Have members of middle management identified any factors that affect their or peer managers' ISA advocacy behavior? This research question is measured with the variable Constraints (challenges).

In chapter 4, the data interpretation section 3 describes the *challenges* participants need to overcome to share ISA. Participating managers had opportunities to express in their own words, the *constraints* affecting advocacy behaviors, and present ideas to overcome the limitations.

The pre-test survey included two items related to the variable *challenges*. The pre-test responses to questions 9a through 9f consistently reflect neutrality, Agree and Disagree Equally, while the selections after the workshop showed higher scores reflecting the participants' preference for future content (video, text, and PowerPoint) and attributes such as language easy to understand and content easy to find. My interpretation of the results is the participants did not have an opinion due to lack of context at this point (pre-test) of the workshop and did not consider past experiences.

The pre-test item 11a, 11d and 11e, asked about constraints experienced affecting their experiences advocating for ISA among peers and employees. The data consistently reflected disagreement or neutrality to their opportunities, involvement, experiences sharing ISA materials, availability of resources and time. The participants were neutral about not having opportunities to advocate (Item 11a: mean=4.41). They disagreed (mean=3.34) they had the resources available to them to contribute to ISA advocacy, and they were neutral (mean=4) about having the time available to advocate. My interpretation of the results of disagreement or neutrality is because they were not familiar with the term, or what was involved in advocating for ISA. At this point of the workshop, they did not have enough information to formulate an opinion on opportunities, their involvement, their experiences, and the availability of resources or time as it relates to ISA advocacy.

During the ISA presentation, I encouraged the participants to ask comments and questions. The content analysis did not yield additional findings under the *challenges and constraints* category from the coded recordings taken during the ISA presentation. However, the following action research exercise yielded *challenges and constraints*. During the group dialogue, three of the Action Research Action Exercise instrument items contributed to *challenges and constraints:* reasons to advocate for ISA (ARAEQ2), *challenges and constraints* presently experienced making it harder to engage in advocacy behavior, (ARAEQ4) and ways to overcome the *challenges and constraints* identified (ARAEQ5).

When discussing the reasons to advocate for information security awareness, challenges were identified as constraints to sharing. One of the very first constraints identified was the concerns of not having enough knowledge and having different levels of knowledge to share. In addition, managers found the lack of guidance as a constraint. I interpret the reason participants do not advocate for ISA or why people hold back from sharing ISA is due to the lack of knowledge and guidance about the specific security topics.

Personal values like viewing others as honest people and lack of appreciation were also identified as constraints making it harder to engage in advocacy. These values, when viewed from the lens of the participants, can lead to inaction towards sharing ISA with others.

Most managers expressed an expectation their IT department provided all the security needed and it was not a topic of concern. This finding was indicative to the manger's trust and dependence on IT services for all security and ISA matters.

Many managers commented of the fact that they have plenty of work already and they lack the time to dedicate to advocacy behaviors. The finding shows there are time constraints to engaging in advocacy behaviors.

Some managers do not appreciate the value of information security awareness. The lack of consciousness of the value of security awareness is constraint that can lead to inaction. Table 5.1 summarizes the challenges and constraints identified during the action research exercise.

Table: 5.1: Challenges Identified During the Action Research Exercise

Action Research Exercise	Challenge or Constraint	Challenges Identified
ARAE2-Reasons to advocate for ISA	Constraints to sharing	Not having enough *ISA knowledge.* Different *levels of knowledge* Lack of guidance The lack of consciousness of the value of security awareness
ARAE3- Challenges presently experienced making it harder to engage in advocacy behavior	Personal values that lead to inaction towards sharing ISA with others. Expectation that their IT department provided all the security Time constraints	Viewing others as honest people Lack of appreciation The manger's trust and dependence on IT services Workload prioritization

The discussion of the ARAEQ4 was specific to identifying *challenges and constraints* presently experienced making it harder to engage in advocacy behavior. In this discussion, participants revisited some of the topics mentioned above, however new findings also emerged.

The complexity or perceived complexity of the subject of Information Security is a challenge. Managers found tasks such as managing multiple sets of credentials difficult. This supports that managers may hold back sharing information on subjects that are complex.

I associated avoiding an appearance of being overly concerned, with the inability to internalize the importance of ISA because they had not been personally affected by a security breach. This perspective can lead to inaction, Siponen and Vance (2010), in regards to sharing ISA with others.

The participants associated the IT restrictions (IT security controls, e.g. firewall filters to websites), on their laptops and computers as a constraint to engaging in advocacy behavior. The IT security controls made it difficult to take actions towards searching and download ISA related content to share. In addition, the respondents were hesitant to communicate their ability to perform activities like downloads to the IT group for fear that alerting the IT department would only lead to more restrictions. While ISA advocacy is a voluntary, the IT restrictions might be seen as strain affecting the manager's decision to support ISA as described by Leach (2003).

Prioritization conflicts with other organizational business urgencies was another constraint identified, similar to a perceived lack of time making it harder to engage in advocacy behaviors. In addition, lack of direction, lack of expectations to advocate for ISA on behalf of senior management, or guidance on their ISA related activities kept management from engaging in advocacy behaviors, as behavior is not identified as part of their functional role (Leach (2003), and Grojean, et al. (2004). This is evidence that managers need guidance, prioritization of the task, and time to engage in ISA advocacy.

Following the identification of challenges was a discussion of options available or suggestions to overcome the challenges. In ARAEQ5, the group explored ways to overcome the constraints and challenges.

One of the first recommendations to overcome the constraints identified was to clarify expectations for ISA advocacy from senior management. These finding support the importance for organizations to establish a climate of ISA and advocacy, starting with the senior management including C-suite leaders of the enterprise.

In addition, managers suggested the organization should share the direct and indirect impacts associated with an informational breach. Understanding the cost and impact on the company’s reputation would encourage middle managers’ motivation to adopt ISA advocacy behaviors. Similarly, explaining the reasons behind the security policies would help them understand the certain restrictions placed, and motivates compliance to best practices.

The groups also suggested more awareness education to increase learning. Suggestions include increased training, and use of delivery methods like using webinars, newsletters, and network messages for awareness tips. These recommendations opine to new information security awareness programs within the organizations.

The post-test survey results also yielded additional findings under the *challenges and constraints* category. There was one item 7a, 7c through 7e suggestive of opportunities for improvements in advocacy behavior. In item 7a, participants agreed (mean=5) they need to find opportunities and dedicate time to advocate for ISA (item 7e).

In item 7b, participants partially agree (mean=5.14) they need to pledge to engaging in ISA advocacy. Similarly, in item 7c, Participants were neutral (mean=4.97) to committing to details such as subscribing to a source of information or resources availability and begin sharing. Item 7d showed the same response to obtain the resources available to contribute to ISA advocacy with a mean of 4.97. I interpret these findings as evidence that not all managers are ready to engage in advocacy behaviors, and there is still conflict in role responsibilities that may need to be addressed. Furthermore, for some participants, their willingness to take action like finding resources to share with employees’ remains unchanged.

The data suggest participants gained consciousness about the importance of information security awareness and recognize gaps they need to overcome in order to advocate.

In summary, the core of the lower levels of ISA advocacy behaviors is not placed on managers not wanting to share ISA; the main challenges discovered show that managers need more guidance, increased awareness knowledge, organizational support, and the creation of a climate that supports advocacy behaviors. Part of fostering an ISA advocacy friendly environment is helping managers understand the reason behind technology restrictions and policies imposed, providing consistent updates about information breaches to avoid dismissal of potential risks. Updates should be in forms that are easy to share in order to avoid a sense of increased work. Organizations should use mechanism that encourage and demonstrate appreciation for advocacy behavior presenting it as a rewarding experience that is meant to help, by indirectly protecting, employees and peers.

As it relates to the content attributes, the information should not be challenging to obtain. The managers and general recipients of the content should be able to understand it to avoid exaggerated worries or concerns about its complexity. In addition, ISA content communication or articles should include guidance or best practices on use that are within the reach of managers.

While not all managers were ready to engage in advocacy behaviors, there was a general sense and evidence that the behaviors were part of the sense of duty a manager has towards their employees. The email responses show their sense of concern for others, such as family and friends. Fostering a climate in favor of ISA advocacy, by encouraging the environment and managing the constraints, is a way to socializing information security, which by nature is perceived to be a technical discipline.

RQ4: Do Action Research workshops have a measurable impact on positive ISA behaviors among Middle Managers who participate? This research question is measured with the variable Commitment (change, attitudes, and values).

The answer to this question is a qualified yes. In chapter 4, the data interpretation in section 1 shows an increased level of knowledge for managers participating in the research.

There is a measurable difference between the *awareness knowledge* expressed in the survey prior to the workshop, the comments analyzed from the awareness presentation, the workshop discussions, the post-test survey, and email follow-ups. The data interpretation section 4, describes the participants' expressed disposition to engage in ISA and advocacy after the ISA presentation. A measurable impact on positive ISA behaviors includes improvements to learning as well as improvements to the practice of advocacy behaviors. The instruments that contributed findings towards the *commitment* category were the content analysis of the ISA presentation, AR action exercise, post-test survey, and the email follow-up.

It was during the action research exercise that the participants expressed through dialogue, exchanges of security best practices and sharing some of their knowledge that it became evident which of the study participants had at least a base awareness knowledge foundation of information security, and which did not. Participants articulated and shared with their colleagues examples of best practices related to password management, email management, online account management and online shopping. The effectiveness of the information security awareness workshop format adds to the evidence supporting the need for and benefits from a broader exposure to ISA utilizing the methodology developed for this thesis study.

The ISA presentation then showed them key facts about information security data breaches and gave them insights on better managing their own personal digital footprint.

The group discussions served as a platform to discuss security concerns and collectively learn to manage those concerns through best practices in secure online behavior. The post-test and email follow-up responses show further evidence that the managers gained knowledge and applied the lessons effectively into their own lives personal and professional information security practices. This is demonstrated by the application of the ISA presentation guidance on password, email, and online account management by thesis study participants.

The content analysis of the ISA presentation yielded reactions to the content shared during the workshop. The main topic of the presentation was about information data breaches. Not surprisingly, some of the reactions included concern (worry) for the safety of their own personal information, the realization of the need for more awareness knowledge, and the need to learn ways to improve security practices. At this point of the workshop, the participants had not committed to ISA advocacy, but their concerns expressed motivation to learn more.

During the group dialogue, I found two of the Action Research Action Exercise instrument items contributed to variable *commitment* was item ARAEQ1 and the call to action. In the first, ARAEQ1, the participants discuss the benefits of advocacy behavior. As they discussed benefits, they expressed the reasons to share ISA was to protect themselves, their employees and their company's information.

As managers, some members of the group expressed their sense of responsibility, accountability and sense of duty toward maintaining their employees trust. Sharing information about security awareness is part of what a manager should do. Similarly, protection of company information was also mentioned by the managers as a reason to share information related to security but also part of their responsibilities as managers.

A benefit and motivation to engage in advocacy behavior was as a means to learn and share the awareness that will benefit themselves and others. The motivations expressed revolved around the protection of their personal information, company information and the information of their peers and employees.

Following the action research action exercise discussions was the “call to action”. This is where managers were asked to write down ISA advocacy activities that they felt were accomplishable, and to which they would personally commit. The result was a consolidated list of sixteen (16) ISA related activities that included communicating, stressing the importance, researching, obtain information to share, increase learning, and engage in activities. This is evidence of their expressed intentions to improve the practice of advocacy behaviors.

By *commitments*, the study refers to identified reasons for managers to improve the practice of learning ISA and advocating for ISA expressed by their attitudes, values, and changes in the experience.

The post-test survey included five items related to *commitments* to learning and *commitments* to the practice of advocacy behavior. The participants were asked to evaluate their motivations towards advocacy, new plans to learn about information security awareness, the effect on motivation to advocate, new plans to engage in advocacy activities as a result from the Action Research workshop.

Post-test item 2 is an indication that managers are committed to new learning. They shared their intention to learn about ISA through activities such as reading about the subject, research, and signing up for notifications, and attending presentations.

Post-test item 4a through 4c allowed managers to share their motivation to advocate for ISA *as it was affected* by the ISA presentation. The data shows the presentation did affect their motivation in a positive way to advocate for ISA (4a). The presentation also motivated managers to *begin engaging* (4b) and *increase their engagement* (4c) in advocacy behaviors. These responses are evidence the Action Research workshop is an effective tool to improve the practice of advocacy behaviors.

The post-test survey item 6 was a write-in section for participants to express their intended engagement in advocacy behaviors. Most of the planned behaviors were encouragements to learn more security awareness, or share the awareness of security through communications with peers. Similarly, in post-test item 8, participants selected form a list their intended advocacy behaviors, which included forwarding informational bulletins thirty-nine percent (39%); speak about ISA events in their staff meetings sixteen percent (16%); invite their local information security department to present ISA in their next departmental meeting eleven percent (11%); share news articles and forwarding ISA emails forty-two percent (42%) each; and talk about policies three percent (3%). Compared to the pre-test where they were asked to evaluate the same list from a current activity point of view, all except "talk about policies" showed an increase in the number of selections. I interpret the increase toward intended behavior as the participants learning about new behaviors they can accomplish to share the awareness of information security. In addition, most of the activities, except "talk about policies" share information provided by the communications channel that they are able to pass on to others through peer-to-peer communication. I interpret the lower score on activity "talk about policies" as an activity that would require *awareness knowledge* to accomplish, to which participants could not commit at the moment.

When the participants were asked to describe their new learning about ISA, the main contributions were they gained awareness of the existence of online threats; they learned the importance of ISA and grew an appreciation for it. They also learned some best practices to reduce their digital footprint. The contributions support action research is an effective took to increase learning.

The post-test results show an immediate impact, with an increased level of knowledge on average. This knowledge gain is shown in the self-assessment of participants on their knowledge gained during the workshop. The data also supports the use of action research theory and methods for developing effective tools to increase learning. Evidence of a positive gain in learning is found in the scores to post-test questions 1a, and 1b. Participants agreed their ISA knowledge increased (mean 6.19) as a result of attending the workshop (1a) and they agreed they now had a higher level of awareness knowledge (mean=5.71) (1b) following their participation in the ISA workshop. The data analysis of the pre-test item 7a and post-test item 1b, shows the T-test results (p<0.05) also supporting there is a significant difference in awareness level of Information Security knowledge as a result of attending this type of ISA workshop. Furthermore, after the positive self-assessment for increased knowledge, there was agreement that managers should be among those responsible for advocacy in the workplace to raise colleagues consciousness on the significance of raising information security awareness (mean=5.51) in the enterprise.

The data supports the workshop also expanded the participants' familiarity with available sources to learn about information security, providing them with options to seek knowledge. In the post-test item 2, the participants reevaluated the same available learning sources as had been presented to them in the pre-test item 8. Their learning source selections after the workshop included new learning activities, including researching ISA independently, attending ISA informational sessions, and asking their local information security groups for alternatives, which were not behaviors widely understood or practiced prior to the ISA workshop by the middle manager study participants.

More evidence of what participants learned about information security concerns and the need for ISA and advocacy is found in post-test item 9 data. The participants described, in their own words the lessons they learned during the Action Research workshop. I summarized the data in themes including an increase in the awareness of online threats, various security behavior best practices, and an understanding of the value of information security awareness. The recounts of lessons learned support the main findings of this study that Action Research workshops had positive effects and measurably contributed to increasing learning of managers of information security awareness.

Similarly, best practices demonstrating the lessons learned were included in the email follow-up with the study participants, which was consistent with the themes and information format previously mentioned under *awareness knowledge* findings. Included were password, online account, and email and information management. The email recounts of lessons learned support the Action Research workshop had a positive effect to learning 3 and 6 weeks after the workshop.

In the email follow-up participants also shared their new or continued approaches for learning ISA. Most choices presented as learning choices were selected for both continued and new learning approaches. The significant number of selections by participants showing their intent to sign up for security notification emails, and search independently around the internet as well as ask their local information security offices are all strong evidence that they applied the lessons learned from the workshop into practice, as they learned new ways to keep informed about security awareness.

