EXAMINING THE RELATIONSHIP BETWEEN SECURITY EFFICACY, AGILITY, AND STRATEGIC ALIGNMENT IN INDUSTRIAL CONTROL SYSTEM ENVIRONMENTS: A CORRELATIONAL STUDY

by

Devecchio Turner

JELENA VUCETIC, PhD, Faculty Mentor and Chair

GLENN BOTTOMLY, PhD, Committee Member

WENBIN LUO, PhD, Committee Member

Rhonda Capron, EdD, Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

July 2018

Abstract

A quantitative non-experimental correlational study was used to examine the relationship between security efficacy, agility, and strategic alignment in U.S.-based ICS environments. This study used a multidimensional theoretical lens for analysis that included strategic alignment theory, agility theory, and integrated system theory. The full population for this study included industrial and control engineers, technicians, and industrial control operators charged with securing ICS environments with a sample frame that included 563 potential respondents in manufacturing, utilities, energy, and various other industries from Cint's database. A survey was used to collect perceptions on the constructs of security efficacy, agility, and strategic alignment within the sample frame, and 107 usable survey responses were received and used for analysis. Correlation and multiple regression tests were performed on collected data to determine the strength and direction of the relationship and to assess the predictive capabilities of security efficacy and agility on strategic alignment. The results revealed significant positive correlations between (a) agility and strategic alignment and (b) security efficacy and strategic alignment. Additionally, security efficacy and agility have a positive and predictive relationship with strategic alignment and account for 40% (agility accounting for 29%) of the variance in strategic alignment. These results indicate that in addition to protecting information assets, the effectiveness of an organization's security program significantly enhances an organization's degree of strategic alignment in ICS environments.

Acknowledgments

I would like to thank committee members Jelena Vucetic, Glenn Bottomly, and Wenbin Luo for their dedication to the completion of this effort.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

In rapidly changing business environments, organizational success is heavily dependent on information technology (IT) (Furukawa et al., 2014; Tallon, Queiroz, Coltman, & Sharma, 2016.). IT enables process capabilities that allow companies to respond to changing business conditions and increase market positioning (Tan, Tan, Wang, & Sedera, 2016). As noted by Davenport and Short (1990), the use of IT is so pervasive that it becomes easy to forget that IT transformed industrial engineering practices in industries such as manufacturing long before being used for productivity gains in carpeted spaces. The use of IT in industrial areas is still prevalent today.

For example, an industrial control system (ICS) is used to manage a variety of modern conveniences we take for granted. Industrial control systems are used to control and manage industrial processes in environments such as those found in water treatment facilities, electrical distribution, fuel distribution pipelines, and bulk energy generation (Janicke, Nicholson, Webber, & Cau, 2015). The National Institute of Standards and Technology (NIST) noted that ICS is a common term used to describe a number of systems including supervisory control and data acquisition (SCADA), distributed control systems (DCSs), and programmable logic controllers (PLCs) in NIST SP 800-53 and 800-82 (Ross, 2105; Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015).

The International Society of Automation (ISA) extends the definition offered by NIST to include additional systems in the context of a more holistic definition by noting these systems

can be standalone or integrated (ISA99, 2017). Bagri et al. (2014) offered that industrial control systems are the core of industrial processes existing in a physical world. ICSs are used to manage entire environments remotely and afford organizations the opportunity to automate functions that once required personnel to be physically present. ICSs are used and owned by a variety of public and private institutions in a variety of settings. For reference, NIST SP 800-82 offered that 85% of the nation's critical ICS infrastructure operates under private entities (Stouffer et al., 2015).

Initially, ICS systems were meant to automate and monitor industrial processes between remote nodes and central stations; this data has now migrated from central monitoring stations to corporate desktop connections (Cvejic, Markovic, & Cvejic, 2014; Hellmann, 2015). Engineers can now view monitoring data from practically anywhere via the remote monitoring capability these systems offer. ICSs are unique purpose systems and their continued expansion outside of these once isolated environments is outside of the original design specification (Ahmed, Obermeier, Naedele, & Richard, 2012; Obeid & Dhaussy, 2016; Piggin, 2014). The data presented with these systems provide critical operational data on a variety of functions such as temperature, pressure, and recorded speed from connected sensors; the resultant data can be stored or be used to trigger pre-determined responses. The expansion of ICS environments over the Internet has allowed companies to expand operations globally, but there are additional risks.

Before the practice of connecting ICSs to business networks and the Internet became a common practice, NIST SP 800-82 noted that security was of little concern due to the isolated nature of these systems (Stouffer et al., 2015). As ICSs systems have migrated from local containment to distributed systems, attacks are now common. A prevailing theme in ICS environments is security through obscurity which is a mode of operation that relies on intimate

knowledge of the environment for any reconnaissance tools to be practical (Janicke, Nicholson, Webber, & Cau, 2015). This practice is not always successful.

Bambauer (2014) demonstrated that if bad actors can remotely manipulate infrastructure systems, public safety and health are at risk. For example, attacks have ranged from completely wiping the hard drives of 30,000 PCs at the Saudi Arabian Oil Company to completely shutting down nation-state programs such as what happened in Iran and Tibet (Bambauer, 2014; Dehlawi & Abokhodair, 2013). Schiavone, Garg, and Summers (2014) noted that despite advances in detection, technology, and adoption of security frameworks, companies are ill-prepared to deal with cyber-attacks. The risks associated with the continued expansion of ICS to insecure networks continues to escalate.

In 2016, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a Department of Homeland Security, reported responding to 290 incidents across the 16 critical infrastructure (CI) segments (ICS-CERT, 2016). The majority of attacks occurred in the Manufacturing (21.7%), Communications (21.3%), and Energy (20.3%) sectors. 26% of the incidents were generated using email. Additionally, ICS-CERT reported that 2016 was the first year a cyber attack resulted in a physical impact to a power grid. Baumbauer (2014) noted that few organizations have the focus on preventing attacks that exists within the electrical grid. The number of incidents investigated by ICS-CERT has increased by 18% since 2014; the communications CI sector has seen a 342% increase in incidents between 2014 and 2016 (ICS-CERT, 2014, 2016).

Background of the Problem

Henderson and Venkatraman (1993) created a theoretical framework that defined how the alignment of business and IT strategies would enable the business world to operationalize IT to

support the business (Renaud, Walsh, & Kalika, 2016). The researchers eventually presented the strategic alignment model (SAM). The SAM would come to be known as the reference model for deriving the most value out of IT (Renaud et al., 2016). The building blocks of strategic fit and functional integration, which were later defined by Henderson and Venkatraman as external and internal functional domains, are the foundation for the SAM.

