Air Force and Civilian Leaders' Experiences Integrating Civilian Information Technology Certification Training into the Military Information Technology Certification Process

Jamie E. Munn, Robert Branch
University of Phoenix, USA
jamieguam@yahoo.com, dr.robertbranch@gmail.com

Abstract

Military leaders, both active duty and general schedule (GS), must understand cyber warfare with its environmental connections and rapid evolution while finding ways to develop strategies that may lessen threats and attacks to government infrastructure. The Department of Defense (DoD) sought certification programs from the civilian sector to help create and enforce safeguards. The purpose of this qualitative exploratory single case study was to gain insight on Air Force leaders' perspectives of integrating civilian information technology (IT) certification training into the military IT certification process, the perception of benefits, and how they aligned with the DoD 8570 directive. The research method consisted of an exploratory case study focused on experiences of both military and civilian leaders at an Air Force Base (AFB) in the Southeastern United States.

Keywords: Department of Defense, Military Leaders, Information Technology, Government Infrastructure, Air Force

Introduction

The United States Department of Defense (DoD) is increasing its emphasis on training of employees including military and civilian members (General Accounting Office, 2013). In addition to military-specific education and training, the DoD encourages all employees to pursue training opportunities including various types of civilian certifications (Kennedy & Neilson, 2002). Shuford (2006) noted DoD leadership considers training and education to be crucial tools in preparing employees, both military and general

schedule (GS), to function in a rapidly changing environment. The DoD explored alternative employee training models ensuring staff have necessary training for ongoing intensive operations (Dobbins & Berge, 2006).

Literature Review

Leaders must understand cyber warfare with its environmental connections and rapid evolution while finding ways to develop strategies that may lessen attacks. In an effort to help mitigate risks on government networks, the DoD sought training and certification programs as a means to help create and enforce safeguards to ensure critical infrastructure was less susceptible to increasingly hostile cyber-attacks (Andress & Winterfeld, 2011). Cyber warfare is not considered a standalone option, but rather a part of a broad national security strategy (Stiennon, 2010). Military leaders find it critical to develop an appropriate policy to counter the threat of cyber terrorism and cyber warfare (Shuford, 2006).

The underlying motivation for this research study was to help military leaders ascertain benefits of the DoD 8570 mandate since its implementation in 2004. For this study to be affective, the researchers required both military and GS employee leaders to answer interview questions actively and honestly. Several studies linked military members and training (Dobbins & Berge, 2006; Duncan, 2015; Kennedy & Neilson, 2002) but none of these studies centered on understanding benefits of implementing new training from a military organizational leadership perspective. Using a qualitative case study approach to compile information on military leaders' perceptions of the training helped to accomplish the goal of this study. Results of the study assisted in determining whether the Computing

Technology Industry Association (CompTIA) Security+ objectives benefited military leaders at an AFB in the Southeastern United States.

Training requirements are expensive, time-consuming and their success remains unproven. A mandate first drafted in 2004 outlined specific training requirements for military members and civilians working in IT related jobs. The document, DoD 8570 mandate, provided specific guidance for integrating the civilian IT certification training into the military IT certification process (DoD 8570.01-M, 2015). The need for increased education in the IT field is necessary for DoD employees because of cyber-attacks the military faces daily on government networks. The general problem is training requirements are expensive and time-consuming and their success remains unproven. Unless the DoD gains an understanding of benefits from civilian certification implementation, the DoD could be investing an estimated $10 million annually on training without providing tangible benefits to the taxpayer (Noble, 2002; Wisher, Sabol, & Moses, 2002).

The military considers training and education to be a continuous process for service members (Anderson, 2002). Approximately 85% of military training and education involves preparing for tasks, jobs, and occupational specialties (Baker, 2016). The specific problem is that documentation is not complete regarding military leaders' perceptions of benefits received from the new training directive implemented; nor is there any information about how leaders perceived the training program aligned with the directive, and if results meet expectations set forth by the DoD 8570 directive. Military leaders may not see benefits of training from their employees who completed the required CompTIA Security+ training as part of the civilian certification. In an effort to maximize levels of education and training used by the military, the DoD may profit from understanding how military

leaders perceive the training to be effective (Wisher et al., 2002). According to Wisher, Sabol, and Moses (2002), it is essential for the DoD to consider military leaders' perceptions in the overall process to understand how the training is impacting the DoD and to understand benefits of the training fully.