The email follow-up data supports the participants' commitments to advocacy behaviors and learning. The responses included specific instances of shared ISA advocacy with peers, employees, family members, and friends. Peer to peer communication, which was recounted by the respondents using words like ‘spoke to’, ‘talked to’, ‘informed’ was the main way to share the awareness knowledge they had learned from the workshop. The *awareness knowledge* they shared included password, email, online account management, and strategies to reduce their digital footprint. Another form of sharing awareness included providing copies of the ISA presentation given in the workshop with peers.

The email follow-up also asks about the participants plans to learning about ISA. The participants selected among seven (7) learning activities or ways to increase their *awareness knowledge*. For each learning activity they distinguished between a new adopted or current learning approach. Sixteen (16) selections were new adoptions of learning approaches while, nineteen (19) selections were a continuation of existing learning tactics. These responses suggest the Action Research workshop had a positive effect on improvements in advocacy behavior practices and ISA learning.

In summary, the Action Research workshop contributes to participants learning, and to improvements to practice through participants contributions to increase ISA advocacy. Participants demonstrated they learned and used the ISA topics discussed during the workshop with their friends, family, peers, and employees after the workshop.

Although at first they did not readily recognize what actions meant to advocate for ISA, once they understood the expectation and what it involved, the findings support most managers did increase activities to increase their own learning, through adopting new and continuing learning approaches. They also demonstrated continual efforts to share what they learned with others to increase their awareness consciousness. In this study, these are the primary engagements considered as ISA advocacy. These engagements of learning and sharing awareness for others to learn were the main goals of leveraging action research. The data supports it was an effective tool to increase the participants learning and to improve the practice of ISA advocacy. Furthermore, it was an effective tool to socialize information security.

Limitations of the Study

The sample size of the population was small but by their nature action research designs provide richer data than purely quantitative studies. Only thirty-eight (38) managers participated in the study, and this limited scope allowed smaller group discussions, which in return yielded a collective voice and a deeper understanding on the participants' perspectives. A larger sample size would allow for greater data collection and the discovery of additional key findings.

Three organizations participated in the study; this was small representation of companies yielding a small amount of data relating to different organizational cultures. This limitation hindered my ability to collect significant findings representing organizational attributes characterizing how things are done in any specific company, however, the participating managers represented different functional areas within their companies.

The organizations represented only a few industries. This means the study may not have enough industry depth to represent effectively the specific security qualities of any particular industry. Since the scope of the study was on a specific group of managers, the effort focused in the discovery of the managers' point of views, and not the organization's attributes, culture or perspectives. Focusing on one type of industry, or larger number of organizations would allow for greater data collection and the discovery of additional key findings.

AR (mixed methods) is action oriented, focus on practical problems, exploring the cause, and generating data based on the experience in order to bring positive change. Its practical approach limits the traditional theoretical framework perspective many research study's follow. Therefore, it is different from the perspective that Action Research is not traditional research. There is not a measurement to prove if a specific theory is supported. Instead, my research proved participants learning increased and the AR study brought forth improvements to practice.

Using an AR mixed method approach leverages a survey, a focus group, and an email follow-up for data collection. Each instrument contributed to understanding the data holistically from a multi-dimensional perspective. The survey categorized the participants' responses while the focus group gave the participants a voice and helped understand the responses at a deeper level. The email follow-up helped measure the longer-term effect of the AR workshop. It was also a limitation as the multiple sources of data was cumbersome to manage and organize. A study of this size needs more resources and time to manage more effectively.

The PowerPoint presentation is only one format, many other learning tools and formats exists that may show effectiveness in sharing information. Although the participants expressed learning format preferences, this study is not a detailed comparison of learning format.

The "use cases" or "industry incidents" shared in the presentation were focused on one type of threat, which is universal to all organizations, disclosure of information. Many other types of threats exist that could also be topics of awareness sessions. With time and/or the development of new technology, new threats emerge and more information security awareness can be shared. Other suitable topics of awareness education could also be effective for the participants' interest and learning, and should be explored to determine the boundaries on the effectiveness of ISA Action Research workshops.

This researched focused on a limited number of variables: *awareness knowledge, advocacy behaviors*, *challenges*, and *constraints*, as it influences middle managers' advocacy. This allowed me to concentrate the responses into the topics of interest and build on key areas from research to practice.

Researcher bias may have been introduced by taking an active approach in participating in the study. My role as the researcher, the workshop facilitator, and presenter of the information security awareness session had the potential to influence bias on the participants. There is a risk that participants may have limited their responses due to the presence of the researcher or due to concern that their organizations may not be seen in a good light. This is a risk in all research. Furthermore, the simple fact that the participants are aware they are part of my research may introduce bias, commonly known as the Hawthorne effect (Economist, 2008; Shuttleworth, 2009). The multiple data collection methods, described in chapter 4 as equivalent forms, literal replication, self-assessments and email follow-ups were designed to manage the possibility of bias.

This study is a representation of motivators influencing ISA and its advocacy at a particular moment in time in the participating organizations. Organizational cultures, management structures, and priorities change with time. More studies are encouraged to monitor changing information security socialization and the role of the middle manager.

Policy Recommendations

There are industries that are regulated more than others are. I found examples of several regulated environments with frameworks and guidelines specifying the need for awareness education (http://www.informationshield.com/security-awareness-requirements.html). Some examples include healthcare, which follows the framework established under the Health Insurance Portability and Accountability Act (HIPAA) 1996. Within the act is the Security Final Rule 164.308 (a) (5) (i) (R), calling for the implementation of a security awareness and training program for all members of its workforce (including management). The ISO/IEC 17799:2005 international security framework includes within the best practices the section 8.2.2 calling for information security awareness, education, and training on organizational policies, procedures. This should include all employees and where applicable, contractors and third parties. The Sarbanes-Oxley Act (SOX) affects all US publicly traded companies, its guidelines includes training and education as it relates to SOX, including the maintenance of registration logs and attendance sheet as evidence of compliance. The framework for the Chemical Sector Cyber Security Program calls for effective cyber security training and security awareness programs for employees.

There is such an abundance of information broadly used on a variety of personal activities and business activities that we should all learn to be aware of the threats, risks, and ways to prevent abuse of information. Following the foundational guidelines of OECD, I reiterate the importance of developing a culture of security. I do recommend a dimension or approach beyond focusing on industry regulatory and compliance; that is, to regulate the use of information and making available information security awareness to all entities. Raising awareness about risk and promoting information sharing, in public and private organizations, applicable everyone interacting with information systems and networks. Personal information, financial information, biometrics information, and healthcare information are just some of the information classifications that need to be defined and protected by all entities that use it. The stakeholders would include the public, businesses, government agencies, private groups, and social entities. Information protection policies should be expanded to include the protection of all sensitive information classifications across all industries and non-commercial uses.

Future Research

This thesis has shown that the action research methodology can be an effective tool to socialize information security awareness. Given these positive, statistically significant conclusions on such a critical issue due to risks from continuous human and bot attacks on all enterprise IT systems, the open questions beyond the scope of this study are also of growing importance. This stresses the urgency to address and enhance enterprise information security awareness. As suggested, managers in varying industrial and business sectors may have particular needs and knowledge gaps that vary substantially from those of the study sample assessed in this study. Therefore, replication of this study with a) a different sample population; b) a substantially larger study population on which demographic information may be usefully assessed to explore issues such as between group, gender, and learning style preferences for enhancing – and sustaining – information security awareness. This indicates c) longitudinal studies assessing whether the knowledge gained is retained and amplified over time; and if not what might be done to enhance information security awareness for enterprise sustainability of best practices.

The Action Research workshop contributed to participants' learning, and to improvements to practice through participants' actions to increase ISA advocacy. Participants demonstrated they learned and used the ISA topics discussed during the workshop with their friends, family, peers, and employees after the workshop. These engagements of learning, sharing awareness for others to learn was the main goal of leveraging action research, the data supports is was an effective tool to increase the participants learning and to improve the practice of ISA advocacy.

Information security awareness and advocacy among non-IT security professionals is of interest for future research as it is meant to create consciousness of security concerns that exists for employees of organizations, management teams, and society in general. Therefore, future researchers may wish to consider further industrial organization issues in designing effective information security awareness advocacy efforts. (Such as, initiating an enhanced on-going firm-wide effort to emphasize clearly the preeminent corporate significance of effective ISA advocacy efforts). It may well be that the methods and learning tools utilized in this thesis study population of middle managers may be more effective in a particular organizational environment. It may also prove to be the case that advocacy behavior can be increased in part through other forms of in-person, blended; or distributed learning. Therefore, further research studies could explore these information security awareness and organizational culture questions.

Students of business and economic history may wish to consider contrasting and hypothesizing varying outcomes from information security awareness advocacy best practices Wherever we have people using technologies, we have an audience to share information security awareness. Opportunities for research within different groups of people can be found in a variety of social structures including our community centers, families, schools, businesses, and employers. Maintaining information security awareness, while coordinating user and device behavior, is a growing challenge for firms in many industries, as prior research predicted. (McKnight, Lehr & Howison, 2007) In today’s society, people are exposed to a variety of technologies of various ages and vintages requiring different practices for information security awareness advocacy and maintenance. For example, some schools in the USA use portable devices like tablets in grade school classrooms. In this situation, we have an opportunity to study ISA and its advocacy among grade school children, recognizing the role of the device and use context, and user behaviors. In another example, elderly groups are taught how to browse the Internet and send email, again, presenting an opportunity for ISA research. Information security awareness and its advocacy is a discipline that should be expanded at multiple societal outlets nationwide, using a variety of tools and multimedia channels of communications. Opportunities for research exist to explore how our communities, employers and students learning about information security awareness.

Opportunities exist to research new ways to share ISA that is relevant to the need of the different audiences and help technology users under different circumstances learn the appropriate security awareness for their situation. Some examples are schools use technology as a teaching aid; a manufacturing company uses technology for the production of widgets. Technology is in these cases are tools used in support of a function and the people are not IT professionals. There is a need to share information security awareness in order to include people using the technology as part of the layers of security. People using technology should be made aware that they are the stewards of information.

The availability of different groups of people for research also presents an opportunity to explore ISA and its advocacy from a broader perspective by including a larger sample size or a narrow scope, like my own experience where only thirty-eight (38) managers participated.

As it pertains to methodologies, opportunities exist for single research methods to reach a broader research population to study a more focused construct. For example, a larger scale survey could explore only the existing levels of ISA knowledge to help determine the need for targeted or general awareness training. A longitudinal study may serve to measure the increase in learning about security awareness as people become engaged at early ages with technology. Case studies of groups or smaller organizations could be used to explore the understanding of motivating commitment to sharing ISA with peers and family; furthermore, it could support the exploration of creating organizational climates that support advocacy behaviors.

Although my study includes a presentation about information disclosure there are multiple security domains that can be topics of information security awareness. There is opportunity for research and development of relevant ISA topics like socializing network security, learning formats like videos and webinars, and dissemination channels like television, radio, or social media to produce awareness outlets to reach different societal groups with sufficient exposure.

This study focused on the understanding of four variables, awareness knowledge, advocacy behaviors, constrains and commitments. While this particular study allowed me to remain focused on these constructs, there are opportunities to expand the exploration and understanding of other key constructs that impact learning and sharing ISA and increase motivation to propose and take actions toward sharing ISA with employees, friends, family, and peers.

This study is not industry specific, which lends itself for reuse across industries. There is however, opportunity to research information security awareness that is industry specific, beyond highly regulated environments, as well as within specific enterprises, industries, market structures, and IT security supply chains. Varying regulatory environments will affect the rate of adoption of new security compliance as a service offering for developing technologies like cloud, mobile and Internet of Things. New technologies affect the complexity and specificity of the information security vulnerabilities of an existing environment, which includes legacy systems, new systems, and Bring Your Own Device user demand.

How well different methods of information security awareness advocacy prove to be effective under varying business and regulatory conditions, there is an increase need to bring forth ISA to all environments, as information is everywhere. In this research, one of the challenges discovered show that managers need more guidance on ISA and advocacy. This means, to quickly and painlessly - first learn more themselves, second increase awareness knowledge and organizational support for ISA and contribute to the creation of a climate and corporate culture that supports advocacy behaviors, as essential enterprise self-defense mechanisms. There are many opportunities for colleagues to consider additional research beyond the scope of this thesis, especially focused on industrial organization and security awareness climate, methods and best practices observed in other regulated and non-regulated environments. Finally, with increased information security compliance, cloud services, and Internet of Things applications, new questions for research emerge on what new security guidelines are needed. These apply not only to middle managers, but also to IT specialists, cloud brokers, and Internet of Things operators. Based on the daily news of yet another "data/credit card/personally identifiable information/trade secret" theft, there is a lack of industry ISA advocacy best practices. We have urgent need perform better against persistent human and technical threats to critical enterprise systems. Research on these rising trends, and the risks to be managed need to be part of enhanced information security awareness.

Last but not least, we note this study was of middle managers, rather than those who are entry level supervisors or the C-suite executives. I conclude my thesis by suggesting that leadership studies of firms' senior executive during normal business conditions, and under crisis situations (either the firm's staff, procedures or practices own making; or triggered by an external event beyond the firm's operational control), would provide informative research that has both theoretical and practical value.   Since the reputational loss may far exceed the direct financial loss of a data breach, and out of a desire to not help attackers, there are, however, reasons that firms do not like to talk a lot about their own internal security procedures and practices except in generalities. Deeper understanding is needed on the impact of an employee with only minimal ISA knowledge or comprehension of the significance of his or her own advocacy behaviors to enterprise financial health and security.

This study suggests that there are many opportunities for firm leadership to play a key advocacy role in maintaining enterprise information security awareness as a firm priority. Further studies of firm leadership in business as usual and corporate data breach crisis conditions, and the correlation with information security awareness advocacy best practices, are encouraged.

References

Ashkanasy, N. M., & O'Connor, C. (1997). Value congruence in leader–member exchange. The Journal of Social Psychology, 137(5), 647.

Avison, D., Baskerville, R., & Myers, M. (2001). Controlling action research projects. Information Technology & People, 14(1), 28–45.

Baskerville, R., & Myers, M. D. (2004). Special issue on action research information systems: Making IS research relevant to practice—foreword. MIS Quarterly, 28(3), 329.

Chen, C., Shaw, R., & Yang, S. (2006). Mitigating information security risks by increasing user security awareness: A case study of an Information Security Awareness system. Information Technology, Learning, and Performance Journal, 24(1), 1–14.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information Management & Computer Security, 16(5), 484–501. Doi:10.1108/09685220810920558

Cluley, G. (2012, May 29). Beware Remove your Facebook timeline scams. Naked Security. Retrieved from http://nakedsecurity.sophos.com/2012/05/29/beware-remove-your-facebook-timeline-scams/

Constantin, L. (2012, October 8). Facebook's phone search can be abused to find people's numbers, researchers say. Computer World. Retrieved from www.computerworld.com/s/article/9232178/Facebook_s_phone_search_can_be_abused_to_find_people_s_numbers_researchers_say?taxonomyId=244

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

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). The SAGE handbook of qualitative research. Sage Publications.

Desman, M. B. (2003). The ten commandments of information security awareness. *Security Management Practices*, 39–44.

Deyhle, J. (2002, February 19). *Two-thirds of security officers say security awareness dangerously inadequate or inadequate in new PentaSafe security awareness index.* PR Newswire Association. Available at www.prnewswire.com/news-releases/two-thirds-of-security-officers-say-security-awareness-dangerously-inadequate-or-inadequate-in-new-pentasafe-security-awareness-indextm-report-76064927.html

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*(3), 349–375.

Economist (2008, Nov 3) The Economist. *Idea: The Hawthorne Effect* Online extras. Retrieved from http://www.economist.com/node/12510632

Falkenberg, L., & Herremans, I. (1995). Ethical behaviours in organizations: Directed by the formal. *Journal of Business Ethics*, *14*(2), 133.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352.

Gelman, A., Hill, J. (2006). Missing-data imputation. In: Data Analysis Using Regression and Multilevel/Hierarchical Models. pp. 529-544. Cambridge University Press

Goldkuhl, G. (2004). *Meanings of pragmatism: Ways to conduct information systems research.* Proceedings from the 2nd International conference on Action in Language, Organisations and Information Systems (ALOIS), Linköping, Sweden.