Strategic alignment between business and IT continues to be a primary concern of businesses today (Furukawa, Hirobayashi, & Misawa, 2014; Tallon & Pinsonneault, 2011; Turel, Liu, & Bart, 2017). The use of IT has enabled companies to accomplish business objectives, enhance speed to market, and ensure rapid returns on investments when implemented correctly. Ghani and Zakaria (2013) posited that IT allows the business to respond to change and effectively execute the defined business model while sustaining alignment. IT must be able to adapt to rapidly changing business conditions. Luftman and Kempaiah noted that, despite the benefits promised by ensuring strategic alignment of business and IT strategy, businesses continued to be plagued by IT failing to meet the needs of the business (as cited Hajikhani & Azadi, 2013, p. 528; Turel et al., 2017). Even when IT and business strategies are aligned, a mechanism is needed that allows fluid execution of initiatives between the two strategies

Agility

Roberts and Grover (2012) offered that agility is as influential as aligning IT and business strategy. While noting the importance of alignment of business and IT, Roberts and Grover suggested that agility is the ability of an organization to respond to rapidly changing business conditions that enable entry into new markets. An organization's degree of agility determines how quickly IT responds with technology to enable the business to meet defined objectives (Lee, Xu, Kuilboer, & Ashrafi, 2016; Thao, Molla, & Peszynski, 2012). As competition in the

marketplace increases, agility becomes key in responding to dynamic changes (Lee et al., 2016; Sambamurthy, Bharadwaj, & Grover, 2003). The need to quickly adapt and respond places "…strain on existing security processes and practices" (Istikoma, Bt Fakhri, Qurat ul, & Ibrahim, 2015, p. 62).

Chakravarty, Grewal, and Sambamurthy (2013) further asserted that agility has risen as a strategic competency against the backdrop of massive globalization, hyper-competitive markets, and consumer choice. The definition of agility, a measure to sense and respond to competitive actions initiated by competitors, continues to highlight the importance of rapidly responding to dynamic business conditions. This rapid response also encompasses the ability to continually innovate in response to market imitations (Lowry & Wilson, 2016; Roberts & Grover, 2012). Agility in ICS environments is vital for capitalizing on market opportunities (Campos, Santos, de Souza, & da Silva, 2013).

Inherent Security Challenges

Production ICSs that connect to corporate systems are implemented in layers to aid in functional segmentation. Foundational work from The Purdue Model for Control Hierarchy provides a functional model for layering with descriptions of the layers and additional information on the benefits of segmentation defined in this model (ISA99, 2004). The main benefit of this layered approach is segregation. According to NIST SP 800-82, the layers are typically zoned off via the use of firewalls (Ahmed et al., 2012; Asgarkhani & Sitnikova, 2014b; Stouffer et al., 2015). The use of network control points is not without challenges. Tightly controlled firewall rules between business and process control networks render traditional tools that are used to monitor post-event security items ineffective (Ahmed et al., 2012; Tzokatziou, Maglaras, Janicke, & He, 2015).

NIST SP 800-82 noted that many ICS systems require continuous operation due to the complexity involved in stopping production. In the event of an attack, having a forensics investigator pause the system for analysis is not practical (Ahmed et al., 2012; Taveras, 2013). Additionally, some environments typically run on low-powered legacy hardware with limited vendor support (Ahmed et al., 2012; Chabukswar & Sinopoli, 2015). The inability to capture live data, triggering of false positives by scanning, customized kernels, and an abundance of devices that are susceptible to system resource exhaustion contribute to making SCADA environments challenging to monitor for forensic analysts.

The remote monitoring and data collection functions of production systems have expanded the reach of ICSs. Adding to the issues for forensic analysts, Alcaraz and Zeadally (2015) also noted that the primary communication protocol used in ICS systems, MODBUS, is inherently insecure. Ponomarev (2015) attributed the insecure nature of MODBUS to the fact that it was only intended for controlled environments. Manipulation of this traffic becomes a trivial task when insecure protocols like MODBUS are wrapped in Internet Protocol (IP) and transmitted over the Internet. With the increased access and exposure of ICSs, the systems are now vulnerable to the same attacks that exist with Internet-based systems (Hellman, 2015).

Gao et al. (2014) asserted that ICSs did not evolve as fast as PCs or telecommunication networks and thus are susceptible to frequent attacks. The slower rate of evolution presents real dangers from exposed vulnerabilities. After installation and certification for safety compliance, patches and updates to an ICS take a back seat to operational stability; the sensitivity to impacting an operational process often results in systems not being updated during their lifetime of 10 to 20 years (Cook, Janicke, Smith, & Maglaras, 2017). Exploitation of an ICS poses a threat to the safety and the preservation of human life (Bambauer, 2014).

In recognition of the risks, legislation has been passed that acknowledges the risk of exposure. For example, President Barrack Obama signed Executive Order 13636 (2013) spurring the creation of NIST's Cybersecurity Framework and Presidential Policy Directive 21 (PPD 21) which superseded two previous presidential directives related to Critical Infrastructure Protection (CIP) programs (The White House, 2013). The continued updates to the security frameworks securing critical infrastructure highlight its impact on the safety of the surrounding environment. The protection of critical infrastructure **s**ystems that process data is a requirement. IT systems used in ICS environments are similar to those used in carpeted office spaces (Kuusk, Koronios, & Gao, 2013).

Despite the similarity in IT systems used to manage corporate and ICS networks, the business processes and rules governing their use are controlled by different groups within the same business. Ginter (2013) noted that business systems and ICSs were managed differently despite both being used to process data. Additionally, the author declared that confidentiality, integrity, and availability, pinnacles of a business system, were reversed in industrial control system environments to focus on availability, integrity, and confidentiality. This focus on availability contributes to the vulnerability of ICSs. The patching of software vulnerabilities is common in IT environments, but patches in ICS environments typically break the system specific nature of these environments. Adding to the security issues associated with ICS management systems, Neitzel and Huba (2014) offered that the continued use of Windows XP, an outdated operating system, is typical.

This research seeks to understand the relationship between business pressure to stay aligned, maintaining agility while responding to rapidly changing market conditions, and the efficacy of security controls in the face of persistent security threats. The strategic alignment

model suggests that when IT and business strategies are aligned, IT is now able to help businesses meet their strategic objectives. The application of this theory in this research will provide additional context for the constructs of agility and security efficacy to support business initiatives (alignment) while providing flexible and secure business transactions in industrial control environments.

Statement of the Problem

The theories of strategic alignment and agility are solely linked to the achievement of value out of IT investments by meeting business objectives and using existing technology to respond to competitive actions initiated by competitors. The problem is that extant literature does not identify a quantitative link between security and the constructs of strategic alignment and agility. The impact of security efficacy and agility on the goal of strategic alignment in ICS environments is not understood. The theories of strategic alignment and agility were created long before today's ICS threat landscape existed; thus, the concept of security is missing in a context that applies to today's business environment. The lack of focus on security in these theories highlights the evolution of a hostile operating environment that did not exist at the inception of these theories.