Theoretical Framework

The theoretical framework for this case study flowed from critical success and risk factor (CSRF) theory to stakeholder theory and also included internal and external stakeholder theory research regarding new training policies and directives, in particular the 8570 directive. The integration of civilian IT certification training into the military IT certification process, CSRF theory, and stakeholder theory were the main theoretical frameworks that influenced this proposal.

Purpose of the Study

The purpose of this study was to gain insight on Air Force leaders' perspectives of integrating civilian IT certification training into the military IT certification process, the perception of benefits of such implementations, and how processes and benefits aligned with the DoD 8570 directive. Gaining insight on Air Force leaders' perspectives of integrating civilian IT certification training into the military IT certification process, the perception of benefits of such implementations, and how processes and benefits aligned with the DoD 8570 directive was important. Conducting this study was vital for the researcher to understand perceptions of the training.

Research Questions

Previous studies focused on military training from service members' perspectives (Cherry, 2010; Grauel, Malone & Wygal, 2012; Mazur & Pisarski, 2015; Stiennon, 2010;

Wilson & Hash, 2015). These studies usually had instances outside the military environment; therefore, limited information is available to the DoD to facilitate leaders' understanding of benefits received from training. The ability to collect viable data depends on the formulation of a solid research question (Creswell, 2013). Specifically, the goal of this research study was to understand the perception of military leaders toward civilian IT certification as part of the training process. The two guiding questions of the study were:

RQ 1: What benefits do senior military and civilian leaders perceive from requiring military and civilian employees obtaining civilian IT certification training?

RQ 2: From the senior military and civilian leaders' ' perspective, how well does the civilian IT certification training program align with the DoD 8570 Directive?

Research Method and Design

The research method chosen was a qualitative approach and the research design was an exploratory case study. An exploratory case study helped understand military and civilian leaders' perceptions of the new training. The research design was a product of underlying logic by a researchers for a research study. Moses and Knutsen (2007) suggested, "Good science should be driven by questions or problems, not by methods" (p. 14). Focus on the fundamental research question presented the necessity to have an adequate scholarly understanding of the goal of the research question (Rubin & Rubin, 2005). In these sections, the rationale for selecting the qualitative methodology, the case study method, and the motivation for choosing this research design are described.

Population

The general population included all senior leaders of the DoD. The focus of this study included senior military and civilian leaders in the IT industry who had experience with the certification process and who supervised members who completed the training. Senior leaders were defined as enlisted members and officers in leadership positions with 10 or more years' experience, and GS employees with 10 or more years' experience in the IT field. There were approximately 200 service members in the combined two IT units (communications squadrons) at the AFB in the Southeastern United States where the study took place. The above criteria matched about 10% of the population. In the event too few participants met the above criteria, the pool would grow by snowballing, reducing the number of years' experience to 5-8 years, or by contacting members who recently retired, but still have experience.

Purposive Sampling

The population under investigation was selected by purposeful sampling units from an AFB in the Southeastern United States to create a more homogenous group, as well as members from a similar environment who are stakeholders for the training implementation. Parameters of the study excluded outside organizations and other branches of the military and focused solely on members assigned to an AFB in the Southeastern United States. The focus of this study was the implementation of Security+ training as part of a new DoD Mandate. Researchers may observe multiple cases hastily, or focus intently on a few cases (Gerring, 2007). The focus of the study was on the stakeholder group of military leaders with interviews as the preference for data gathering. If face-to-face interviews were not conceivable or if follow-up questions were asked, a phone interview would be needed; however this was not needed for the study.