Grojean, M. W., Resick, C. J., Dickson, M. W., & Smith, D. B. (2004). Leaders, values, and organizational climate: Examining leadership strategies for establishing an organizational climate regarding ethics. *Journal of Business Ethics, 55*(3), 223–241. http://www.informationshield.com/security-awareness-requirements.html

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risk in software process improvement: An action research approach. *MIS Quarterly, 28*(3), 395.

Kaarst-Brown, M. L., & Guzman, I. R. (2008). *Decisions, decisions: Ethnography or mixed-method approaches to study cultural issues in IS research?* Proceedings from the Cultural Attitudes Towards Technology and Communication (CATaC) biennial conference, June 24-28. Nimes, France.

Kaarst-Brown, M. L., & Robey, D. (1999). More on myth, magic, and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People, 12*(2), 192–217.

Kamberelis, G., & Dimitriadis, G. (2013). *From structured interviews to collective conversations.* New York: Routledge.

Katsikas, S. K. (2000). Health care management and information systems security: Awareness, training or education? *International Journal of Medical Informatics, 60*(2), 129–135.

King, S., & Stuart, D.H. (2012). Action research: A first grade teacher's journey of deepening. *Ohio Reading Teacher, 42*(1): 34.

Krebs, B. (2012, May 17). *Facebook takes aim at cross-browser "LilyJade" worm.* Krebs on Security. Retrieved from http://krebsonsecurity.com/2012/05/facebook-takes-aim-at-cross-browser-lilyjade-worm/

Kritsonis, A. (2005). Comparison of change theories. *International Journal of Scholarly Academic Intellectual Diversity, 8*(1), 1–7.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685–692.

Leedy, P. D., & Ormrod, J. E. (2009). *Practical research: Planning and design* (9th ed.). Portland, Pearson Education.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 173–186.

Martensson, P., & Allen, S. L. (2004). Dialogical action research at Omega Corporation. *MIS Quarterly, 28*(3), 507–536.

Mattise, N. (2012, June 7). *Another hack? Last.fm warns users to change their passwords.* Ars Technica. Retrieved from http://arstechnica.com/security/2012/06/another-hack-last-fm-warns-users-to-change-their-passwords/

McKnight, L. W., W. Lehr, & J. Howison (2007) Coordinating User and Device Behavior in Wireless Grids, in Fitzek, F., & Katz, M., (Eds.), *Cognitive Wireless Networks.* Springer.

McKnight, L. W., Sharif, R. M., & Van de Wijngaert, L. (2002). Wireless grids: Assessing a new technology from a user perspective. *Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges,* 170–181.

McLean, K. (1992). (ed.) *Information security awareness: Selling the cause.* Proceedings from the IFIP TC11 Eighth International Conference on Information Security, Singapore, 27-29 May. Amsterdam: North-Holland.

McNiff, J., & Whitehead, A. J. (2006). *All you need to know about action research.* London: Sage Publications.

Meglino, B. M., Ravlin, E. C., & Adkins, C. L. (1989). A work values approach to corporate culture: A field test of the value congruence process and its relationship to individual outcomes. *Journal of Applied Psychology, 74*(3), 424–432.

Meglino, B. M., Ravlin, E. C., & Adkins, C. (1991). Value congruence and satisfaction with a leader: An examination of the role of interaction. *Human Relations, 44*(5), 481–495.

Mejias, R. J. (January, 2012). *An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk.* Paper presented at the 2012 45th Hawaii International Conference on System Sciences, Maui.

Merriam-Webster's collegiate dictionary (11th ed.). Available from www.merriam-webster.com.

Mwanahiba, M., & Luke, D. (1991, Sep/Oct). Professional development: Action research workshop: The Nairobi model. *Public Administration & Development (1986-1998), 11*(5): 521.

Newton, R. & Rudestam, K. (1999). How Do I Prepare Data for Analysis. In: Your Statistical Consultant: Answers to Your Data Analysis Questions. Pp. 5-23 (1st ed) SAGE Publications

Organisation for Economic Co-operation and Development. (2002). OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD Publishing. http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm

Posner, B. Z., Kouzes, J. M., & Schmidt, W. H. (1985). Shared values make a difference: An empirical test of corporate culture. *Human Resource Management, 24*(3), 293.

Racoma, J. A. (2012, June 20). *Pinterest locks out hacked accounts, investigates security breach.* CMS Wire. Retrieved from www.cmswire.com/cms/customer-experience/pinterest-locks-out-hacked-accounts-investigates-security-breach-016607.php

Ramsay, M., & Anderson, E. (2008). Interactional workshops for mental health nursing students: An action research cycle and reflections of students' experiences. *Mental Health Nursing 28*(3): 12–15.

Rokeach, M. (1968). *Beliefs, attitudes and values: A theory of organization and change.* San Francisco, Jossey-Bass

Rokeach, M. (1973). *The nature of human values.* New York, NY: Free Press.

Rudestan, K. & Newton, R. (2007). Surviving Your Dissertation (3rd ed.) SAGE Publications

Ruben, R. (2012). *Exploring an underdog case: What hinders or motivates participatory behavior in animal advocacy*. (Doctoral dissertation). UMI Dissertation Publishing.

Saldana, Johnny, (2013) The Coding Manual for Qualitative Researchers (2nd ed.) SAGE Publications

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. *Advances in Experimental Social Psychology, 25*(1), 1–65.

Schwartz, S. H., & Bilsky, W. (1987). Toward a universal psychological structure of human values. *Journal of Personality and Social Psychology, 53*(3), 550–562.

Shuttleworth, M (Oct 10, 2009). Hawthorne Effect. Retrieved Nov 05, 2014 from Explorable.com: https://explorable.com/hawthorne-effect

Silveira, V. (2012, June 7). *LinkedIn member passwords compromised.* LinkedIn blog. Retrieved from http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

Siponen, Mikko. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

Siponen, Mikko. T. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society*, *31*(2), 24–29.

Siponen, M & Vance, A (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly 34(3), 487-502.

Spears, J L & Barki, H (2010). User participation in Information Systems Security Risk Management.MIS Quarterly 34(3), 503-522.

Stanleigh, M. (2008). Effecting successful change management initiatives. Industrial and commercial training. *Industrial and Commercial Training*, *40*(1), 34–37.

Steiner, D. D. (1988). Value perceptions in leader-member exchange. *The Journal of Social Psychology*, *128*(5), 611–618.

Stephanou, A. (2008). The Impact of Information Security Awareness Training on Information Security Behavior, 1–120.

Thomas, A. P. (1990). A study of cognitive factors affecting the successful implementation of end-user information technology. *ProQuest Dissertations & Theses (PQDT)*. State University of New York at Buffalo, ProQuest, UMI Dissertations Publishing, 1990. 9033741.

Wada, F., Longe, O., & Danquah, P. (2012). Actions speak louder than words: Understanding cyber-criminal behavior using criminological theories. *Journal of Internet Banking and Commerce, 17*(1).

Whittaker, Z. (2012, November 8). *Twitter user passwords reset after accounts breached.* ZD Net. Retrieved from www.zdnet.com/twitter-user-passwords-reset-after-accounts-breached-7000007108/.

Zaiontz C. (2014, November 10, 2014) Real Statistics Using Excel. www.real-statistics.com

Zorz, Z. (2012, May 18). *Worm targets Facebook users via PMs.* Help Net Security Retrieved from www.net-security.org/malware_news.php?id=2114.

Zorz, Z. (2012, May 22). *Beware of fake Facebook account cancellation emails*. Help Net Security. Retrieved from www.net-security.org/malware_news.php?id=2119.

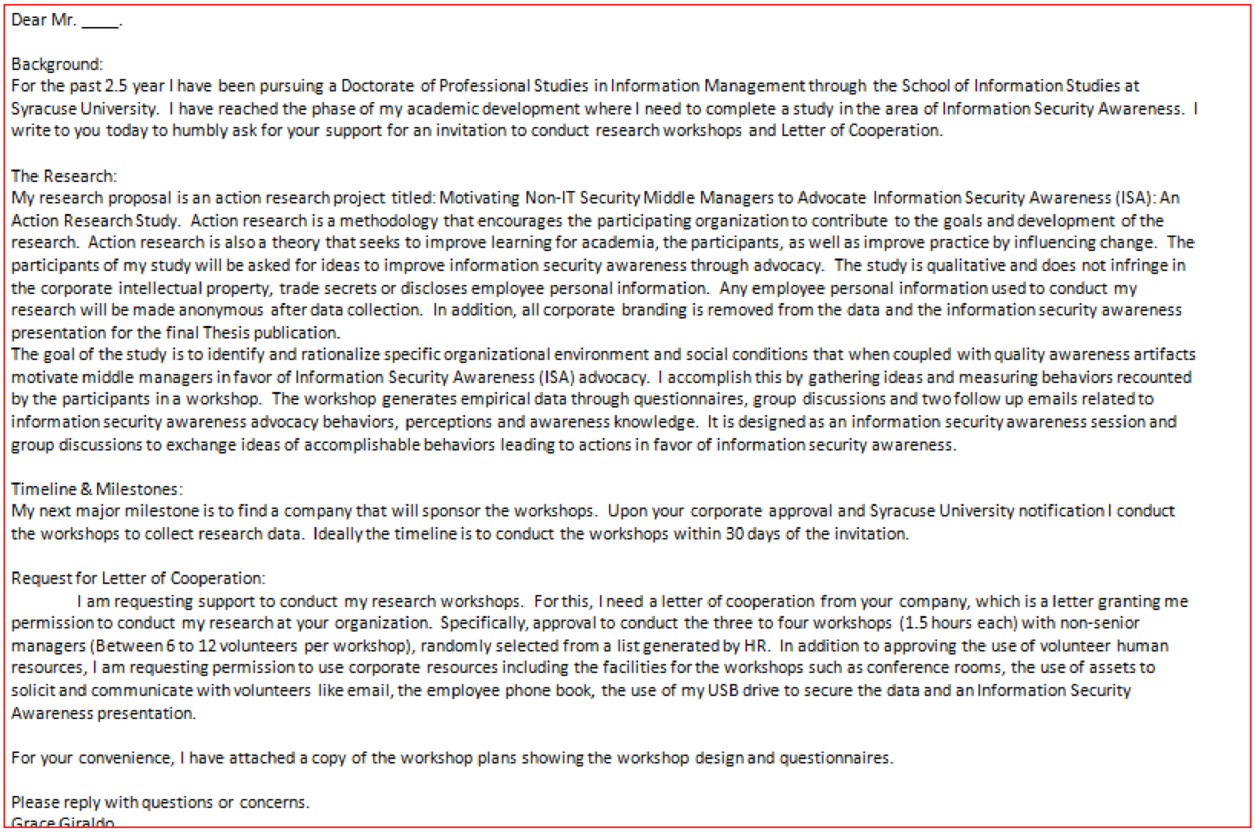
Zorz, Z. (2012, October 24). *Bogus Twitter direct messages lead to iPad scam, surveys, and phishing.* Help Net Security. Retrieved from www.net-security.org/secworld.php?id=13831.

APPENDICES

Appendix 1: Definitions of Terms

Terms	Definition Used in Study
Action Research (AR)	A research methodology where the researcher and the participants collaborate on ideas and recommendations leading to improvements in organizational practice.
Action Research Workshop	The workshop is a methodological tool use to query through activities change on participants ISA advocacy behavior. The workshop activities contribute an opportunity for the participants to increase their security knowledge and recommend improvements in ISA advocacy practices
Advocacy	Supporting a cause (Merriam-Webster, 2013)
Advocacy Behavior	Supporting a cause while providing guidance and motivation, usually driven by high quality leadership who demonstrate their commitment to success (Stanleigh, 2008 p.37; Merriam-Webster, 2013)
Information Security (IS)	A specialized technical discipline focused on the protection of information. "InfoSec involves a complex interaction between technical, organizational and behavioral factors" (Dutta & Roy, 2008 p.1)
Information Security Awareness (ISA)	The degree to which organizational members understand the importance of IS security, the appropriate levels of security required, and their individual responsibilities in maintaining the security of their information resources
ISA Artefacts	Awareness instruments used to disseminate information security (IS) information; E.G. intranet articles, published incidents, videos, and information repositories
ISA Content	Guidelines serving as a source for the creation of information security awareness E.G. Organizational security policies, security practices, industry regulations, and reports of industry incidents
ISA Knowledge	Knowledge of organizational security policies and/or practices
ISA Program	Events, materials, presentations, and courses planned and disseminated by the organization's information security department as part of an organized effort to influence employees in secure computing or information handling practices
Middle Management	Non-IT security managers from multiple offices in business, IT, and finance departments who are not considered executive manager

Appendix 2: Request for Sponsorship Email



Dear Mr. ____.

Background:
For the past 2.5 year I have been pursuing a Doctorate of Professional Studies in Information Management through the School of Information Studies at Syracuse University. I have reached the phase of my academic development where I need to complete a study in the area of Information Security Awareness. I write to you today to humbly ask for your support for an invitation to conduct research workshops and Letter of Cooperation.

The Research:
My research proposal is an action research project titled: Motivating Non-IT Security Middle Managers to Advocate Information Security Awareness (ISA): An Action Research Study. Action research is a methodology that encourages the participating organization to contribute to the goals and development of the research. Action research is also a theory that seeks to improve learning for academia, the participants, as well as improve practice by influencing change. The participants of my study will be asked for ideas to improve information security awareness through advocacy. The study is qualitative and does not infringe in the corporate intellectual property, trade secrets or discloses employee personal information. Any employee personal information used to conduct my research will be made anonymous after data collection. In addition, all corporate branding is removed from the data and the information security awareness presentation for the final Thesis publication.
The goal of the study is to identify and rationalize specific organizational environment and social conditions that when coupled with quality awareness artifacts motivate middle managers in favor of Information Security Awareness (ISA) advocacy. I accomplish this by gathering ideas and measuring behaviors recounted by the participants in a workshop. The workshop generates empirical data through questionnaires, group discussions and two follow up emails related to information security awareness advocacy behaviors, perceptions and awareness knowledge. It is designed as an information security awareness session and group discussions to exchange ideas of accomplishable behaviors leading to actions in favor of information security awareness.

Timeline & Milestones:
My next major milestone is to find a company that will sponsor the workshops. Upon your corporate approval and Syracuse University notification I conduct the workshops to collect research data. Ideally the timeline is to conduct the workshops within 30 days of the invitation.

Request for Letter of Cooperation:
I am requesting support to conduct my research workshops. For this, I need a letter of cooperation from your company, which is a letter granting me permission to conduct my research at your organization. Specifically, approval to conduct the three to four workshops (1.5 hours each) with non-senior managers (Between 6 to 12 volunteers per workshop), randomly selected from a list generated by HR. In addition to approving the use of volunteer human resources, I am requesting permission to use corporate resources including the facilities for the workshops such as conference rooms, the use of assets to solicit and communicate with volunteers like email, the employee phone book, the use of my USB drive to secure the data and an Information Security Awareness presentation.

For your convenience, I have attached a copy of the workshop plans showing the workshop design and questionnaires.