Few articles have attempted to quantitatively link security to the constructs of agility and strategic alignment in ICS environments. The mitigation of concerns within environments centered on these theories must take into account changes that have happened as ICSs have evolved into the always-on environment that exists today. The problem the research seeks to solve is an understanding of the relationship between production business units need for agility, the need for strategic alignment between business IT and strategy, and the impact of security on the goals of agility and strategic alignment in ICS environments.

ICSs have become more distributed to allow for the creation of new business opportunities; thus, their optimal use requires alignment of business and information technology (IT) strategy (Kuusk et al., 2013). Seminal work from Smaczny (2001) offered that the alignment of business and IT suggests chronological order, in that the business decision precedes IT enabling that decision. This ordinal relationship puts pressure on IT security to ensure policies are in place to allow business transactions to take place securely (Istikoma et al., 2015; Pieters, Dimkov, & Pavlovic, 2013). When security breaches happen in ICS environments, the converged attack depends on failures in either physical or IT domains (Aleem, Wakefield, & Button, 2013). Existing attempts to remediate attacks on ICSs have not been successful; the U.S. government continues to research the use of legislation to remediate the issue (Hellmann, 2015).

The research literature on information security in industrial control environments indicates that we know the importance of alignment (Apol, Hadiwidjojo, Djumahir, Rahayu, & Sarno, 2013; Coltman, Tallon, Sharma, & Queiroz, 2015; Gerow, Thatcher, & Grover, 2015; Goepp & Avila, 2015; Hajikhani & Azadi, 2013;), we know the importance of agility (Campos et al., 2013; Martin, 2012; Roberts & Grover, 2012; Zhenhua, Jie, Sisi, & Xia, 2017), we know the impact of information security breaches and how to properly secure them (Aamir, Poncela, Uqaili, Chowdhry, & Khan, 2013; Almalawi, Yu, Tari, Fahad, & Khalil, 2014; Logan, 2015); however, we know little about the relationship between the pressure put on information technology professionals to rapidly deploy these systems to maintain alignment and the challenges faced by information security professionals to adequately secure these environments.

Purpose of the Study

This study seeks to explore the extent of the relationship, if any, between security efficacy, agility, and strategic alignment. By exploring the extent of the relationship, if any,

between security efficacy and strategic alignment, empirical data can be used to show additional benefits of security efficacy. Understanding the extent of the relationship, if any, between agility and strategic alignment, will emphasize the need for businesses to sense and respond to changing business conditions efficiently.

Istikoma et al. (2015) offered that security efforts that do not enable or support business objectives resulted in initiatives aimed at controlling investments in security and a focus on risk prevention. Further, Tu, Yuan, Archer, and Connelly (2018) offered that information security is often not linked to enabling the business to complete strategic objectives, but focused on attack prevention and mitigation; the authors noted that this disconnect resulted in the ignoring of security risks. By studying the impact of security efficacy in addition to agility, their impact on strategic alignment can be more clearly understood.

Tallon and Pinsonneault (2011) suggested that future researchers focus on the impact of alignment in dynamic business environments. Agility, as previously noted, is the ability to respond to rapid change. Enforcing security in agile work environments can be challenging (Istikoma et al., 2015). In dynamic environments, timely communication of changes, in addition to the ability to effectively implement secure solutions allows organizations to respond appropriately and securely to changing market conditions. ICS environments often have relatively static environments (Cook et al., 2017), but new business acquisitions and business moves require that security be ready at a moment's notice to facilitate the business executing strategic objectives (Istikoma et al., 2015). This research seeks to close the gaps caused by (a) business pressure to stay aligned, (b) the need for agility while responding to rapidly changing market conditions, and (c) the ability to securely venture into new markets in the face of persistent security threats.

This study will extend the theoretical constructs of the SAM created by Henderson and Venkatraman (1993) to encompass information security and agility in the model's original foundational components of business strategy, information technology strategy, organizational infrastructure and process, and IT infrastructure and process. This research will contribute to theory by identifying the impact if any, security efficacy and agility have on an organization's ability to maintain strategic alignment.

Significance of the Study

The contribution to the field of Information Assurance and Cybersecurity provided by this research includes an understanding of the impact that together with agility, security efficacy has on strategic alignment in ICS environments. An understanding of the link between these constructs provides additional considerations that must be understood to properly secure business transactions (Yaokumah & Brown, 2014). Information security's primary goal must be to protect the business while enabling the business to meet its strategic objectives (Istikoma et al., 2015). An understanding of the constructs of agility and strategic alignment helps broaden the focus of security professionals from prevention and risk mitigation (Tu et al., 2018) to strategic business enablement in a secure fashion.

In the field of IT, providing the extent of the relationship, if any, between security efficacy, agility, and strategic alignment aids in understanding how security efficacy and agility may contribute to strategic business/IT alignment in ICS environments. Understanding the link between security efficacy, agility, and strategic alignment helps businesses securely venture into new markets. By adding the element of security efficacy, securely entering new markets is enabled while maintaining strategic alignment.

Research Questions

The research questions, guided by theories in integrated systems theory, agility, and strategic alignment, provide the guardrails for this study. The questions sought out relationships between themes in literature. This study will extend the theoretical constructs of the SAM created by Henderson and Venkatraman (1993) to encompass information security and agility in the model's original foundational components of business strategy, information technology strategy, organizational infrastructure and process, and IT infrastructure and process. This research will contribute to theory by identifying the impact that security efficacy and agility has on an organization's ability to maintain strategic alignment in ICS environments.

For this study, exploration of two independent variables and one dependent variable outline the structure of the relationships. Trochim (2006) asserted that when predictor variables alter outcome variables, the relationship is said to be causal. The independent variables, agility and security efficacy, are measuring an organization's ability to respond to competitive actions initiated by competitors and effectiveness of security controls respectively. The dependent variable, strategic alignment, measures the amount of alignment between IT and business strategies. The following questions guided this research

1. What is the extent of the joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments?

    $H_0$1. There is no statistically significant joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments.

    H_a1. There is a statistically significant joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments

Sub Questions

Two additional sub-questions specifically addressed the relationship between the independent and dependent variables.

2. What is the extent of the relationship between agility and strategic alignment in companies that have industrial control environments?

   $H_0$2. There is no statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

   H_a2.There is a statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

3. What is the extent of the relationship between security efficacy and strategic alignment in companies that have industrial control environments?

   $H_0$3. There is no statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

   H_a3.There is a statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

Definition of Terms

Agility – The ability of IT to quickly respond to allow the business to respond to changing market conditions or competitors (Roberts & Grover, 2012).

Distributed Control System (DCSs) – A type of ICS that is used to control production systems within the same geographic location.

Industrial Control Systems (ICSs) - Real-time systems used to control and monitor industrial plant functions.

Operational Technology – The use of technology to sense and detect changes in operational environments (Kuusk et al., 2013).