Data Collection

The study population recruited from two IT units located at an AFB in the Southeastern United States. The population, which included both military and civilian leaders from the two IT units contained five potential members from unit A and five potential members from unit B based on the inclusion of both military and civilian leaders with 10 or more years' experience in the IT field. Potential senior AF military and civilian leaders with 10 or more years' experience in the IT field were recruited using data from public organizational forums. Once members were identified using public data from the unit's online forums, they were contacted by a personal email, personal phone or in-person while in an off-duty status to confirm the accuracy of information they provided and determine a willingness to participate in the study. The recruitment of AF leaders took place through personal communications only and there was no in-person contact during work hours. All interaction concerning the study took place through non-government communication channels and all recruits were made aware participation was voluntary and was in no way an AF requirement.

Leaders were individually interviewed and responses from military and civilian leaders were recorded and transcribed and used as two of the data sources along with public information from CompTIA website and other public sources add an additional viewpoint, and to support triangulation of findings. The CompTIA website contains a subsection on the web page listing trends. There are additional information, articles, research, and programs that may add value to the case study. All data were transcribed by the researcher and triangulated using the NVivo 11 software program. The researcher used NVivo software to assist with coding and identifying emergent themes. Interview questions

provided data to assist in data triangulation. The data analysis may lead to group-specific critical success and risk factors that are compared and contrasted with previous findings.

Face-to-face interviews occurred using one primary and one back-up recording device. When and if there was a need for follow-up or clarifying questions that evolved during the course of the study, the researcher conducted those follow-up questions either in person, via the telephone, or through e-mail correspondence, depending on the participant's preference and availability. Follow-up questions were not necessary for every participant and only took place for clarification of information. All follow-up and clarifying questions were documented in the summary of interview questions and included in the final study.

The Analysis of the Data

Transcribing interviews verbatim occurred first. Once this was complete, a copy of the transcript was sent to the participant to member-check for accuracy and to ensure there was no miscommunication during the interview. Allowing participants to remove any information they believed might include any personally identifiable information or information they deemed confidential was essential to protecting the rights of participants. There were no requests for removal of information. Once the participant approved the transcription, data recording was filed and the transcript became part of the official research documentation and was part of the detailed analysis.

The computer software NVivo 11 was used to support the data analysis process. NVivo 11 offered support for coding, comments, visualization, and multiple document types and helped reduce risks of researcher bias and reduce mistakes (NVivo, 2017). NVivo is the software that helped organize and analyze data collected from transcripts.

NVivo was used to compare, evaluate, assess, and identify various elements of speech from data obtained after uploading transcriptions. Manual coding was also an option using Microsoft excel as a potential tool to assist in the process. While manual coding was not as common as using NVivo software, there is value added to using both manual and automatic coding through NVivo. Excel was used to do some manual coding with data from the CompTIA website. The data analysis process reduced researcher bias and offered a detailed comparison not only of cultural differences of CSRF in this study but also in comparisons to previous studies.

Interview Results

Research questions guided interview questions and helped to achieve an in-depth look at military leaders' experiences as well as identify critical success and risk factors into how the training program aligned with the DoD 8570 Directive. Questions one through seven were designed to focus on leaders' experiences with the DoD 8570 Directive. The first seven questions allowed participants to gain comfort with the interview process and transparently share their experiences. All participants held organizational leadership positions within their careers and each had the rank of Captain through Lieutenant Colonel for officers, Master Sergeant through Chief Master Sergeant for enlisted, and GS 11 or higher for the civilian side, all with at least 10 years' experience. The second set of questions focused solely on leadership; four questions provided participants an opportunity to reflect on their leadership roles and experience, explain their leadership development, and what they would have done differently based on reflection. The final set of questions contained four questions focusing on the impact of the DoD 8570 mandate. Interview questions aligned to the two main research questions.

Documentation Analysis

Content data analysis for the documentation consisted of interviews as well trend and analysis data retrieved from CompTIA website found under the subsection on the page listing trends associated with the certification. The data from the CompTIA website provided trends that directly correlated to the research. The trends that were used from the website included data for leadership, work implications, as well as data about DoD adoption of the certification. Furthermore, the website provided data on growing threats of computer security as well as the need for education on network protection. The information along with the data analysis from the interviews and the previous studies were important for data triangulation.