Please reply with questions or concerns.
Grace Giraldo

Appendix 3: Security Awareness Action Research Workshop Facilitator Form

Workshop: ____

Date: __________ Time: ______ Location: ______________

Facilitator: ___________________ Facilitator’s phone #: ___________________

Facilitator’s Role:

- Be objective.
- Listen.
- De-identify the responses.
- Protect participants from harm.
- Go over ground rules.
- Present the sample ISA content artifacts, including audiovisual presentations on security incidents or security policy awareness, which is shown to the participants in large group

Appendix 3: Action Research Workshop Facilitator Form		
Workshop Step	**Main Points**	**Overview of Facilitator Activities**
Before participants arrive 30-45 minutes	Preparation	Arrive half an hour to forty-five minutes early with consent forms and presentation. Make sure signage with directions to room is posted Make sure tape recorder is working and ready Set up room (flip charts, notepads, tables, and chairs in groups of 4.) Load “Facts” presentation and test technology
IN LARGE GROUP		

Appendix 3: Action Research Workshop Facilitator Form		
Workshop Step	**Main Points**	**Overview of Facilitator Activities**
After participants arrive: 15 minutes	Welcome, Provide overview of study, and obtain Consent forms	Welcome participants, offer them refreshments, and help them make name tents Check their names off on the roster Begin workshop with introduction to facilitator and any assistants including your role(s), Provide a brief explanation of the purpose of the research, the purpose of workshop meeting, and overview of the AR Workshop process (what will happen during the day) Give the participants the workshop paperwork (2 copies of consent and information forms) and allow 10 minutes complete Offer to answer questions about the consent form. Collect the consent forms and briefly review them for completeness

Appendix 3: Action Research Workshop Facilitator Form		
Workshop Step	**Main Points**	**Overview of Facilitator Activities**
Pre-test 10 minutes	Administer Introductory Questionnaire to gather baseline "before" data	Hand out individual (coded) questionnaires and explain purpose -These allows me to compare whether this workshop is an effective way to generate change in IS advocacy behavior or knowledge -I am interested in their personal opinions and actual actions, not generic information or what they feel they could be doing - Reassure that it is okay if they are not doing any IS advocacy activity -Information is coded to conceal their identity but allows matching to follow-up questionnaires, -individual responses are only be seen by the researcher -They have about ten minutes to complete this Briefly explain the five main question areas: 1. Demographics – data collected to describe the participants and used for data analysis and results. 2. Your current IS knowledge level – your perception of understanding of information security. 3. Current sources of Information Security material including perceptions of content, format, timing and value - your perspective on the ISA provided 4. Your current Information Security learning comfort level – your perception on learning opportunities. 5. Your advocacy experiences – Your perspective on advocacy behaviors Collect pre-test, quickly scan, and put in envelope;
Treatment, part 1: Facts 20 minutes	ISA Presentation motivating facts to inform and engage	Allow about 15 minutes to present Motivating Facts about IS, ISA and ISA advocacy: -Why ISA is important (present facts about ISA in general and at firm to motivate them to care and want to make a difference) -Present facts about the importance of advocacy behaviors on the part of non-IT security managers such as themselves (reinforces that their role is important and they can make a difference) Answer participants questions or clarify points

Appendix 3: Action Research Workshop Facilitator Form

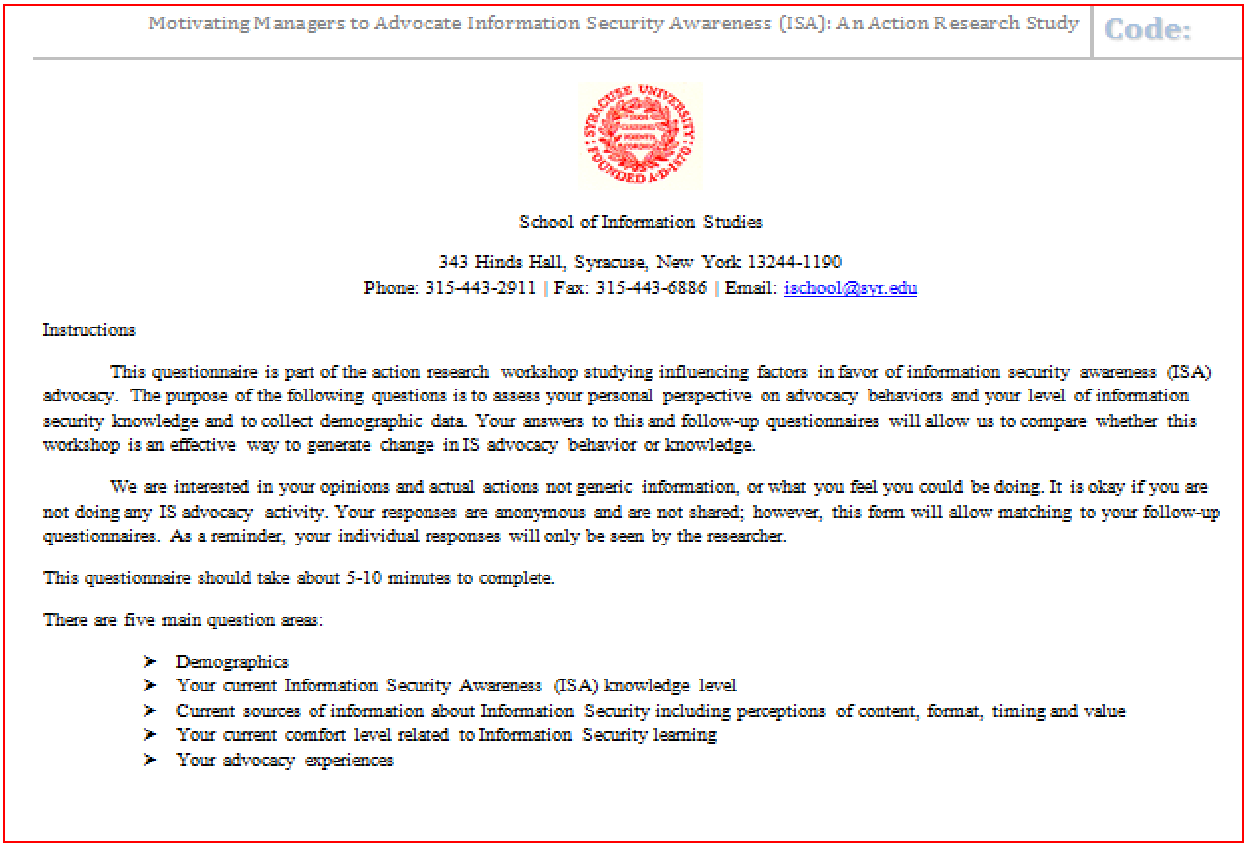
Workshop Step	Main Points	Overview of Facilitator Activities
Treatment, part 2: Action research, current action exercise 25 minutes	-Obtain information about current advocacy activities and IS knowledge -Engage in sharing and discussion	Provide Instructions, including: -Goal of part 2 is to share their personal experiences and activities, -They will have 15 minutes to share, discuss and make notes before they are presented to the larger group -Request that notes be written on flip chart of white board paper, -Request they identify one or more presenters for their group -Ask groups to make lists of what they are collectively DOING NOW (not ideas) so that they are ready to present back to the larger group: Provide three to four focal questions around their individual advocacy behaviors, reasons behind these behaviors, and perceived challenges or opportunities associated with ISA advocacy Allow additional 10 minutes to present to large group, debrief some of the ideas, obtain elaboration, answer questions
Post-test 1 10 minutes	Gather comparison data for pre-test/post-test differences (Time period 0)	Pass out and collect post-workshop questionnaire with matching questions to pre-test, except worded to address changes since beginning They will have 10 minutes to complete the post-test. E.g. Has your level of IS knowledge changed as a result of this workshop? How would you rank your current IS advocacy behavior? Describe any new advocacy activities you plan to implement in the coming days and weeks?

Appendix 3: Action Research Workshop Facilitator Form

Workshop Step	Main Points	Overview of Facilitator Activities
At end of Workshop 10 minutes	Close the AR workshop	Thank everyone for participating and sharing their ideas, and for being information security advocates on behalf of the organization Ask about ways in which your department could help make their advocacy activities easier Remind them about the follow-up email contact at the two-week and four week points; Explain that follow-up email will have a few questions on how they are doing with their new advocacy behaviors Remind them on how to contact you or your office if they have any questions in the meantime Thank them again for participating in the study and sharing their ideas

Appendix 4: Pre-Test Introductory Questionnaire

Administered PRIOR to Facts Presentation (Treatment Part 1)



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study | Code:

School of Information Studies

343 Hinds Hall, Syracuse, New York 13244-1190
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Instructions

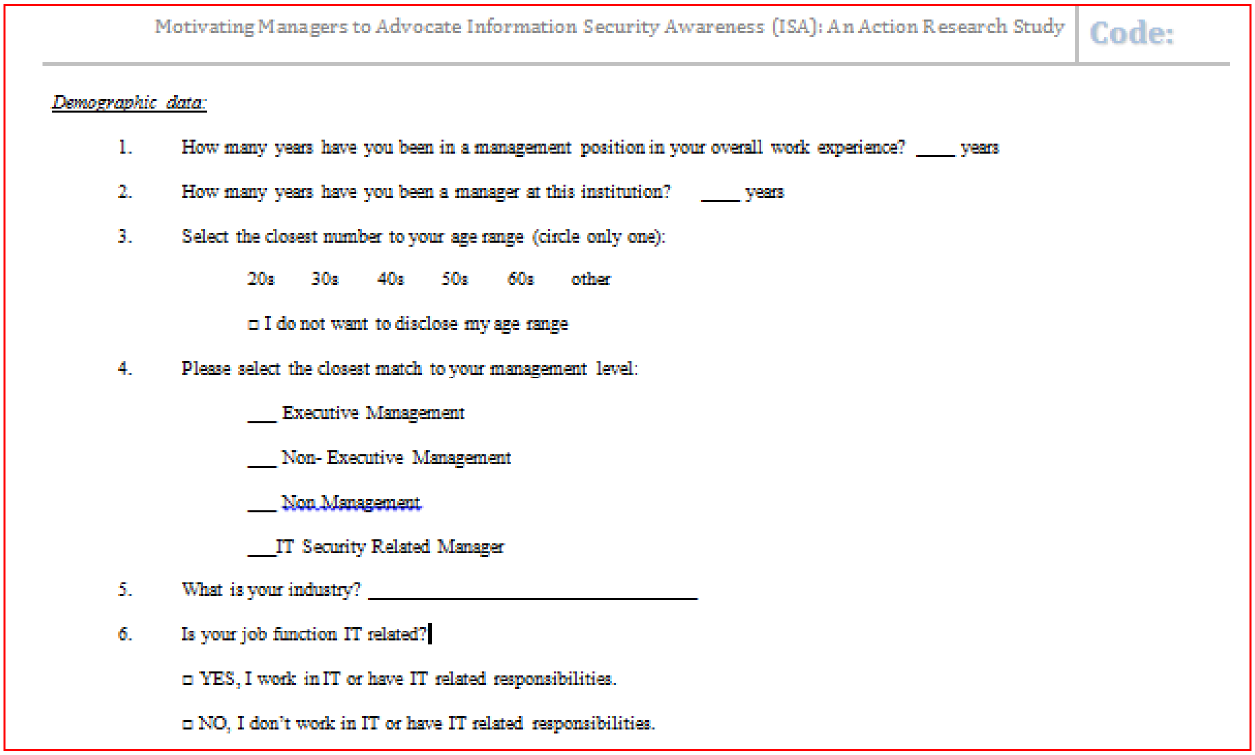
This questionnaire is part of the action research workshop studying influencing factors in favor of information security awareness (ISA) advocacy. The purpose of the following questions is to assess your personal perspective on advocacy behaviors and your level of information security knowledge and to collect demographic data. Your answers to this and follow-up questionnaires will allow us to compare whether this workshop is an effective way to generate change in IS advocacy behavior or knowledge.

We are interested in your opinions and actual actions not generic information, or what you feel you could be doing. It is okay if you are not doing any IS advocacy activity. Your responses are anonymous and are not shared; however, this form will allow matching to your follow-up questionnaires. As a reminder, your individual responses will only be seen by the researcher.

This questionnaire should take about 5-10 minutes to complete.

There are five main question areas:

- Demographics
- Your current Information Security Awareness (ISA) knowledge level
- Current sources of information about Information Security including perceptions of content, format, timing and value
- Your current comfort level related to Information Security learning
- Your advocacy experiences



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

Demographic data:

1. How many years have you been in a management position in your overall work experience? ____ years

2. How many years have you been a manager at this institution? ____ years

3. Select the closest number to your age range (circle only one):

   20s 30s 40s 50s 60s other

   □ I do not want to disclose my age range

4. Please select the closest match to your management level:

   ___ Executive Management

   ___ Non- Executive Management

   ___ Non Management

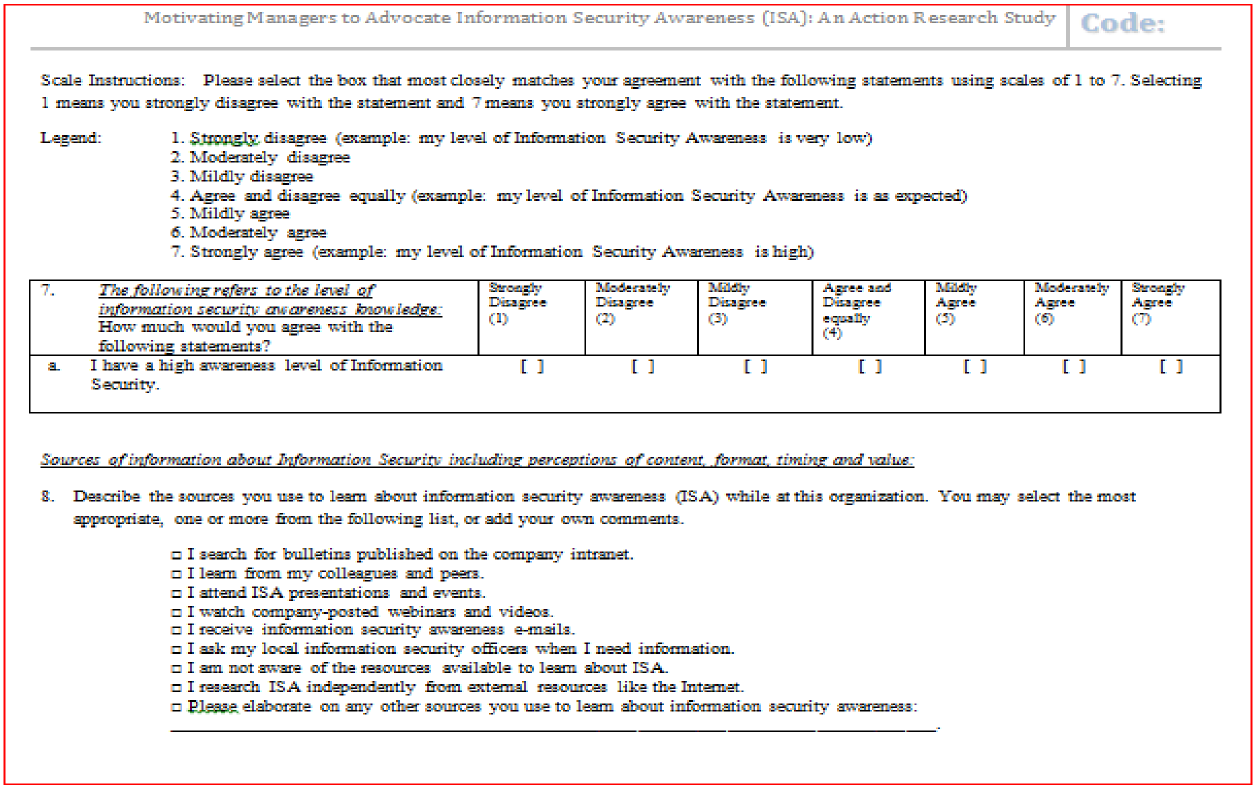
   ___IT Security Related Manager

5. What is your industry? ________________________________

6. Is your job function IT related?

   □ YES, I work in IT or have IT related responsibilities.

   □ NO, I don't work in IT or have IT related responsibilities.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

Scale Instructions: Please select the box that most closely matches your agreement with the following statements using scales of 1 to 7. Selecting 1 means you strongly disagree with the statement and 7 means you strongly agree with the statement.