Programmable Logic Controller – A type of ICS that utilizes a microprocessor with memory to carry out logic functions to control distribution system***s.***

SCADA – Supervisory Control and Data Acquisition – a type of ICS that is used to manage and monitor systems across multiple geographic locations.

Security Efficacy – The effectiveness of implemented security controls to prevent abuse of IT assets (Kankanhalli, Teo, Tan, & Wei, 2003).

Strategic Alignment – The extent to which IT supports the business strategy, and the business uses IT to complete strategic moves (Huang, 2012).

Research Design

This research seeks to explore the extent of the relationship, if any, between security efficacy, agility, and strategic alignment. This study's focus on *the what* and the measurable context of *extent* utilizes a quantitative approach. The use of observation and measurement aligns with the post-positivist view and is the philosophy employed in this study. The research goals require the use of closed-ended questions, the collection of data through surveys, and consideration for the hypotheses this study seeks to answer, resulting in a quantitative approach, an approach that will produce the required knowledge.

Bhattacherjee (2012) declared that non-experimental research is a term that is often used to describe research where treatments are not employed such as correlational studies, survey research, and observational research. This study will use a non-experimental correlational design. This design is appropriate when exploring the relationship between variables without specifying a direction. Surveys were used to collect data from participants. Similar studies have used surveys as the data collection tool for correlational studies (Gerow, Thatcher, & Grover, 2015; Yaokumah & Brown, 2014). This exploratory correlational model used multiple regression for

analysis. The use of multiple regression applies when several predictor variables are thought to have an impact on the outcome variable (Bhattacherjee, 2012; Field, 2013). Figure 1 represents the theoretical model for this study.

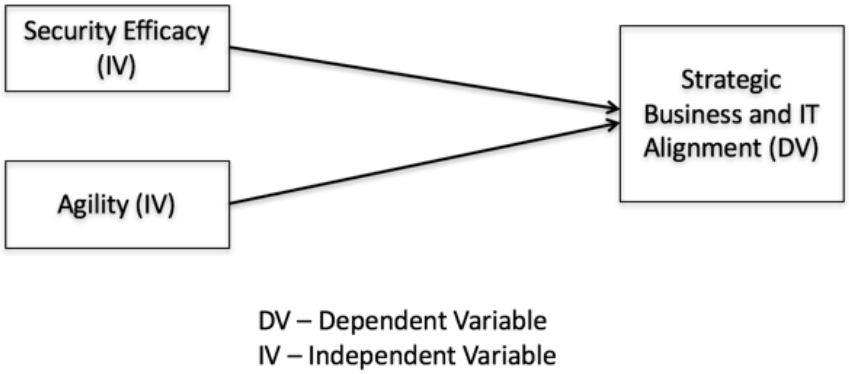

Figure 1. Construct relationship

This study targeted professionals responsible for securing ICS environments across a variety of industries. The population for this study included industrial positions such as control engineers, technicians, and operations positions across a variety of industries that utilize ICSs such as energy, manufacturing, and distribution. Cint's database of industrial positions provided the sample frame for this study. Probability-based random sampling was used to select participants from the sample frame.

Assumptions and Limitations

Assumptions

One of the assumptions in this study is environments that use ICSs have achieved strategic alignment between business and IT, deriving the most value out of infrastructure investments. As noted by Kuusk et al., (2013) this alignment is vital for optimal value generation

in ICS environments. Furthermore, the second assumption suggests that these environments, due to the sensitive nature of critical infrastructure, place security as a top concern. A third assumption is ICS environments are sensitive to competitive actions that threaten market positioning. The fourth assumption is that corporate governance structures exist in the respondent's environment with operational and business technology units operating as separate entities with the common goal of protecting business and information assets. Yaokumah and Brown (2014) offered that security of information assets is an integral part of corporate governance.

Limitations

This study's focus on US-based ICS environments in municipalities, energy, manufacturing, and a variety of other industries limits the ability to apply the results to ICSs globally. Additionally, the collection of results via survey does not guarantee respondent participation (Fowler, 2009). Another limitation is that survey responses can only speak to the observed relationships between the constructs. The data collected only measured the perception of the participants and does not correspond to absolute values of the measured constructs.

Finding respondents with ICS experience was difficult because traditional IT job titles do not apply in operational environments. The same personnel setting up platforms in operational environments, in some cases, also support IT. For example, some companies utilize IT personnel to operate their ICS environments, while others use industrial control engineers/operators or process automation technicians. A broader population that represented job titles used by NIST SP 800-82 (Souffer et al., 2015) was selected, and additional qualifying questions were asked to remove unqualified candidates. In this case, explicitly identifying IT as a pool in a survey respondent tool has the potential to exclude valuable participants. Finally, the sensitive nature of

security efficacy has the potential to elicit extreme reactions with those charged with care and feeding of systems providing this function. Bhattacherjee (2012) offered that social desirability bias, where respondents tend to "spin the truth" to avoid negative comments about work environments, is common in survey research and hurts the validity of results.

Organization of the Remainder of the Study

The remainder of this study follows with Chapter 2 providing a review of theories in strategic alignment, security efficacy, and agility along with a review of ICSs and recent cyber-attacks. Chapter 3 will provide additional information on the research methodology, research questions, and hypotheses used to conduct this study. Chapter 4 provides an analysis of the results received from the surveys while also covering a variety of statistical tests used to explain the direction of the relationships among constructs. Chapter 5 will close the study while explaining the results, highlighting conclusions, and addressing implications for additional research.

CHAPTER 2. LITERATURE REVIEW

Boell and Cecez-Kecmanovic (2010) offered that literature reviews are instrumental in collecting and synthesizing information in research projects. This project used the literature review as a method of finding gaps in the literature and framing existing knowledge on the topics under review. This literature review will cover the evolution of strategic alignment, agility, and security theory into real-world concepts measurable in businesses today. This review will discuss the application of the concepts in ICS environments along with three different types of ICSs. This review will also provide examples of attacks in addition to suggested methods of protecting ICSs. This chapter will discuss potential gaps in the literature followed by future considerations for ethical concerns. Additionally, a consolidated review of these constructs applied to ICS environments provides potential contributions to future research. This chapter will close with a critique of previous research, findings, and a summary of the information provided.

Methods of Searching

The research questions guided this research by providing constructs for review. Literature from various IT domains provided a broader view of the constructs used in this study. Keyword searches, using the constructs and their synonyms, utilizing Boolean search operations were used to provide relevant articles in online databases. The abstracts of potentially relevant articles were searched for keywords to speed up the identification process. Further analysis of identified articles ensured the selected content enhanced understanding. Relevant articles were then digested, sorted, and saved.