Data analysis indicated AF leaders assigned to an AFB in the Southeastern United States considered the DoD 8570 certification to be all-encompassing while providing limited information on specifics of the DoD 8570 mandate. The CompTIA website provided trend and analysis data concerning the certifications and certification process as well as provided key areas for companies to focus efforts. The website indicated organizations that required the certification were better educated to deal with baseline security breaches. Based on interviews, participants all indicated the need for a baseline certification was relevant and important. A further review of the CompTIA website listed reasons for professionals to gain certification. According to the CompTIA website, "Nine out of 10 employers agree that certifications are critical in finding the right person for the job" (2017, para 3). The site lists specific details of how, when, and what forms of training and certification are available for the process.

Findings from the study also concluded leaders were in-line with the DoD mandate, but the recommended policy and guidance from high level, DoD leaders was lacking. Lack of policy and guidance led to a wider variation of how the program was mandated. Data collected from the participant's interviews supported the CompTIA website map was not all encompassing. The website provides an organization guideline, but the military being a unique entity needs to develop more detailed policies and guidelines to maintain CEUs and to keep better track of assigned military personnel.

The review of previous documentation to include studies and scholarly articles was broadly focused and not specific to the DoD or more specifically to military leaders. Focus on the analyzed documentation led the researcher to find common words and phrases that were used to develop themes for the study and focus more narrowly on the specific topic and group. When entering the data collected from all three data sources into the NVivo 11 software program, the key words were clearly highlighted and identified to assist the researcher with identification to include commonalities amongst the various data sources.

Reoccurring themes, based on the coding of participants' interviews, previous studies and the CompTIA website data provided the basis for identifying issues involved in the leaders' perceptions of benefits of the DoD 8570 mandate and are required for the future development for the mandate and the certification. Participants provided their opinions and perceptions about their experiences as individuals in leadership positions that corresponded to the intent of the research and interview questions. The final chapter focuses on conclusions, implications, and recommendations and examines limitations.

The problem addressed with this study is that documentation was not complete on military leaders' perceptions of benefits received from implementing the new training

directive. There was no information available regarding how leaders perceived the training program alignment with the directive or if results met expectations set forth by the DoD 8570 directive. The primary motivation for this research study was to help military leaders determine benefits of the DoD 8570 mandate since its implementation in 2004. Several study findings previously linked military members and training but none of these studies focused on understanding benefits of implementing new training from a military organizational leadership perspective (Dobbins & Berge, 2006; Duncan, 2015; Kennedy & Neilson, 2002). A qualitative case study approach was used to compile information on military leaders' perceptions of the training implementation. Results of the study assisted in determining military leaders at an AFB in the Southeastern United States perceived the DoD 8570 initiative as beneficial.

Thematic Comparison and Contrast

Documentation was incomplete on military leaders' perception of benefits received from implementing the training directive. There was no information on how leaders perceived the training to align with the directive and if results met expectations set forth by the training directive. The implementation of the mandate was mostly left to the operational force at unit level organizations and above, with little to no oversight according to the literature and input from participants. Interviews allowed the researcher to gather in-depth data from face-to-face meetings. Trends emerged from data collection and analysis, and trends continue with little improvement over time; six themes emerged from data provided by participants.

Theme 1: Combined experiences, lessons, and history to make decisions. The first theme that emerged from interviews was the understanding of combined experiences,

lessons and history helps leaders make decisions. Effective leadership procedures and expending the groundwork of individuals' experiences provides leaders the necessary skills needed to make decisions, provide required effects to subordinates, and provide influence (Lerstrom, 2008). Organizations implementing new training requirements make an investment risk and need to consider significant recurring maintenance costs (Fryling, 2010). Making decisions to impact the total force, the entire DoD, must have careful consideration about the complexity of such a mandate. Organizations in the healthcare industry and the military have become more intricate over time, using experiences as a basis to make decisions and rely on those past experiences and lessons learned to form findings (Lisko & O'Dell, 2010).