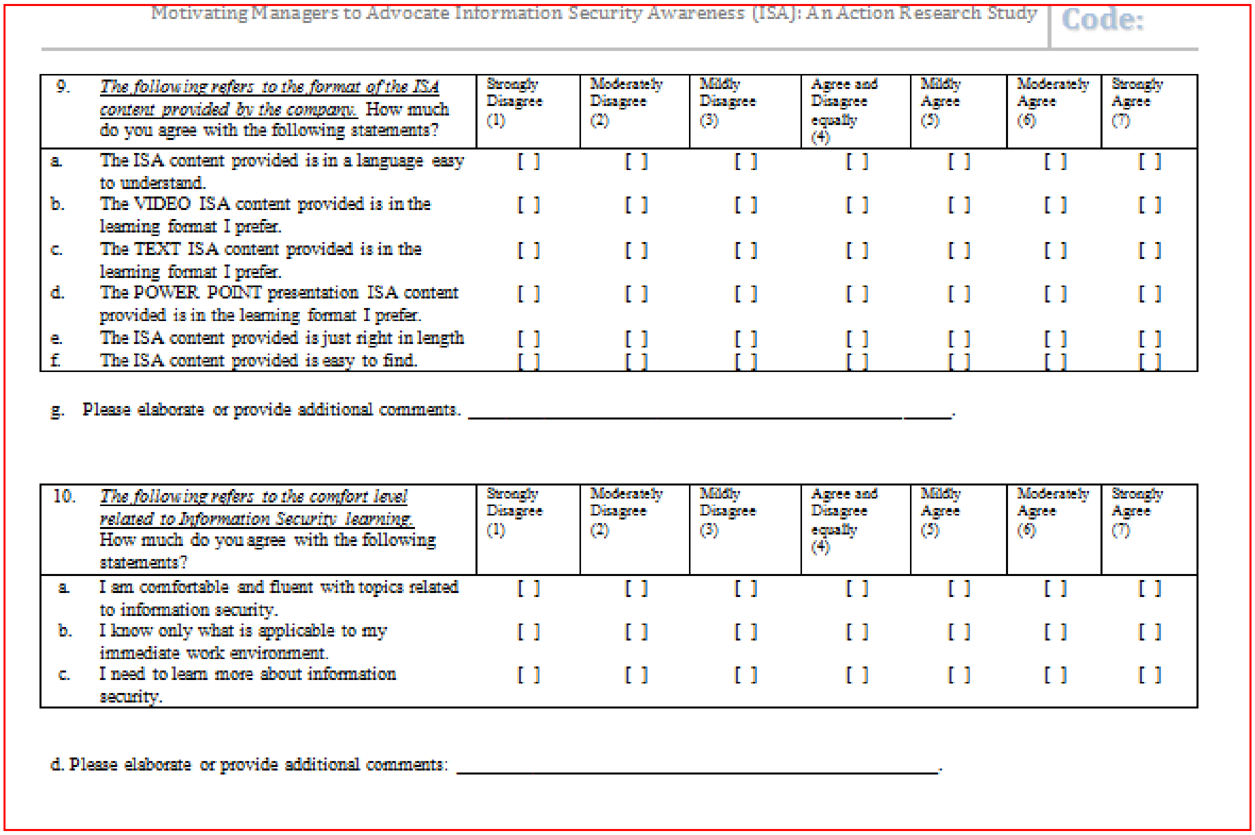
Legend:
1. Strongly disagree (example: my level of Information Security Awareness is very low)
2. Moderately disagree
3. Mildly disagree
4. Agree and disagree equally (example: my level of Information Security Awareness is as expected)
5. Mildly agree
6. Moderately agree
7. Strongly agree (example: my level of Information Security Awareness is high)

7.	*The following refers to the level of information security awareness knowledge:* How much would you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	I have a high awareness level of Information Security.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Sources of information about Information Security including perceptions of content, format, timing and value:

8. Describe the sources you use to learn about information security awareness (ISA) while at this organization. You may select the most appropriate, one or more from the following list, or add your own comments.

□ I search for bulletins published on the company intranet.
□ I learn from my colleagues and peers.
□ I attend ISA presentations and events.
□ I watch company-posted webinars and videos.
□ I receive information security awareness e-mails.
□ I ask my local information security officers when I need information.
□ I am not aware of the resources available to learn about ISA.
□ I research ISA independently from external resources like the Internet.
□ Please elaborate on any other sources you use to learn about information security awareness:
____.



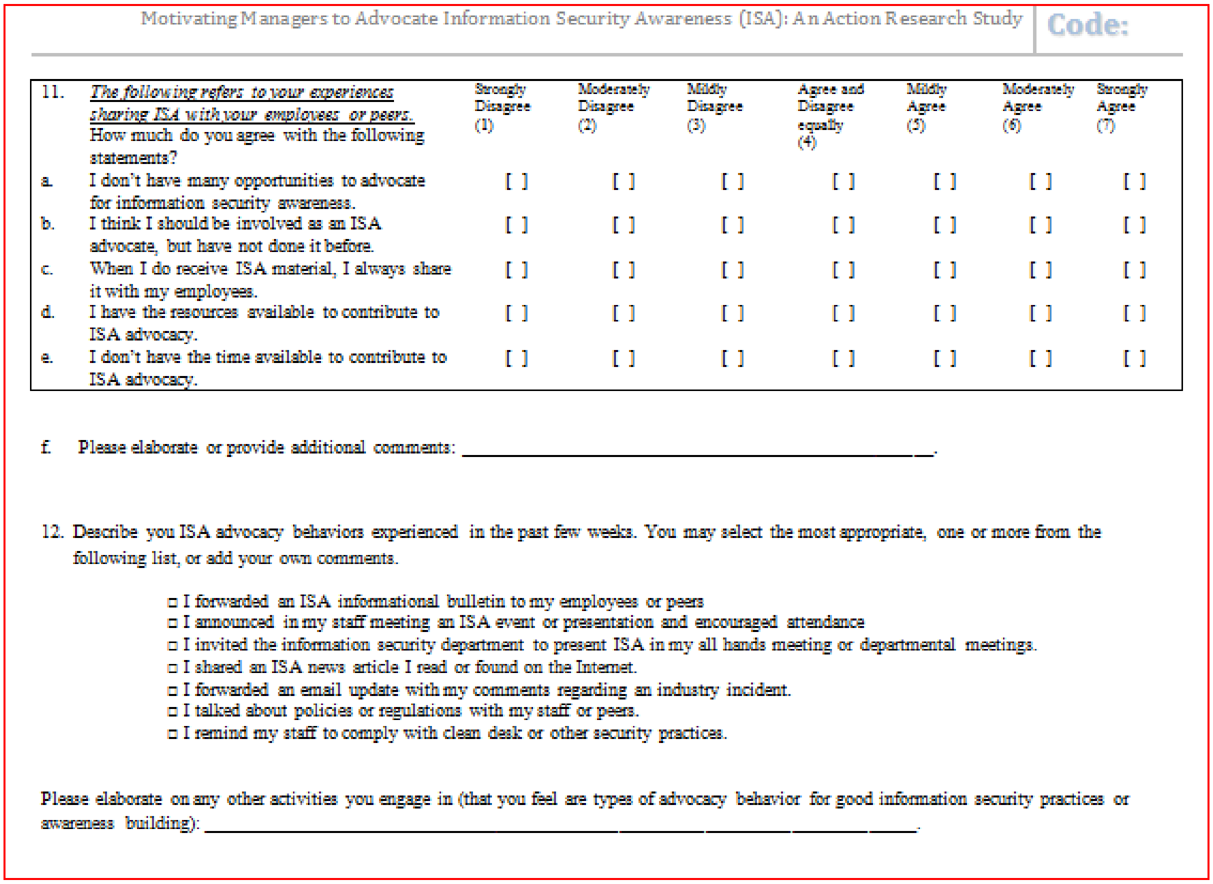
Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study | Code:

9.	*The following refers to the format of the ISA content provided by the company.* How much do you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	The ISA content provided is in a language easy to understand.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	The VIDEO ISA content provided is in the learning format I prefer.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	The TEXT ISA content provided is in the learning format I prefer.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
d.	The POWER POINT presentation ISA content provided is in the learning format I prefer.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
e.	The ISA content provided is just right in length	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
f.	The ISA content provided is easy to find.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

g. Please elaborate or provide additional comments. ____.

10.	*The following refers to the comfort level related to Information Security learning.* How much do you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	I am comfortable and fluent with topics related to information security.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	I know only what is applicable to my immediate work environment.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	I need to learn more about information security.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

d. Please elaborate or provide additional comments: ____.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study | Code:

		Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
11.	*The following refers to your experiences sharing ISA with your employees or peers.* How much do you agree with the following statements?							
a.	I don't have many opportunities to advocate for information security awareness.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	I think I should be involved as an ISA advocate, but have not done it before.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	When I do receive ISA material, I always share it with my employees.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
d.	I have the resources available to contribute to ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
e.	I don't have the time available to contribute to ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

f. Please elaborate or provide additional comments: ____.

12. Describe you ISA advocacy behaviors experienced in the past few weeks. You may select the most appropriate, one or more from the following list, or add your own comments.

□ I forwarded an ISA informational bulletin to my employees or peers
□ I announced in my staff meeting an ISA event or presentation and encouraged attendance
□ I invited the information security department to present ISA in my all hands meeting or departmental meetings.
□ I shared an ISA news article I read or found on the Internet.
□ I forwarded an email update with my comments regarding an industry incident.
□ I talked about policies or regulations with my staff or peers.
□ I remind my staff to comply with clean desk or other security practices.

Please elaborate on any other activities you engage in (that you feel are types of advocacy behavior for good information security practices or awareness building): ____.

Appendix 5: Treatment Part 1: Facts

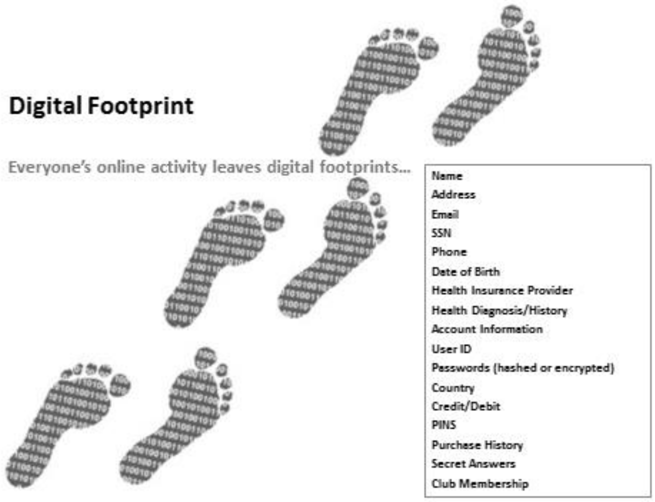
Facts to present motivating facts to inform and engage:

You have been invited because you serve in a management capacity in some aspect of our organization, but do not have specific responsibility for Information Security. In fact, information my job and the job of other specialized IT professionals.

The following describes the type of facts that was presented to the large group during the Action Research Workshop. These are facts, not made up stories. The goal is to share with you a problem we still have and ask for your ideas on how managers such as your selves might contribute to helping us with it. The facts I am about to present will hopefully convince you of the importance of information security activities, the importance of IS awareness on the part of your subordinates, peers, and even superiors, and the importance of your own *advocacy behaviors* on behalf of the company. After the presentation, you are welcome to ask questions.

Artifact Presentation Description

These slides are just sample extracted from the ISA presentation. The following slide introduced the term Digital Footprints to the audience. During the narrative, I expanded on the definition of the term as traces of information an online user leaves behind when conducting common online activity such as email, shopping, etc.

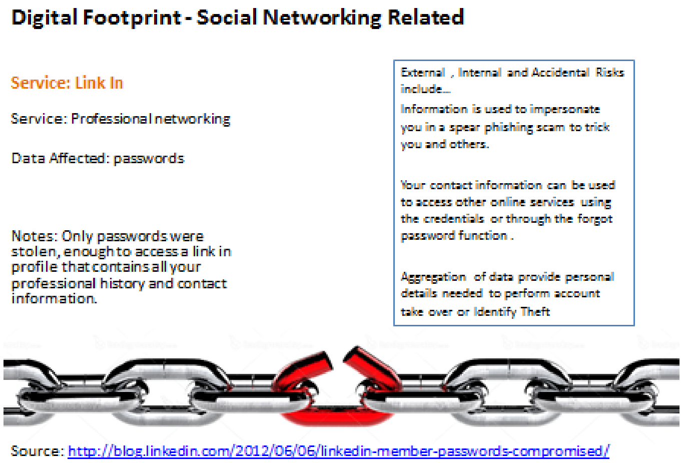


Digital Footprint

Everyone's online activity leaves digital footprints...

Name
Address
Email
SSN
Phone
Date of Birth
Health Insurance Provider
Health Diagnosis/History
Account Information
User ID
Passwords (hashed or encrypted)
Country
Credit/Debit
PINS
Purchase History
Secret Answers
Club Membership

The following is an example slide of an industry breach. It includes the source (external threat), perpetrator (online attacker), the intent (to obtain user information), and the consequence (information disclosure).



Digital Footprint - Social Networking Related

Service: Link In

Service: Professional networking

Data Affected: passwords

Notes: Only passwords were stolen, enough to access a link in profile that contains all your professional history and contact information.

External , Internal and Accidental Risks include...

Information is used to impersonate you in a spear phishing scam to trick you and others.

Your contact information can be used to access other online services using the credentials or through the forgot password function .

Aggregation of data provide personal details needed to perform account take over or Identify Theft

Source: http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

Digital Footprint - Online Purchasing

Service: Zappos Online Retail, owned by Amazon

Data Affected: your name, e-mail address, billing and shipping addresses, phone number, the last four digits of your credit card number, and/or your cryptographically scrambled password (but not your actual password).

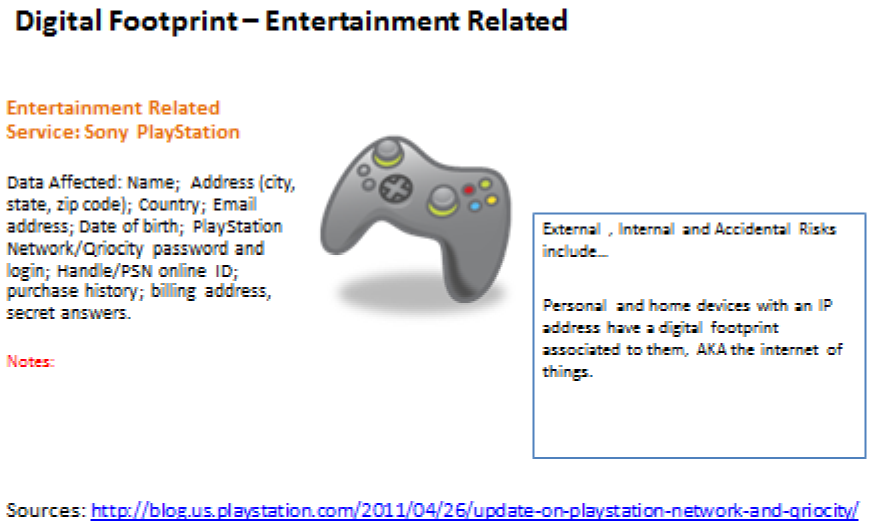
Notes: Zappos did not encrypt its customers' e-mail and shipping addresses, phone numbers, the last four digits of the payment card because as it is not required by the PCI-DSS rules.

Source: http://blogs.zappos.com/securityemail

External , Internal and Accidental Risks include...

Email account takeover is a gateway to many online services.

Aggregate data is used to validate a service account, activate a credit card, forward your phone calls and change something like your shipping address.



Digital Footprint – Entertainment Related

Entertainment Related
Service: Sony PlayStation

Data Affected: Name; Address (city, state, zip code); Country; Email address; Date of birth; PlayStation Network/Qriocity password and login; Handle/PSN online ID; purchase history; billing address, secret answers.

Notes:

External , Internal and Accidental Risks include...

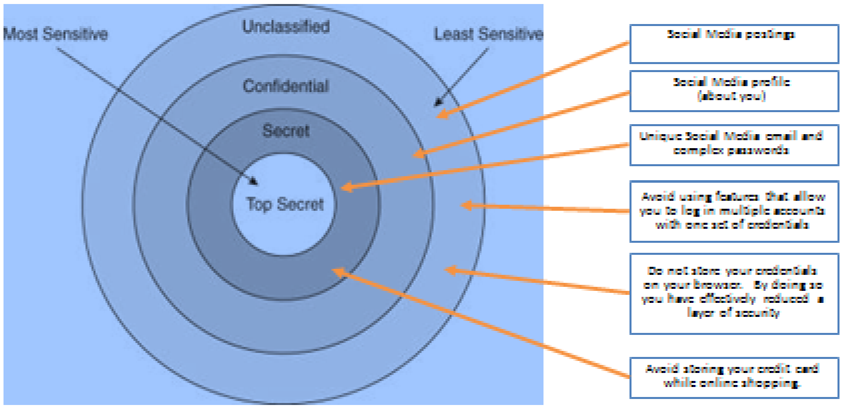
Personal and home devices with an IP address have a digital footprint associated to them, AKA the internet of things.