Key themes among the articles were noted and further categorized. Appropriate theories were identified to help test the proposed research questions. Google Scholar and the Capella Library were the primary data sources used. In the case of Google Scholar, Ulrich's Web aided

in validating whether an article had been peer-reviewed. An example of search strings that yielded results followed this format: Example 1- (busine*) AND (techno*) OR (information*) AND (align* OR integra* OR strateg*). Example 2 - (busine*) AND (techno*) OR (busine*) AND (information*) AND (align* OR integra* OR strateg*) AND (qualita*). Bhattacherjee (2012) noted that utilizing the patterns above allows for adjustment to widen or narrow results. ENDNOTE and Microsoft OneNote were used to save articles of interest. Saving the articles to OneNote allowed for easy editing and classification/grouping of articles along with the ability to save PDF printouts with notes included. ENDNOTE also allowed for searching specific sections of archived articles. Use of these tools allowed for flexible searching on portions of documents in the data library that ultimately resulted in precise data captures.

Theoretical Orientation for the Study

Business Transformation

The use of IT in manufacturing processes is a well-documented practice that is used to aid in modeling and analysis, which are tools used to transform manufacturing processes (Davenport & Short, 1990). Modeling and analysis have allowed for the evaluation of proposed manufacturing process changes in real-time to review expected results before implementing changes. Davenport and Short (1990) noted that the use of IT to reshape work processes had primarily taken place in manufacturing environments; its utility in office environments, up to that point, had been to increase the speed in which work was completed.

Against the backdrop of insignificant productivity gains from investments and increasing amounts of office work, Davenport and Short (1990) completed a study that sought to introduce the concept of using IT to help transform business processes in non-industrial environments. The authors noted that IT could do more than increase the completion rate of redundant functions, it

could reshape business processes in the same fashion as demonstrated in manufacturing environments.

Business processes, characterized by having recipients and crossing business lines, are defined as a series of related tasks that result in pre-determined business objectives (Davenport & Short, 1990). Business process examples can include things such as order entry, employee vacation requests, requisition of supplies, and submittal of travel expenses for reimbursement. Davenport and Short (1990) posited that the majority of business processes existed before the use of IT in business systems was prevalent, further contributing to the potential for duplication of efforts and lacking the view of a bigger picture to enhance the flow of work versus increasing the volume of work.

Davenport and Short (1990) asserted that the redesign of business processes must follow five steps (a) developing business vision and process objectives, (b) identifying processes to be redesigned, (c) understanding and measuring existing processes, (d) identifying IT levers, and (e) designing and building a prototype of the process. Despite the use of IT to transform business processes, several issues can remain and must be addressed to ensure continual improvements. Davenport and Short identified remaining items such as (a) management's role in new business activity, (b) the definition of new structures, (c) required skills, (d) a functional view of IT to enable the business, and (e) the direction for IT as items that need continuous improvements.

With this work, the authors redefined the concept of using IT to help engineer business processes and coined IT and business process redesign. From the beginning, the authors noted that, without management support, the effort would not succeed. Ironically, the authors also noted that this process must be iterative to sustain the ever-evolving rate of change within IT.

Davenport and Short closed with the notion that companies that could reshape business processes around IT would be successful. This shift allowed IT to enable the business to meet objectives.

Strategic Alignment Theory

Despite the work completed by Davenport and Short (1990), the expected value from IT investments did not materialize; in fact, substantial investments in IT were considered to have aided in the demise of the services sector (Roach, 1990). Henderson and Venkatraman (1993) set out to address the issue of IT not meeting the needs of the business. During that time, the role of IT in supporting business strategies was apparent, but IT's ability to influence strategies was still limited (Henderson & Venkatraman, 1993). The researchers eventually presented the strategic alignment model (SAM). The authors noted their desire for the SAM to be used as a reference model for using IT to transform the marketplace.

Henderson and Venkatraman (1993) attributed the concept of strategic alignment to the ability of a company to create a support structure for the products that it markets and its ability to respond to imitation by competitors. This concept introduced the shift of using IT for productivity gains to use as a means of enhancing competitive advantage; strategic alignment is a process that requires exploitation of IT capability. The assumptions of strategic fit and functional integration create the foundational basis for the SAM. The process of strategic fit encourages companies to look at the market in which their products are positioned to focus on strategies aimed at segment differentiation, otherwise known as external domains, as well as internal domain functions that determine administrative functions to support delivery of organizational objectives (Henderson & Venkatraman, 1993). Henderson and Venkatraman offered that this lack of alignment between business domains and IT strategy is the reason for unrealized value in IT investments.

Functional integration is the process of aligning IT and business strategy; this is not a new concept. Henderson and Venkatraman (1993) noted that most of the current research, at that time, focused on aligning IT with internal domain functions. This operational integration is crucial, but it does not allow IT to aid in shaping and transforming business strategy. Strategic integration creates the link between business strategy and IT strategy that allows IT to enable the business to execute and carry out its strategic objectives, thus enhancing external positioning and competitive advantage (Henderson & Venkatraman, 1993). It is the addition of strategic integration that completes the picture in utilizing IT to fully exploit fluctuations in market trends and mitigate the impact of market imitations. The SAM remains a priority for businesses today and continues to serve as a reference for aligning business and IT strategy (Coltman et al., 2015; Wu, Straub, & Liang, 2015).

The work of Henderson and Venkatraman (1993) continues to influence how IT can shape the business. This seminal work has been used as a foundational reference for using analytics to enhance strategic alignment and business transformation (Shanks, Bekmamedova, & Willcocks, 2013), using IT governance to enhance organizational performance (Hajikhani & Azadi, 2013; Wu, Straub, & Liang, 2015), and has been used to expand into additional theories relating IT to business profit mechanisms (Drnevich & Croson, 2013).

Implications. Four significant implications result from this model. The first is IT's inability to generate value for the business due to a misalignment of IT and business strategy. Second, managers need to re-invent the purpose and reach of a firm's IT strategy. The assumption is born from the need to focus on internal and external domains (Henderson & Venkatraman, 1993). Without focus, IT cannot position the business to capitalize on market opportunities. Third, performance metrics for IT must focus on enabling the business to meet its

objectives. Henderson and Venkatraman offered that IT's ranking factors should encompass the ability to provide a competitive cost structure, deliver top-notch service, create a market reference that positions IT as a profit center, and act as an investment center through seeking out technologies and training to enhance IT competence. Finally, managers must understand the ever-changing nature of strategy. Henderson and Venkatraman (1993) claimed that continual reassessment of strategy is essential in remaining competitive.

Agility Theory

Henderson and Venkatraman (1993) offered that aligning IT strategy to external business domains positions companies to utilize IT to respond to market conditions. Sambamurthy et al. (2003), a seminal work, postulated that firms that wish to build competitive advantage must find ways to detect changing market conditions and respond to those changes. The authors went on to note that agile firms can sense opportunities and a company's degree of agility determines its ability to respond to changes via value creation and innovation in market space and differentiation. Tallon and Pinsonneault (2011), who used Sambamurthy et al. (2003) to define agility, declared that, regarding priority, agility offers benefits that cement its ranking next to aligning IT and business strategy. IT as a strategic differentiator, as described by Henderson and Venkatraman (1993), is realized and Sambamurthy et al. (2003) offered that this emergence has generated a desire to understand how IT influences firm performance. It is evident that IT has transitioned from evolving processes and methodology in industrial environments (Davenport & Short, 1990) to a strategic enabler of business processes (Henderson & Venkatraman, 1993).