Theme 2: Flexibility is required for change. The second theme that emerged from data is flexibility is a desired attribute of leaders and leadership within the organization, as it fosters the capability to adjust not only themselves, but also plans, missions, training, and guidance to the organization to fit complex and ever-changing environments. All participants viewed the requirement of flexibility as an important attribute to the adoption of the DoD 8570 Directive. Successful leaders are able to adapt their leadership style to goals, tasks, missions, and objectives to meet needs of the organization (Yukl, 2013). Air Force leaders are familiar with the mindset that flexibility is the key to airpower; however, perceptions from the case study indicated leaders in this study do not actually think there was enough flexibility when the mandate was implemented.

Theme 3: Clear guidance is needed. Guidance is needed from the top down and this was the third theme to emerge from interviews supporting this statement. The first

draft of the mandate was released in 2004 and leaders felt the guidance was clear; each subsequent year, there was more guidance to clarify. In 2015, the DoD distributed a memorandum identified as, Department of Defense Cyber Security Culture and Compliance Initiative (DC3I); the memo gives clear guidance on military efforts to crack down on cyber security breaches by delivering raw numbers and data on attacks on DoD Networks, (Department of Defense, 2015). While the guidance was published, leaders from the case study felt the mandate still needed for clarification and perhaps harsher guidelines. The majority of participants expressed a desire for more guidance from their individual leadership. The implementation phase has since passed, but guidance was needed, even more so, on the way ahead.

Theme 4: Areas for improvement. There were areas in need of improvement. This began from the initial implementation of the mandate into the current program. A continuous improvement process is an ongoing effort to improve current products, processes and services (Stiennon, 2010). According to participants' responses, leaders need to be able to provide subordinates with feedback and develop a process to assist them in understanding concepts, policies, events, and issues involved in the DoD 8570 Directive. Feedback is deficient from the top down. Effective feedback is valuable information that is used to make significant decisions; successful organizations are top performers because they steadily search for ways to improve (Singh, 2013). Effective feedback has benefits for the entire organization. The growth of the directive and the success of the training program would benefit greatly if more feedback from employees was requested.

Theme 5: Success and risk factors. The fifth theme that emerged was the success and risk factors associated with the implementation of the training directive. Success and

risk factors found during the study assisted the researcher in understanding benefits gained from implementing civilian IT training programs and critical factors that influenced the mandate. The continuing education requirements emerged as a competency needing emphasis based on the analysis of data provided by a majority of participants.

Most participants provided examples supporting the idea that there were both success and risks factors associated with the implementation of the program. Application of the critical success and risk factor theory to a project and creating project-specific goals requires a definition of project success, which is defined as measurable results such as return on investment, but may also encompass subjective definitions that may differ between projects, organizations, and stakeholder groups (Miles, 2012; Sedera, Gable & Chan, 2004). Leadership contributes important information for CSRF theory stakeholders and their impact within CSRF theory are a significant element of the project's success (Goo, Yim, & Kim, 2013). Success and risk factors are investigated based on implementation-related specific factors, such as training implementation (Floyd & Yerby, 2014), as well as constructed on short-term and long-term aspects (Cassidy, 2006), such as consequences of the implementation of the new policy. The understanding of success and risk factors and incorporating best practices supported the positive outcome of the study.

Theme 6: Level of involvement and workload. The last theme of level of involvement and workload emerged as a theme while focusing on RQ2. At the time of this study, participants all expressed an increased workload as a result of the implementation of the DoD 8570 directive; managing the training is a daunting process that is never-ending. Each military member is certified at different times in their careers, so continuous tracking is needed for each of them as they progress through and maintain continued education as

required. The burden did not stop with tracking training, it continued into the workplace putting a strain on work centers that had members who had yet to complete the training. This was an increased workload for technicians as well as a burden to leaders. All interviewees expressed they had an increased workload and had to be very involved with the tracking and training to ensure compliance with the DoD 8570 directive. Prior to this study, this was not identified as a potential outcome, but participants each made it clear the training had increased their workload, at least initially. When a new program is implemented, initial stages may require more work, but once things settle down the workload should begin to leverage with benefits (Baker, 2016).