Sources: http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/

Attack Motivators

- Financial gain
- Hacktivism
- Reputation
- Competitive Advantage
- Identity theft
- Stolen goods
- Revenge

Think about the true value of your information



Social Media postings

Social Media profile (about you)

Unique Social Media email and complex passwords

Avoid using features that allow you to log in multiple accounts with one set of credentials

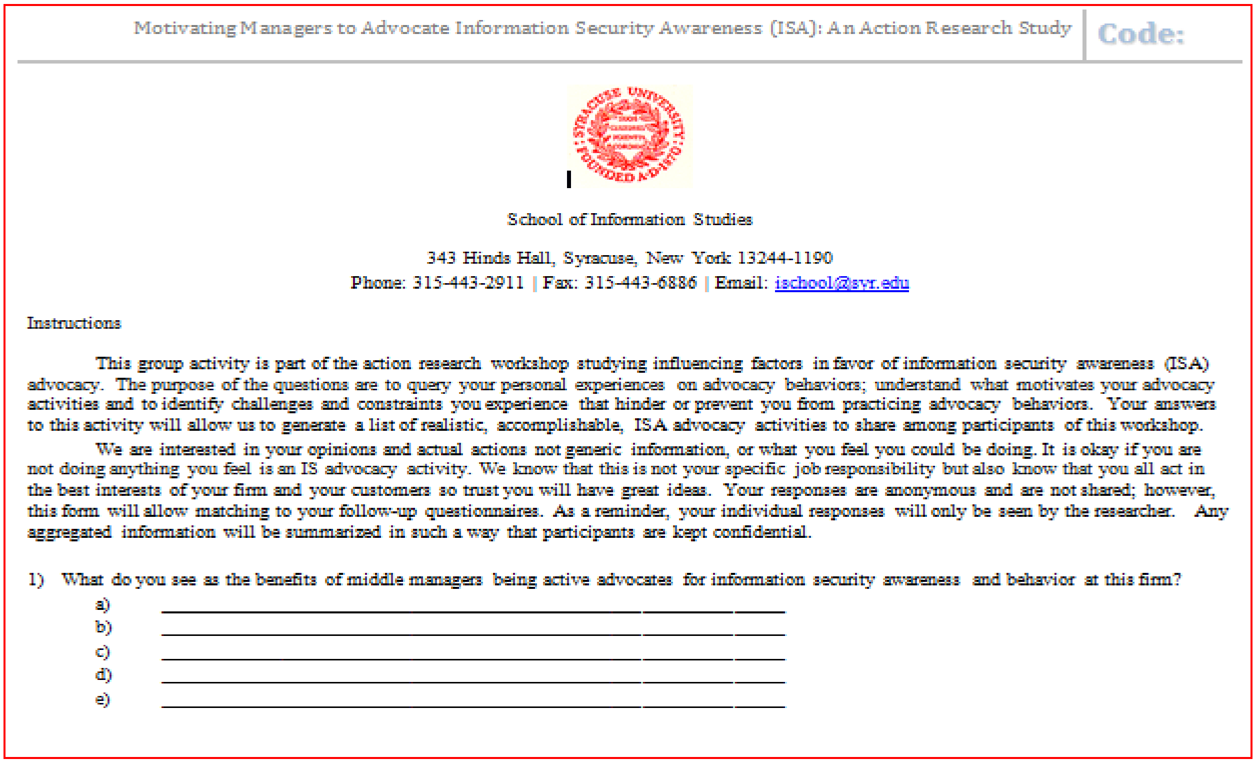
Do not store your credentials on your browser. By doing so you have effectively reduced a layer of security

Avoid storing your credit card while online shopping.

Does anyone have any questions about the presentation?

Appendix 6: Treatment Part 2: Action Research, Action Exercise

Groups work to develop actionable items related to security awareness behaviors.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

School of Information Studies

343 Hinds Hall, Syracuse, New York 13244-1190
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Instructions

This group activity is part of the action research workshop studying influencing factors in favor of information security awareness (ISA) advocacy. The purpose of the questions are to query your personal experiences on advocacy behaviors; understand what motivates your advocacy activities and to identify challenges and constraints you experience that hinder or prevent you from practicing advocacy behaviors. Your answers to this activity will allow us to generate a list of realistic, accomplishable, ISA advocacy activities to share among participants of this workshop.

We are interested in your opinions and actual actions not generic information, or what you feel you could be doing. It is okay if you are not doing anything you feel is an IS advocacy activity. We know that this is not your specific job responsibility but also know that you all act in the best interests of your firm and your customers so trust you will have great ideas. Your responses are anonymous and are not shared; however, this form will allow matching to your follow-up questionnaires. As a reminder, your individual responses will only be seen by the researcher. Any aggregated information will be summarized in such a way that participants are kept confidential.

1) What do you see as the benefits of middle managers being active advocates for information security awareness and behavior at this firm?

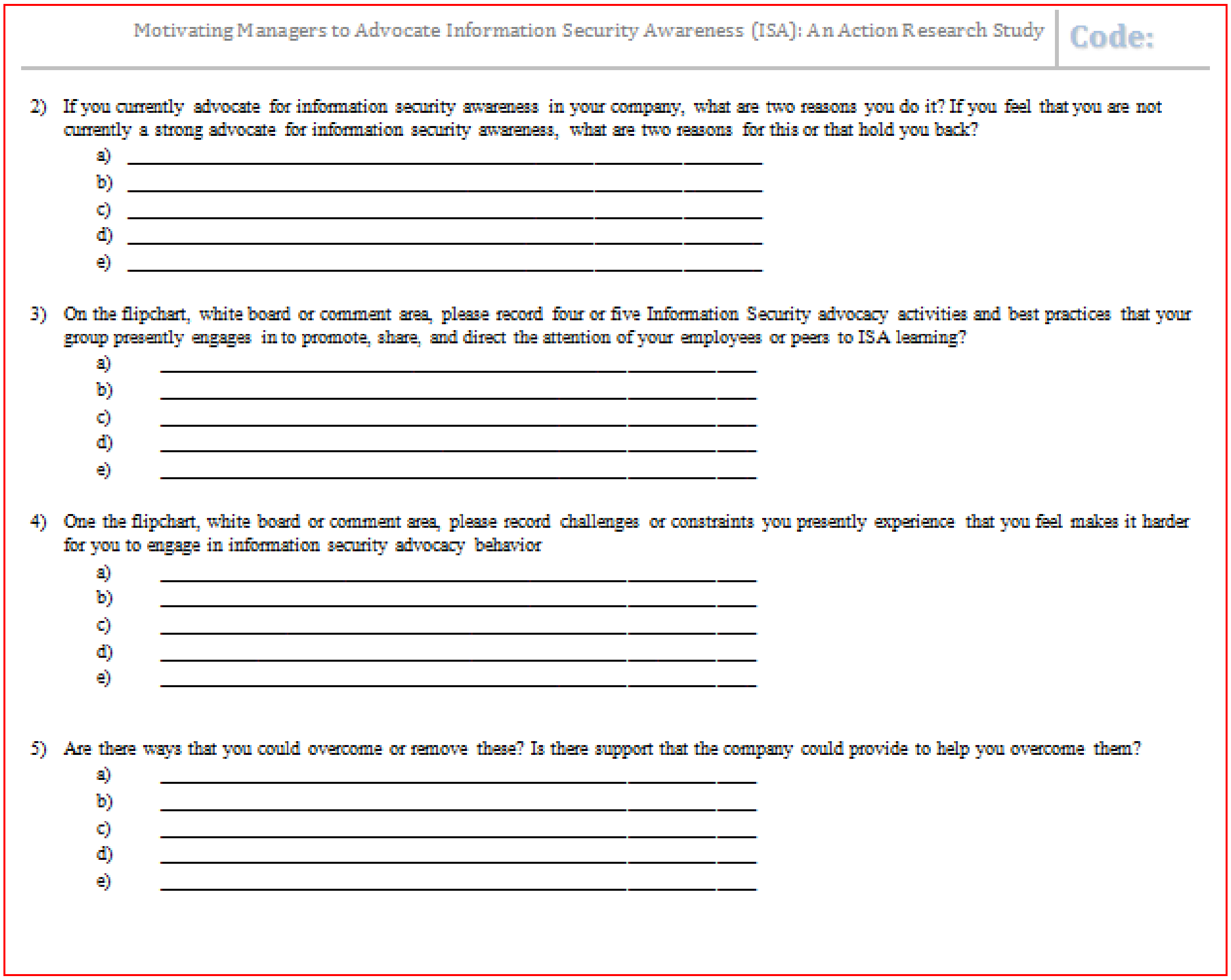
a) ____

b) ____

c) ____

d) ____

e) ____



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

2) If you currently advocate for information security awareness in your company, what are two reasons you do it? If you feel that you are not currently a strong advocate for information security awareness, what are two reasons for this or that hold you back?

a) ______________________________
b) ______________________________
c) ______________________________
d) ______________________________
e) ______________________________

3) On the flipchart, white board or comment area, please record four or five Information Security advocacy activities and best practices that your group presently engages in to promote, share, and direct the attention of your employees or peers to ISA learning?

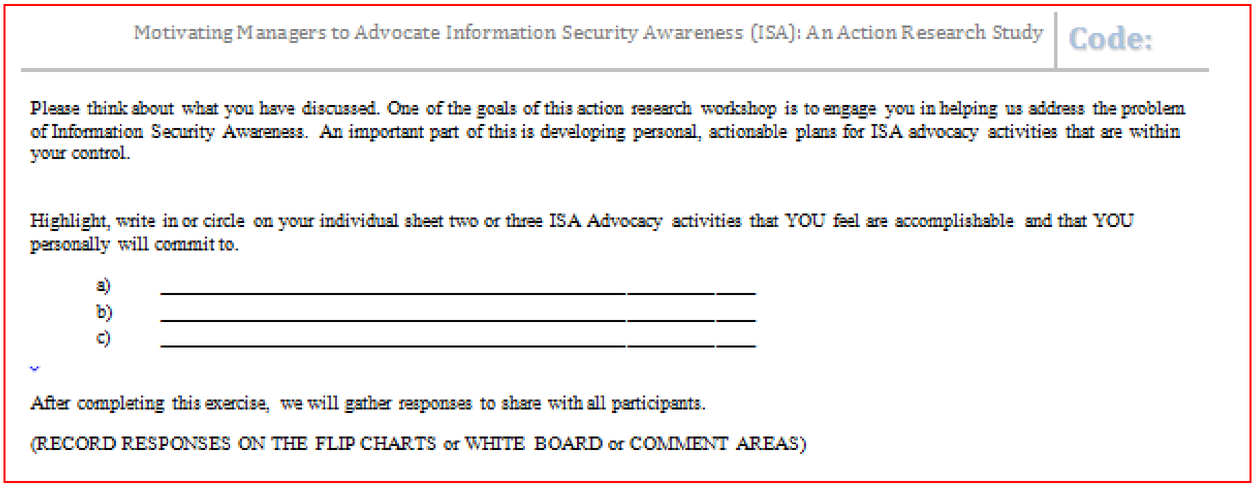
a) ______________________________
b) ______________________________
c) ______________________________
d) ______________________________
e) ______________________________

4) One the flipchart, white board or comment area, please record challenges or constraints you presently experience that you feel makes it harder for you to engage in information security advocacy behavior

a) ______________________________
b) ______________________________
c) ______________________________
d) ______________________________
e) ______________________________

5) Are there ways that you could overcome or remove these? Is there support that the company could provide to help you overcome them?

a) ______________________________
b) ______________________________
c) ______________________________
d) ______________________________
e) ______________________________



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

Please think about what you have discussed. One of the goals of this action research workshop is to engage you in helping us address the problem of Information Security Awareness. An important part of this is developing personal, actionable plans for ISA advocacy activities that are within your control.

Highlight, write in or circle on your individual sheet two or three ISA Advocacy activities that YOU feel are accomplishable and that YOU personally will commit to.

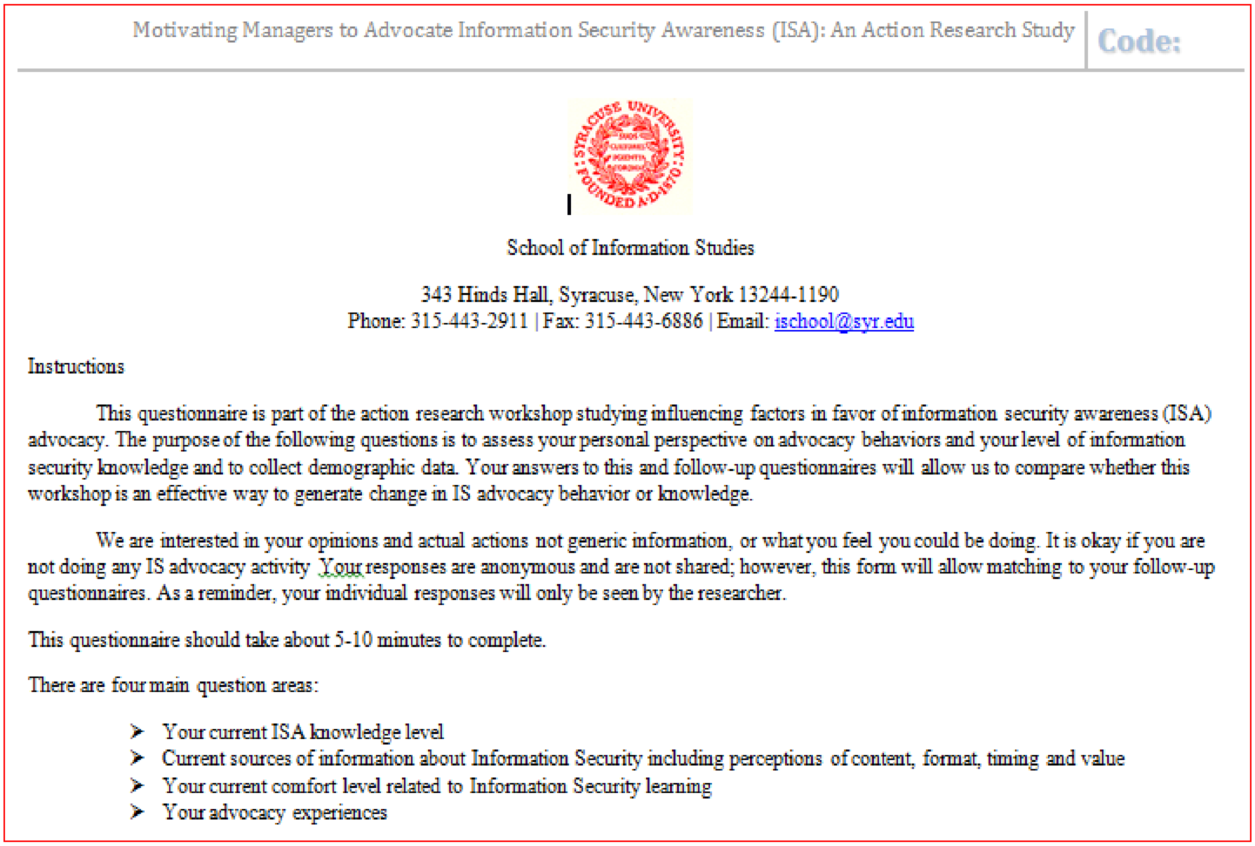
a) ______________________________
b) ______________________________
c) ______________________________

After completing this exercise, we will gather responses to share with all participants.