To help with this understanding, Sambamurthy et al. (2003) presented a model that explains the strategic role of IT through an examination of factors that impact firm performance; more specifically, the authors posited that dynamic organizational capabilities such as agility,

digital options, and entrepreneurial alertness along with calculated processes like capability building, entrepreneurial action, and co-evolutionary adaptation impact could predict firm performance. The model's foundational theories of IT management, entrepreneurship, and strategy to define IT's role in agility highlight the relationship between agility and competitive action with the entrepreneurship while using resource and capabilities strategy. The convergence of these themes aids in defining the role that organizational capability and strategic processes play in firm performance (Sambamurthy et al., 2003). This seminal work lays the foundational model for companies that wish to use technology to sense and respond to market changes.

The theory uses the following constructs

Dynamic Organizational Capabilities

- Agility - as the ability to use existing customers, partners, and processes to respond to market changes.
- Digital options - describe a firm's ability to exercise known capabilities to capture value
- Entrepreneurial alertness - a firm's ability to seek out and capitalize on new opportunities.

Strategic Processes

- Capability building – uses the logic of leverage and represents relationships amongst competence, digital options, agility, and entrepreneurial alertness.
- Entrepreneurial action – uses the logic of opportunity to describe how firms exercise their capabilities for competitive action.
- Co-evolutionary adaptation – the process of learning over time and that causes companies to launch competitive products as a result of digital options (Sambamurthy et al., 2003).

Seminal work from Ferrier, Smith, and Grimm (1999) offered that when companies produce product or service innovations that change the market landscape, also known as competitive actions, disruptions occur that allow initiators to capitalize on a brief period of enhanced financial gain until the market adjusts and identical offerings are made available. Companies can initiate competitive actions in multiple product lines with varying degrees of quality. Sambamurthy et al. (2003) used the number and quality of competitive actions to rate IT competence, a measure of a company's capability to utilize IT assets to realize strategic IT-based innovation; a higher IT competence results in a more significant number of competitive actions with varying degrees of complexity.

Sambamurthy et al. (2003) highlighted their intent for this model's use as a tool to explore, test, and grow future research in the relationship between IT investments and firm performance. This work has served as a foundation for additional works in shaping the role of agility in dynamic environments (Tallon & Pinsonneault, 2011; Tan et al., 2016), using IT as a sensing capability (Roberts & Grover, 2012), and expressing how digital options are reshaping business strategy (Setia, Venkatesh, & Joglekar, 2013).

Implications. There are three significant implications associated with this theory. First, information technology has taken on a role of transforming business strategy to maintain competitive standing in the market through the generation of digital options. Sambamurthy et al. (2003) offered that the execution of frequent and intricate competitive actions, as a result of a high degree of IT competence, reinforces the role IT plays in an organization's degree of agility. Second, the evolution of IT investments, organizational capabilities, competitive actions, and firm performance highlights a perspective that showcases the value of periodic reshaping of capabilities and conduct (Sambamurthy et al., 2003). The final implication highlights the value

of learning. Through the observation of the consequences associated with competitive actions, decisions can be made to repeat or modify capabilities.

Integrated System Theory

Seminal work completed by Hong, Chi, Chao, and Tang (2003) defined security as a collection of systems with the common goal of protecting the integrity and privacy of an organization's information assets. Managing the collection of resources charged with this task requires a variety of approaches. According to Hong et al. (2003), extant literature, before 2003, gave little guidance for a framework that encompassed management of a holistic information security management theory. To address the lack of a holistic framework, Hong et al. (2003) desired to create an integrated theory that combined elements of information policy theory, risk management theory, control and audit theory, management system theory, and contingency theory to lay a theoretical pinning that aids in understanding managerial obstacles, predicting effectiveness, and the modification of strategies.

The key points from each theory are summarized below

- Security policy theory – the process of planning, gaining consensus, drafting, implementing, and periodic review of information security requirements
- Risk management theory – the use of risk analysis and assessments to predict information security vulnerabilities
- Control and audit theory – the process of an organization creating security control systems with audit controls designed around measuring the performance of the control
- Management system theory – the belief that an organization should create and maintain an information security management system to protect assets

- Contingency theory – the process of utilizing information security as a contingency plan that is meant to prevent, detect and react to internal and external threats (Hong et al., 2003, p. 243).

Hong et al. (2003) offered that their approach to this theory is to thoroughly explain a smaller scale theory and extend it to similar domains. The component theories share a theme of protecting data, but alone, no one theory is enough to cover all areas. Hong et al. (2003) postulated that an integrated system theory based on contingency management combines components of the member theories of security policy, risk management, control and audit, and management systems to form a robust framework. By focusing on fast-paced environments, sequential management and contingency processes, management feedback loops, and linking managerial activities to organization objectives, a more holistic theory exists inherently. The result is a theory that contributes strategies and procedures, provides an understanding of an organization's behavior toward an information security strategy, and serves as a building block for further research (Hong et al., 2003).

The work provided by Hong et al. (2003) has served as an underpinning for the transition of the business footprint into unprotected areas (Kruger & Noxolo Mama, 2012). It has also been used as a model for assessing security in manufacturing environments (Ismail et al., 2014), and as a reference to understand the impact of security on supply chain performance (Pn, 2014). The above works showcase the theory's relevance in a wide range of security perspectives further highlighting the importance of an integrated theory on future research initiatives. Hong et al. (2003) supported the use of their study in furthering research by noting it offers enhanced understanding for security professionals in different settings.

Implications. The integrated system theory and its component theories address implications and gaps within its member theories. First, information management and techniques are crucial to contingency management in dynamic environments. Second, the combination of ordered management and contingency processes produces a holistic focus on security, risk management, control and auditing, and security management activities. Information security is a function of security policy, risk management, internal control, information auditing, and contingency management (Hong et al., 2003). Third, periodic information security management cycles replace the notion of static policies. Hong et al. (2003) declared that feedback received during this cycle could serve as input for the management process. Finally, managerial security activities could be ordered sequentially and connected to organizational objectives.