Implications

The DoD implemented the DoD 8570 mandate in 2004 and since this time, there were several revisions released. The directive provides specific guidance on processes for obtaining the required civilian certification training, CompTIA Security+ and previously CompTIA A+, as well as testing site locations. The results found training to be sufficient for providing the baseline to security standards. However, the training program requires revisions for better integration, to strengthen the current training program and new processes, as supported by leaders from the top down.

The lack of uniformity across the DoD in this study, if left to continue could undermine the program and lead to more confusion. The program is better served with strict guidance on how to maintain the program and what each of the leaders' roles in the training process should be. While there is an understanding that each unit, base, and organization has a different mission, the reoccurring issue discussed was lack of a strict policy and guidance on how to maintain such a program.

The funding of the program was relevant to the study. The availability of enough funds for the certification training and classes is a vital part of implementing the mandate; funding can make or break the organization's training plan, if funding is not provided it may not be a priority (Wilson & Hash, 2015). Initial stages indicate funding was not readily available in all cases, while funding seems to be a non-issue at the time of this study. While the DoD covered funding for the certification and CEUs, the implication was participants in this study found this to be an expense that was not needed.

Recommendations for Practical Application

Study participants based on their combined experiences understood the requirement for the civilian certification training and shared their experiences, opinions, and perceptions on the need for DoD 8570 Mandate. All participants worked on an AFB in the Southeastern United States and were either civilian or military members working for the Air Force and understood concepts and requirements of the training. Recommendations do not go against any of the DoDs regulations, policies, or directives, but instead could assist with improving the current program.

- The DoD review and revise the current 8570 directive to clarify CEU training requirements and maintaining the certification.
- The DoD review and consider an in-house or a DoD written and approved certification test as a possible cost savings.
- The DoD should conduct a survey on benefits received for completing the training to understand the ROI since the integration of the training better.
- The DoD, or each branch, should have better and clearer guidance and policies for who is to manage the training and at what level.

- The DoD should reconsider the implementation of the DoD 8570 mandate and better develop something more military specific.
- The DoD–the military community should survey or interview those people who were mandated to complete the training and get feedback on the implementation and the current status of the program.
- The DoD should consider how and if this certification is and will impact retention of employees.
- The DoD should consider the workload balance and if the certification is causing additional work and more stress on the workplace to maintain the certification.

Summary

Findings from this qualitative exploratory case study revealed the DoD 8570 mandate, although successfully implemented required revisions and new processes and policies to strengthen the program. For leaders assigned to an AFB in the Southeastern United States, the return on investment was not clearly seen. Many leaders felt certification offered baseline knowledge of security concepts, while others felt a DoD certification was just as valuable.

The DoD should address and emphasize within the 8570 mandate attributes of individuals' combined experiences, lessons, and history to assist in decision-making. The mandate should also address, revise and emphasize the guidance, polices surrounding the training program, and provide more information on how to manage the program. The DoD should improve training and education, specifically as it pertains to individual workloads and discover how to ensure certifications remain intact. Finally, revisions in the program

would vastly improve the success and potentially save money with consideration to a DoD created certification program.

References

Anderson, L. J. (2002). *Servicemember's guide to a college degree* (2nd ed.). Mechanicsburg, PA: Stackpole Books.

Andress, J., & Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Waltham, MA: Syngress.

Baker, M. (2016). Striving for effective cyber workforce development. Retrieved from http://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473577.pdf

Cassidy, A. (2006). *A practical guide to information systems strategic planning* (2nd ed.). Boca Raton, Florida: Auerbach Publications.

Cherry, J. D. (2010). *Information assurance within the United States Air Force* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Full Text. (Order No. 3397838)

CompTIA. Security+ Certification. (2017). Retrieved from http://www.compTIA.org.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). London, UK: Sage Publications.

Department of Defense. (2015). *Cybersecurity Culture and Compliance Initiative (DC3I)* [Memorandum]. Washington, DC: Department of Defense. Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf

Dobbins, B. W., & Berge, Z. L. (2006). Support for distance education and training. *Distance Learning, 3*(1), 1.