(RECORD RESPONSES ON THE FLIP CHARTS or WHITE BOARD or COMMENT AREAS)

Appendix 7: Post-Test 1 – Questionnaire at End of Workshop

Administered AFTER the Action Research, Action Exercise (Treatment Part 2)



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study | **Code:**

School of Information Studies

343 Hinds Hall, Syracuse, New York 13244-1190
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Instructions

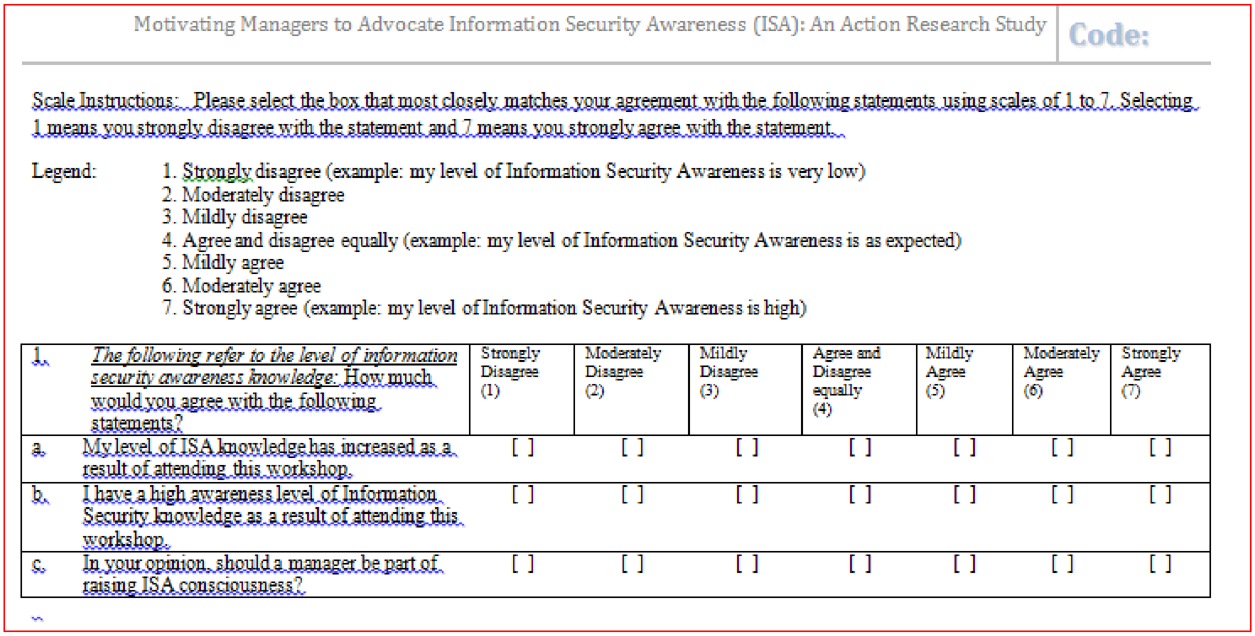
This questionnaire is part of the action research workshop studying influencing factors in favor of information security awareness (ISA) advocacy. The purpose of the following questions is to assess your personal perspective on advocacy behaviors and your level of information security knowledge and to collect demographic data. Your answers to this and follow-up questionnaires will allow us to compare whether this workshop is an effective way to generate change in IS advocacy behavior or knowledge.

We are interested in your opinions and actual actions not generic information, or what you feel you could be doing. It is okay if you are not doing any IS advocacy activity Your responses are anonymous and are not shared; however, this form will allow matching to your follow-up questionnaires. As a reminder, your individual responses will only be seen by the researcher.

This questionnaire should take about 5-10 minutes to complete.

There are four main question areas:

- Your current ISA knowledge level
- Current sources of information about Information Security including perceptions of content, format, timing and value
- Your current comfort level related to Information Security learning
- Your advocacy experiences

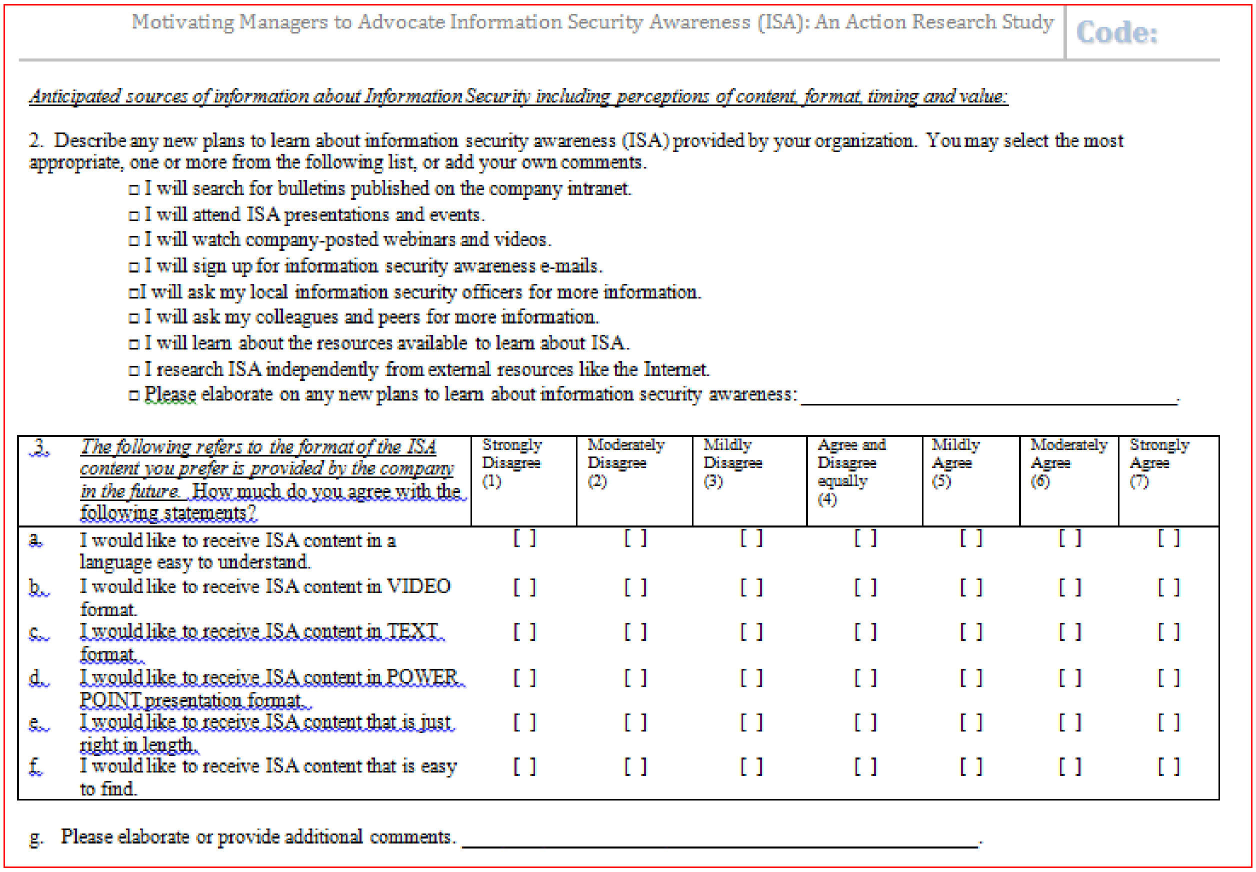


Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study | **Code:**

Scale Instructions: Please select the box that most closely matches your agreement with the following statements using scales of 1 to 7. Selecting 1 means you strongly disagree with the statement and 7 means you strongly agree with the statement.

Legend:
1. Strongly disagree (example: my level of Information Security Awareness is very low)
2. Moderately disagree
3. Mildly disagree
4. Agree and disagree equally (example: my level of Information Security Awareness is as expected)
5. Mildly agree
6. Moderately agree
7. Strongly agree (example: my level of Information Security Awareness is high)

1.	*The following refer to the level of information security awareness knowledge:* How much would you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	My level of ISA knowledge has increased as a result of attending this workshop.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	I have a high awareness level of Information Security knowledge as a result of attending this workshop.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	In your opinion, should a manager be part of raising ISA consciousness?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

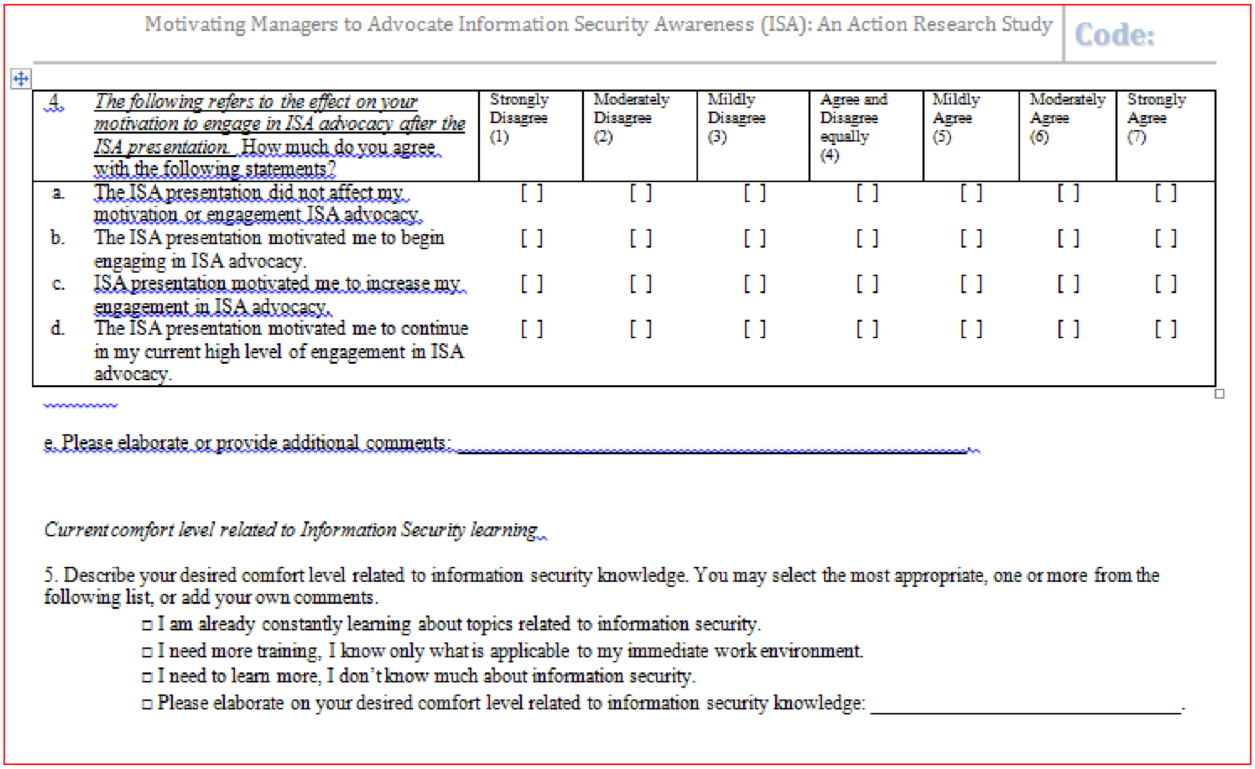
Anticipated sources of information about Information Security including perceptions of content, format, timing and value:

2. Describe any new plans to learn about information security awareness (ISA) provided by your organization. You may select the most appropriate, one or more from the following list, or add your own comments.

□ I will search for bulletins published on the company intranet.
□ I will attend ISA presentations and events.
□ I will watch company-posted webinars and videos.
□ I will sign up for information security awareness e-mails.
□I will ask my local information security officers for more information.
□ I will ask my colleagues and peers for more information.
□ I will learn about the resources available to learn about ISA.
□ I research ISA independently from external resources like the Internet.
□ Please elaborate on any new plans to learn about information security awareness: ______________________________.

3.	*The following refers to the format of the ISA content you prefer is provided by the company in the future.* How much do you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	I would like to receive ISA content in a language easy to understand.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	I would like to receive ISA content in VIDEO format.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	I would like to receive ISA content in TEXT format.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
d.	I would like to receive ISA content in POWER POINT presentation format.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
e.	I would like to receive ISA content that is just right in length.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
f.	I would like to receive ISA content that is easy to find.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

g. Please elaborate or provide additional comments. ____.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

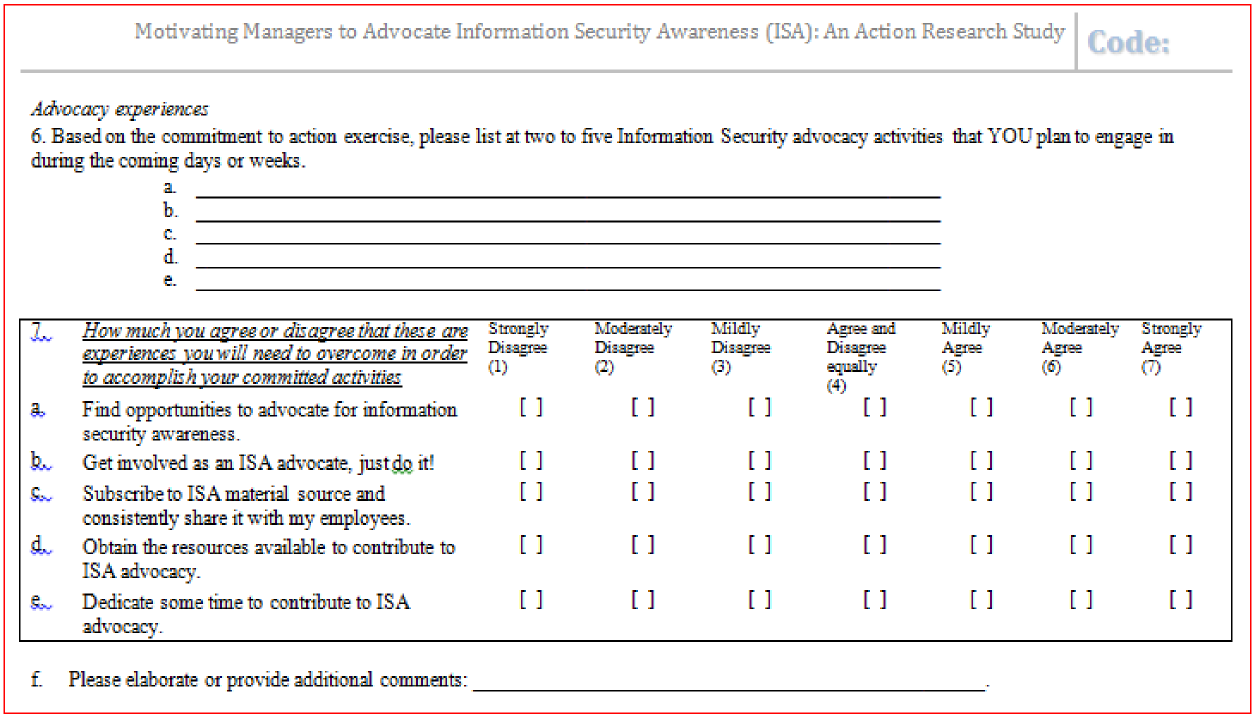
4.	*The following refers to the effect on your motivation to engage in ISA advocacy after the ISA presentation.* How much do you agree with the following statements?	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	The ISA presentation did not affect my motivation or engagement ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	The ISA presentation motivated me to begin engaging in ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	ISA presentation motivated me to increase my engagement in ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
d.	The ISA presentation motivated me to continue in my current high level of engagement in ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

e. Please elaborate or provide additional comments: ____.

Current comfort level related to Information Security learning.

5. Describe your desired comfort level related to information security knowledge. You may select the most appropriate, one or more from the following list, or add your own comments.