Connections between Theories

The basis for the integration of these theories into a work regarding the relationship between security efficacy, agility, and strategic alignment in industrial environments is vital for a variety of reasons. The theories of alignment and agility work well together as IT is used to transform business strategy and enable companies to sense and detect shifts in market positioning that allow for the recognition of product vacancies and saturation based on customer trends. Henderson and Venkatraman (1993) declared that if a business indeed invokes market-changing products or services, the market will respond with imitations, a condition that requires a response to maintain competitive advantage and market relevance. Sambamurthy et al. (2003) suggested that the initiation of change and the response to market imitators is defined as a competitive action, also adding that IT influences the quality and complexity of the competitive action initiated as a response. When IT and business strategies are aligned, the business can use IT to sense and respond to competitive actions, thus making a firm agiler. Henderson and

Venkatraman (1993) based strategic alignment on the concept of a business building a support structure for its products and being able to respond to imitators.

Strategic alignment remains a top concern for executives (Wu, Straub, & Liang, 2015). Understanding the need to remain agile while maintaining strategic alignment is critical for companies that wish to stay competitive. Competitive advantage cannot be delivered by systems only; an organization's ability to exploit IT over a sustained period can aid in achieving key market positioning (Henderson & Venkatraman, 1993). Positioning is critical in competitive markets, and agility theory and strategic alignment well highlight this fact. Sambamurthy et al. (2003) suggested that the logic of positioning refers to a firm's ability to execute moves that enable market differentiation and uniqueness. The use of IT to execute these moves is in alignment with the strategy provided by Henderson and Venkatraman (1993) regarding the advantages afforded when market positioning relies on IT.

Companies are using IT to enable strategic objectives and enhance competitive advantage (Apol et al., 2013; Cao, Baker, & Hoffman, 2012; Gerow, Grover, Thatcher, & Roth, 2014). As reliance on IT to enable business objectives continues to increase, business transactions are quickly expanding outside of carpeted spaces into a digital arena that is plagued by security threats (Aleem et al., 2013; Otero, 2015; Schiavone, Garg, & Summers, 2014). Additionally, this digitization changes the definition of business assets. Yaokumah and Brown (2014) asserted that information assets are items of a defined value such as humans, technology, digital, or other.

With businesses increasingly shifting toward digital transactions, protection from would-be criminals becomes vital. Further, Schiavone et al. (2014) reported that technology enables expansion of criminal behaviors at a global level. Despite the protection of the business having the highest priority within any information security program, the lack of management support in

enabling security to achieve this goal has resulted in unsuccessful security initiatives (Istikoma et al., 2015; Schiavone et al., 2014). Management must be able to weigh the goals of the business with the need to conduct transactions securely. The authors of a tool to measure the effectiveness of a company's security controls, Kankanhalli et al. (2003) asserted that the lack of a comprehensive information security management strategy leaves companies without a mechanism to measure the effectiveness of security tools. Schiavone et al. (2014) claimed that the frequency, amount of data stolen, and inability to deter information security incidents highlight the fact that, given the advances in technology targeted at detection, companies are ill-prepared.

The strategic alignment and agility theories presented do not account for the aspect of security in a non-secure transaction-based arena, the effectiveness of security controls, or the increasing amount of attacks on digital information. Integrating the security aspect into agility and alignment theory presents a new dynamic where secure business transactions occur without putting the business at risk, and agility maintains its standing with alignment without the sluggishness with the misalignment of business, IT, and security strategy.

Review of the Literature

Importance of Alignment

To get an idea of the correlation between IT investment and employee productivity, Apol et al. (2013) completed a study that compared the two variables, IT investment and employee productivity. Although a linear correlation between IT investment and productivity could not be defined, a positive correlation existed between productivity and the capability and ability to support investments. Additional studies have tried to glean a correlation between alignment and

productivity.

Gerow et al. (2014) conducted a meta-analysis to test if alignment hindered or aided firm performance. The findings of the study more clearly predicted the relationship that Apol et al. (2013) tried to establish a year earlier. A meta-analysis of 78 articles showed statistical evidence that firm performance did increase, but the authors noted uncertainty with the conclusion due to the many factors affecting alignment. Differing from the predictions made by Apol et al. (2013), this study noted that no paradox in alignment exists.

Drnevich and Croson (2013) posited that the impact IT has on a company's ability to generate profit is the only accurate measure of success. Drnevich and Croson supported the notion that IT must be used to develop a business-level strategy but also highlighted the difficulty in measuring the direct benefit of investment in IT. This view differs from those that seek to measure the usefulness of IT regarding employee productivity (Apol et al., 2013; Gerow et al., 2014), in that the research seeks to quantify IT regarding its ability to shape business-level strategy. Despite the viewpoint offered, there are no guarantees offered regarding the ability of IT to reshape the business and increase profit mechanisms.

Several articles have noted IT/business level integration failures despite alignment of business and IT strategy. Hajikhani and Azadi (2013) sought to address the failure of IT projects within organizations despite alignment of business and IT strategy. More specifically, the authors were looking to determine the impact of IT governance on business and IT alignment. Hajikhani and Azadi (2013) offered that the purpose of their correlational study was to determine the impact of traditional alignment, as determined by governance and maturity models, on technology delivery mechanisms. The authors used a web-based survey to collect data from hospital business and technology executives in Tehran. The authors noted the experimental

nature of the study and its roots in positivist research.

The work of Hajikhani and Azadi (2013) is impressive because IT governance is a vehicle that is used to ensure alignment between business and IT strategy. The results were put into a balanced scorecard to understand the correlation between variables. The work conducted by the authors is one of a few studies that utilized a balanced scorecard approach to allow for classification of IT and business indicators (Hajikhani & Azadi, 2013, p.531). The research showed that IT governance structures alone did not have a strong enough impact on the results.

In ICS environments, strategic alignment is a crucial strategy that drives optimal profit returns (Gonzalez-Benito & Lannelongue, 2014; Kussk et al., 2013). The use of equipment in addition to equipment replacement intervals are all part of an integrated strategy. Gitzel, Schmitz, Fromm, Isaksson, and Setzer (2016) offered that alignment is critical to lifecycle management and the optimization of long-term planning. When IT strategy is aligned to support operational objectives in ICS environments, companies are better positioned to increase firm performance (Asgarkhani & Sitnikova, 2014; Sardana, Terziovski, & Gupta, 2016). The value provided by strategic alignment in ICS environments can vary based on how the IT organization is positioned to support the business. Siurdyban (2014) offered that in environments where the localized business units are allowed drive development, the focus switches from whether IT is centralized or decentralized to a model to where decisions are centralized where needed. This localization of technology innovation allows alignment tailored to the supported business unit.

Strategic alignment in ICS environments extends to the types of IT used to support the business. Goepp and Avila (2017) offered that in ICS environments, the links between the business, IT solutions, and the operating domain be well understood at an operational level to derive the most value from deployed solutions. This alignment is necessary to ensure the

business need is understood and, the proposed technology solves a business problem. Additionally, Alcaraz and Zealy (2013) offered that alignment through governance is mandatory for any critical control system. Governance is responsible for ensuring that the alignment between business and IT supports the completion of strategic objectives in ICS environments.