Duncan, S. (2015). The U.S. Army's impact on the history of distance education. *The Quarterly Review of Distance Education, 6*(4), 397-404. doi:10.4324/9780203463772

Floyd, K. S., & Yerby, J. M. (2014). Information systems faculty perceptions of ethical work climate and job satisfaction. *Journal of the Southern Association for Information Systems, 2*(1). Retrieved from http://dx.doi.org/10.3998/jsais.11880084.0002.102.

Fryling, M. (2010). Total cost of ownership, system acceptance and perceived success of enterprise resource planning software: Simulating a dynamic feedback perspective of ERP in the higher education environment (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3402347)

General Accounting Office. (2013). *Military transformation: Progress and challenges for DoD's advanced distributed learning program*s. (GAO-03-393). Washington, DC: U.S. General Accounting Office.

Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge, MA: Cambridge University Press.

Goo, J., Yim, M-S., & Kim, D. J. (2013). A path way to successful management of individual intention to security compliance: A role of organizational security climate. *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS)* (pp. 2959- 2968). http://dx.doi.org/10.1109/HICSS.2013.51

Grauel, D. W., Malone, V. F., & Wygal, W. R. (2012). Marching an Army acquisition program toward success. *Defense AT&L, 41*(6), 20-23. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=AD1016013

Kennedy, G. C., & Neilson, K. (Eds.). (2002). *Military education: Past, present, and future.* Westport, CT: Praeger.

Lerstrom, A. (2008). Advising Jay: A case study using a situational leadership approach. *NACADA Journal*, *28*(2), 21-27. http://dx.doi.org/10.12930/0271-9517-28.2.21

Lisko, S. A., & O'Dell, V. (2010). Integration of theory and practice: Experiential learning theory and nursing education. *Nursing Education Perspectives, 31*(2), 106-8. Retrieved from http://journals.lww.com/neponline/pages/default.aspx

Mazur, A. K., & Pisarski, A. (2015). Major project managers' internal and external stakeholder relationships: The development and validation of measurement scales. *International Journal of Project Management, 33*(8), 1680-1691. doi: 10.1016/j.ijproman.2015.07.008

Miles, S. (2012). Stakeholders: Essentially contested or just confused? *Journal of Business Ethics, 108*(3): 285–298. doi:10.1007/s10551-011-1090-8.

Moses, J. W., & Knutsen, T. (2007). *Ways of knowing - Competing methodologies in social and political research.* New York, NY: Palgrave Macmillan.

Noble, D. F. (2002). Technology and the commodification of higher education. *Monthly Review, 53,* 10. Retrieved from http://www.monthlyreview.org/ 0302noble.htm

NVivo. (2017). NVivo features and benefits Retrieved from http://www.qsrinternational.com/products_nvivo_features-and-benefits.aspx

Rubin, H. J., & Rubin, I. S. (2005). *Qualitative interviewing: The art of hearing data.* Thousand Oaks, CA: Sage.

Sedera, D., Gable, G. G., & Chan, T. (2004, June 14-16). *Measuring enterprise system success: The importance of a multiple stakeholder perspective.* Paper presented at the 12th European Conference on Information Systems, Turku, Finland.

Singh, A. (2013). A study of role of McKinsey's 7S framework in achieving organizational excellence. *Organization Development Journal, 31*(3), 39-50. Retrieved from http://search.proquest.com/docview/1467437673?accountid=35812

Stiennon, R. (2010). *Surviving cyberwar*. Lanham, MD: Government Institutes.

Wisher, R. A., Sabol, M. A., & Moses, F. L. (2002). *Distance learning: The soldier's perspective* (ARI Special Report No. 49). Alexandria, VA: US Army Research Institute for the Behavioral and Social Sciences. doi:10.1037/e517442010-001

Wilson M., & Hash, J. (2015). Information technology security awareness, training, education, and certification. Retrieved from http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm

Yukl, G. (2013). *Leadership in organizations* (8th ed). Upper Saddle River, NJ: Pearson Prentice Hall.