□ I am already constantly learning about topics related to information security.
□ I need more training, I know only what is applicable to my immediate work environment.
□ I need to learn more, I don't know much about information security.
□ Please elaborate on your desired comfort level related to information security knowledge: ________________________.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

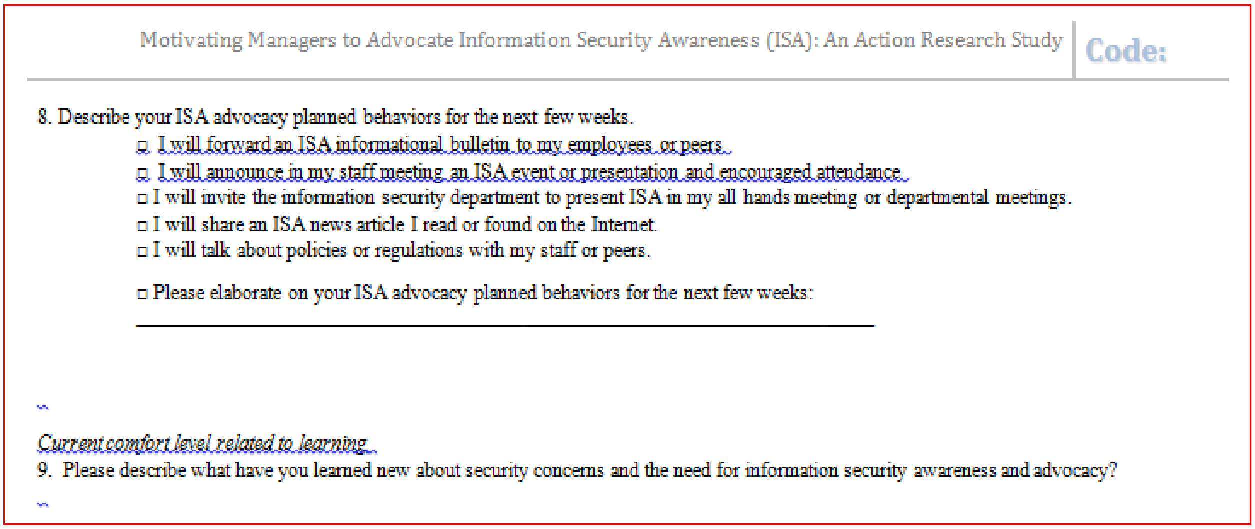
Advocacy experiences

6. Based on the commitment to action exercise, please list at two to five Information Security advocacy activities that YOU plan to engage in during the coming days or weeks.

a. ____
b. ____
c. ____
d. ____
e. ____

7.	*How much you agree or disagree that these are experiences you will need to overcome in order to accomplish your committed activities*	Strongly Disagree (1)	Moderately Disagree (2)	Mildly Disagree (3)	Agree and Disagree equally (4)	Mildly Agree (5)	Moderately Agree (6)	Strongly Agree (7)
a.	Find opportunities to advocate for information security awareness.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
b.	Get involved as an ISA advocate, just do it!	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
c.	Subscribe to ISA material source and consistently share it with my employees.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
d.	Obtain the resources available to contribute to ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
e.	Dedicate some time to contribute to ISA advocacy.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

f. Please elaborate or provide additional comments: ____.



Motivating Managers to Advocate Information Security Awareness (ISA): An Action Research Study **Code:**

8. Describe your ISA advocacy planned behaviors for the next few weeks.

□ I will forward an ISA informational bulletin to my employees or peers.
□ I will announce in my staff meeting an ISA event or presentation and encouraged attendance.
□ I will invite the information security department to present ISA in my all hands meeting or departmental meetings.
□ I will share an ISA news article I read or found on the Internet.
□ I will talk about policies or regulations with my staff or peers.

□ Please elaborate on your ISA advocacy planned behaviors for the next few weeks:
____

Current comfort level related to learning

9. Please describe what have you learned new about security concerns and the need for information security awareness and advocacy?

Appendix 8: Facilitator's Closing Script

The researcher follows the script to set expectations for follow-ups.

It has been a learning opportunity to hear your opinions and feedback on this matter.

Before we close, I wonder if you have any additional thoughts on how the organization could better support your information security advocacy activities or those of your staff.

(LEAD DISCUSSION AND DOCUMENT IDEAS)

Thank you. That is very helpful

As a reminder, I will be sending two follow-up e-mails with similar questions about your individual engagements in information security advocacy.

The first e-mail will be sent in two weeks' time, and the second will be sent in four weeks' time.

Your responses are very important and beneficial for completing the research.

Your participations will contribute to understanding Information Security advocacy.

For those willing to share additional thoughts, ideas, and concerns, I would like to invite you to participate in an interview about management's role in ISA advocacy. I will send an interview meeting invitation. Please remember that your participation is voluntary.

Thank you again and I look forward to your feedback when I reach out to you in two weeks.

Appendix 9: Post-Test 2 – Three -Week Follow-up:

Commitment to Change Questionnaire

Thank you for participating in the information security advocacy action research workshop. The feedback, comments, and suggestions are valuable data that will be considered for the organization's improvement of ISA best practices. The purpose of this e-mail is to gather follow-up thoughts, ideas, and concerns regarding security and information security awareness advocacy.

Based on your ISA workshop participation, please express your feedback on the workshop and share your ideas on how to promote information security awareness, as well as your experiences in contributing to ISA advocacy. Please answer the following questions:

1. Based on the commitment to action exercise, please list at two to five Information Security advocacy activities that YOU have engage in the last few weeks.
   a. ______________________________

   b. ______________________________

   c. ______________________________

   d. ______________________________

   e. ______________________________

2. Describe any new or continued approaches since the ISA workshop to learning about information security awareness (ISA). You may select the most appropriate answer or add your own comments.

NEW ☐ Continued ☐ I search for bulletins published on the company intranet.

NEW ☐ Continued ☐ I currently attend ISA presentations and events.

NEW ☐ Continued ☐ I watch company-posted webinars and videos.

NEW ☐ Continued ☐ I sign up for information security awareness e-mails.

NEW ☐ Continued ☐ I ask my local information security officers for more information.

NEW ☐ Continued ☐ I ask my peers or colleagues about ISA.

NEW ☐ Continued ☐ I learn about ISA independently from external resources like the Internet.

Please elaborate or provide additional comments. ____

Appendix 10: Post-Test 3 – Six -Week Follow-up:

Commitment to Change Questionnaire

Thank you for participating in the information security advocacy action research workshop. The feedback, comments, and suggestions are valuable data that will be considered for the organization's improvement of ISA best practices. The purpose of this e-mail is to gather follow-up thoughts, ideas, and concerns regarding security and information security awareness advocacy.

Based on your ISA workshop participation, please express your feedback on the workshop and share your ideas on how to promote information security awareness, as well as your experiences in contributing to ISA advocacy. Please answer the following questions:

1. Based on the commitment to action exercise, please list at two to five Information Security advocacy activities that YOU have engage in the last few weeks.
   a. ____
   b. ____
   c. ____
   d. ____
   e. ____

2. Describe any new or continued approaches since the ISA workshop to learning about information security awareness (ISA). You may select the most appropriate answer or add your own comments.

NEW ☐ Continued ☐ I search for bulletins published on the company intranet.

NEW ☐ Continued ☐ I currently attend ISA presentations and events.

NEW ☐ Continued ☐ I watch company-posted webinars and videos.

NEW ☐ Continued ☐ I sign up for information security awareness e-mails.

NEW ☐ Continued ☐ I ask my local information security officers for more information.

NEW ☐ Continued ☐ I ask my peers or colleagues about ISA.

NEW □ Continued □ I learn about ISA independently from external resources like the Internet.

Please elaborate or provide additional comments.

____

Appendix 11: Sample Consent Form (IRB approved)

School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-1190
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Project Title: Motivating Non-IT Security Middle Managers to Advocate Information Security Awareness (ISA): An Action Research Study

My name is Grace Giraldo, and I am a doctoral student at Syracuse University iSchool of Information Studies. I am inviting you to participate in a research study. Involvement in the study is voluntary, so you may choose to participate or not. This sheet will explain the study to you and please feel free to ask questions about the research if you have any. I will be happy to explain anything in detail if you wish.

I am interested in learning more about specific environment and social conditions that when coupled with quality awareness artifacts have influence and motivate middle managers in favor of Information Security Awareness (ISA) advocacy. Furthermore, this inquiry investigates how we can engage non-security management in advocating for IT security behavior among their direct reports and peers.

You will be asked to participate in an Action Research Workshop where I will be asking for personal opinions and to recount actions related to information security awareness and the role of our non-IT managers. After the workshop, I am asking you respond to two follow-up emails. The workshop will take approximately 1.5 hours. The follow-up emails will each take only 5-10 minutes to complete.

All information will be kept confidential, only the researcher (myself) will be able to see your individual information. In any academic articles I write or any professional presentations that I make, I will use a made-up or coded name for participants, and I will not reveal individual details. I will also change details about where you work and refer to the organization as a large financial institution.

Confidentiality cannot be guaranteed when participants work in group settings. Other participants in your group will hear your opinions and will know how you answer questions. While we will discourage anyone from sharing this information outside of the group, we cannot guarantee confidentiality by other group members**.** We will do our best to keep all of your personal information private and confidential, but absolute confidentiality cannot be guaranteed. Please be reassured that the topic of this workshop is developmental, rather than critical. We are looking for ideas about how to improve our information security awareness activities with the help of managers such as you. Your ideas are important to us.

This study involves the audio recording of the group action research workshop facilitated by the researcher. Neither your name nor any other identifying information will be associated with the audio recording or the transcript. Only the researcher will be able to listen to the recordings. Audio tapes will be transcribed by the researcher and/or 3rd party transcriptionist service and erased once the transcriptions are checked for accuracy. Transcripts of the group discussions will be used for data analysis. The transcripts may be reproduced in whole or in part for use in presentations or written products that result from this study. Neither your name nor any other identifying information (such as your voice or picture) will be used in presentations or in written products resulting from the study.

If you have any questions, concerns, or complaints about the research, contact the research chair Dr. Michelle Kaarst-Brown (315-559-2451) or the researcher Grace Giraldo (302-740-1779). If you have any questions about your rights as a research participant, you have questions, concerns, or complaints that you wish to address to someone other than the investigator, or if you cannot reach the investigator, contact the Syracuse University Institutional Review Board at 315-443-3013.

All of my questions have been answered, I am 18 years of age or older, and I wish to participate in this research study. I have received a copy of this consent form. (If consenting electronically, please *print a copy for your records.)*

___ I agree to be audio recorded as one of many voices in the group discussion.

___ I do not agree to be audio recorded, but am willing to participate in small group discussions and am willing to write down my responses to questions in order to participate in large group discussions.

___ I do not agree to be audio recorded and so cannot participate in the workshop at this time.

Only for electronic consent, include:

By replying to this email, I agree to participate in this research study and understand the terms of informed consent. I agree that I will sign a hard copy of this consent form at the workshop.

____ ________________________
Signature of participant Date

____
Printed name of participant

____ ________________________
Signature of researcher Date

Grace Giraldo
Printed name of researcher

Appendix 12: Resume of Professional Experience

901 Glen Falls Ct
Newark, DE 19711
(302) 282-3145, (302) 740-1779
GGiraldo@SYR.EDU

Grace Giraldo

MS, CISSP, CCNA, CCDA, MCSE

Summary

- Information Risk Manager, Technology Program Manager, Team Leader, IT Analyst
- CISSP#105192, CCNA/CCDA
- Certified Information Systems Security Professional #105192
  Languages: English and Spanish (speak, read, and write)

Education

- Master of Science, Marshall University in Huntington, WV: 1992–1999
  Major: Management Information Systems
- BS Computer Science, Inter American University in San Juan, PR, 1982 – 1987
  Major: Computer Science
  Certifications and Training

- Managing Multiple IT Projects
- Project Management for Information Systems
- Getting Results without Authority
- Principles of Application Development (Project Management Training) – Microsoft Framework
- MCSE, MCP+I, Win NT, Win 2K Professional and Server Certifications
- Security + (Server security)
- Cisco Certified Network Assoc. (CCNA) Certification #CSCO10388132
- Cisco Certified Design Assoc. (CCDA) Certification
  Experience

8/2006 – Present: Information Risk Lead, JP Morgan Chase, Wilmington, DE

- Manage and support security checkpoints during project life cycle.
- Advise management and line of business risk managers on specific application compliance and technologies to ensure best practices and security goals.

- Ensure IT risk standards are met: Provide consulting, security strategy and operational support to cross-functional security activities and project teams, including infrastructure compliance, vulnerability identification and remediation, policy development, and infrastructure security.
- Offer application security support for Third Party Oversight (Vendor) risk assessments.
- Serve as Subject Matter Expert for online credit card and related products.
- Provide hands-on security testing for internal applications.
- Offer test management, forecast, budget, and compliance validation for external applications.
- Provide exceptional communication and interpersonal skills. Demonstrate strong leadership to both internal and external contacts with strong team orientation, analytical aptitude, business acumen, and problem-solving skills.

4/2003 – 8/2006: Technical Program Manager (Tech Lead), JP Morgan Chase, Wilmington, DE

- Disaster Recovery Program Lead – Developed, piloted, and implemented online applications Disaster Recovery (DR) program for the Corporate Internet Group (CIG). Provided ongoing program maintenance and execution to ensure all online applications had a DR executable plan. Served as leader of DR team, chair of weekly project meetings, and representative to corporate DR program. I prepared and presented workload goals, objectives, status, and results on a monthly basis.
- Served as technical liaison and project representative for CIG's Technical Operations network and infrastructure team. I communicated with external and internal business partners about technical needs.
- Application Development Analyst – Managed projects intended to maximize efficiencies and save on operations costs. Ensured the overall success of development projects.
- Ensured technical infrastructure standards were met, including high availability, disaster recovery planning, storage solutions, and security requirements.
- Provided the scope of technical requirements and hardware estimates for infrastructure.
- Managed the technical and business relationships and service levels.
- Supported developers and implementer requests throughout projects.
- Documented operational tasks and functions, and managed troubleshooting information.

2/2002 – 4/2003: Sr. Infrastructure Architect, Wilmington Savings Fund Society, Wilmington,

DE

- Managed the Enterprise Windows 2000 Active Directory design, and project implementation.
    - Planned and led the implementation team in the infrastructure migration of Novel 4 to Windows 2000 Active Directory.
    - Configured and supported knowledge base desktop, servers and production web, database, and file-print servers.
    - Evaluated, tested, and deployed software, system upgrades, and security patches.
    - Implemented best practices for tested labs and changed control to ensure quality of deployments.

    - Implemented standard server image and rolled out servers to 26 retail branches, laying out infrastructure foundation necessary for a bank-wide software system conversion to a new vendor.
- Proposed and managed project to implement the use of ISDN service for network disaster recovery.
- Proposed project and implemented the use of centralized UPS for Operations Computing Center.
- Managed vendor deployment of network communication between the bank and the vendor's primary processing location.

9/2000 – 9/2001, Director of IT Operations and IT Infrastructure, eMoneyAdvisor, Inc., Paoli,

PA

- Served as Technical Lead for infrastructure operations (servers, network, and desktops). Managing End-to-End Information Technology.
- Served as Enterprise Administrator in a Windows 2000 Active Directory environment.
    - Configured and supported desktop and production web, database, and file & print servers.
    - Configured and implemented remote installation for desktop deployment.
    - Deployed software, system upgrades, and security patches. Administered backup, MS Exchange 2000, Oracle8i, and SQL.
- Production Code Elevation:
    - Changed control reviews.
    - Coded elevations from test servers to production.
- Collocation Project Manager – Provided foundation and vendor management for the outsourcing of collocation services. Managed the implementation of the data center installation. Offered deployment and ongoing support of Internet/Intranet web, database and file servers, and networking hardware (CISCO switches and routers).
- Team Leadership – Prioritized workload and developed team.
- Planned solutions for hardware and software evaluation, testing, product recommendation, and implementation. Examples include Norton Antivirus and Veritas Backup Exec.

1999 – 9/2000: Technology Infrastructure Project Manager, Wingspanbank.com (Bank One),

Wilmington, DE

- Managed project life cycle for E-Commerce technology solutions.
    - Set up server infrastructure for development efforts.
    - Duties included identifying scope, risk, scalability, and cost; managing project plan; identifying server and connectivity requirements; implementing and supporting projects.

    - Managed projects using MS Project.
    - Facilitated environments: test, development, integration, QA, and production.
    - Coordinated application fail over and other tests.
- Technology vendor management – Evaluated product lines for server hardware, OS, networking equipment, and web hosting provider.
- Managed Windows NT servers' management and deployment.
    - Deployed and administered NT OS server platform for new web hosting facilities.
    - Created best practices documentation and checklist to ensure all NT platform servers complied with OS version, security, remote access, and application licensing.
    - Coordinated backup implementation and testing.
- Oversaw budget forecasting and maintenance
    - Provided foundation for project initiative's cost forecast.
    - Maintained, revised, and reported actual versus forecasted costs.
    - Conducted server hosting cost comparison between local data center and contracted web hosting facilities.
- Collocation site
    - Provided foundation for the outsourcing of collocation services.
    - Supported remote site, installed hardware, and managed network.

1997 – 1999: Executive Support Team Leader, First USA Bank (Bank One), Wilmington, DE

- Managed desktop support.
    - Supported bank executives.
    - Managed procurement, testing, deployment, and remote connectivity.

Desktop Support Team Leader

- Served as desktop support site leader for remote corporate departments.
    - Coordinated mass desktop deployment for remote site.
    - Managed desktop team that supported 500+ clients.
    - Main duties included installing and maintaining desktop applications, managing inventory, reporting, and ensuring that customer service met expectations and service-level agreements.
    - Supported MS Office products.