Agility

Tallon and Pinsonneault (2011) asserted that agility is as necessary as aligning IT and business strategy. While noting the importance of alignment of business and IT strategy, the authors offered that, in the face of disruptive change, possessing the ability to deliver appropriate responses is as important as alignment. The introduction of this component adds another factor in stark contrast to the original intent of the strategic alignment model. Tallon and Pinsonneault (2011) base their findings on results taken from a study of 1600 of 2800 firms in the S&P index with profits ranging from $300 million to under $3 billion.

Roberts and Grover (2012) took a different approach when defining agility, thereby, introducing a new dimension in the equation of the impact of agility on strategic alignment. Roberts and Grover (2012) aligned with Tallon and Pinsonneault (2011), whom all used Sambamurthy et al. (2003) for theory testing when defining agility as the ability of a company to respond to unanticipated change. Roberts and Grover add that organizations must be able to take advantage of social mediums to detect and respond to changes in customer trends. This view suggests that IT infrastructure could detect those changes. Although the approach and application of IT to aid in agility differ, this research does help define another variable in the dimension of the agility argument.

The link between IT infrastructure and agility as defined by Sambamurthy et al. (2003) automatically extends to industrial environments that use IT infrastructure. Martin (2012) offered

that the ability to quickly respond to market fluctuations is key to profitability in industrial companies. Additionally, agility in ICS environments is vital for capitalizing on market opportunities (Campos, Santos, de Souza, & da Silva, 2013). As manufacturing and industrial facilities strive to meet increasing demand and market capitalization, the use of technology in this space goes beyond task completion. Yang (2013) offered that the ability of technology to respond to increasing demand and drive product improvements is now a pillar in the creation of competitive systems in the industrial arena.

Further supporting this view, Zhenhua, Jie, Sisi, and Xia (2017) offered that the agility and responsiveness, spurred by new technology innovation applied to industrial processes, would allow industrial environments to meet new market demands. For example, Oborski (2014) offered that the complex nature of order fulfillment and supply chain management interactions will continue to drive the push for enhanced processing in the industrial control systems space. Technologies that enable this enhanced processing via the use of supply-chain partners continue to evolve outside of the confines of traditional organizations, such as in cloud-hosted facilities that open up new access potential.

Aravind, Sudheer, Vinodh, and Anand (2013) argued that market volatility and customer choice in production environments drove the push to use technology to deliver services to customers faster. The use of technology to predict and meet market swings aligns with the theoretical definition of agility (Sambamurthy et al., 2003). Chiang and Zhang (2016) offered that as computing technology used in industrial spaces continues to evolve, the use of IT to take advantage of gaps in the market enhances with each development. Agility plays a vital role in ensuring industrial processes evolve to meet client demand (Oborski, 2014). The drive to meet

customer demand and the need to innovate continually ensures that agility in ICSs continues to be a top priority.

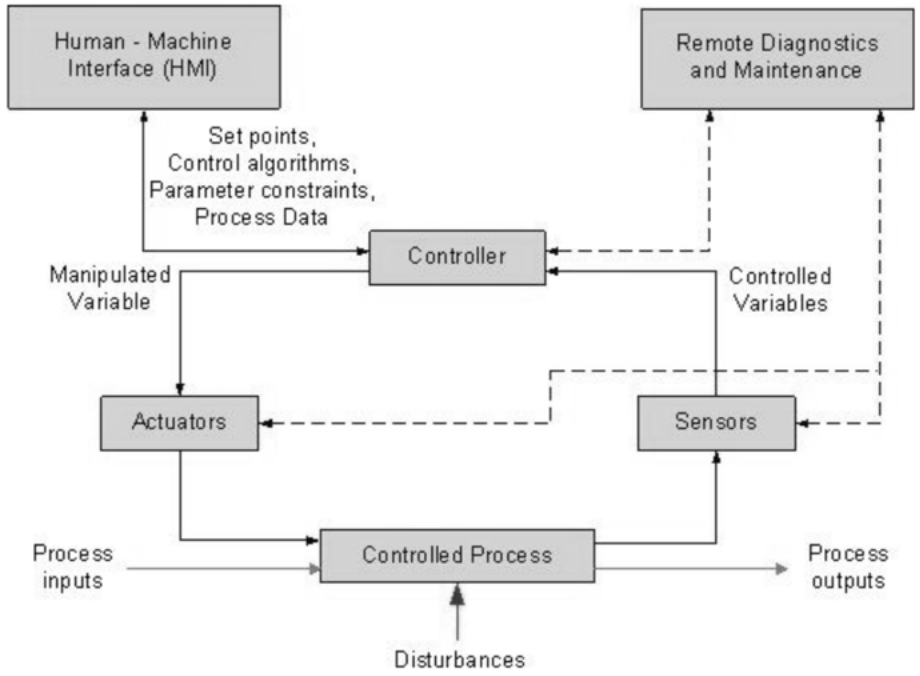

Figure 2. ICS Overview. Reprinted from Guide to Industrial Control Systems (ICS) Security (p. 2-4), by Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A, 2015, S*pecial Publication (NIST SP)-800-82 Rev 2*. Used with permission.

ICS Overview

According to NIST SP 800-82 and ISA-62443, an ICS is a general term used to describe several types of control systems found in industrial, manufacturing, and critical infrastructure environments. Industrial control systems are often proprietary, and many of them have been in service for decades (Janicke et al., 2015). An industrial control system combines an array of components with a common goal of controlling and processing industrial objectives; for example, an objective could be the delivery of water or the creation of energy. (Stouffer et al., 2015). Figure 2 depicts an overview of the components in an ICS.

The process piece of the system is responsible for output while the control component defines parameters for output such as rate. NIST SP 800-82 offered that the control component includes loops that allow for output to be controlled manually, based on pre-configured settings (open-loop), or to be balanced where output impacts input (closed-loop). Knijff (2014) provided a simple explanation of a closed-looped system when he described setting the temperature on a thermostat, and while determining the current temperature, the thermostat can send a signal to turn on or off the central heating/cooling unit. Stouffer et al., (2015) provided the following in NIST SP 800-82 when explaining the primary function of an ICS:

> A typical ICS contains numerous control loops, human interfaces, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. A control loop utilizes sensors, actuators, and controllers (e.g., PLCs) to manipulate some controlled process. A sensor is a device that produces a measurement of some physical property and then sends this information as controlled variables to the controller. The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller. (p. 2-3).

Due to the impact, these systems can have on the health and safety of a community, the best practice is to deploy using safety integrity levels that define the probability of failure (ISA99, 2017). These levels can map to contextual security zones that restrict access between zones to protect the integrity of the industrial process. In the context of ICSs, safety is the removal of variables that can cause injury, death, and render equipment inoperable (Stouffer et al., 2015). The next few paragraphs provide an overview of three types of ICSs, mainly supervisory control and data acquisition (SCADA), a distributed control system (DCS), and a programmable logic controller (PLC).

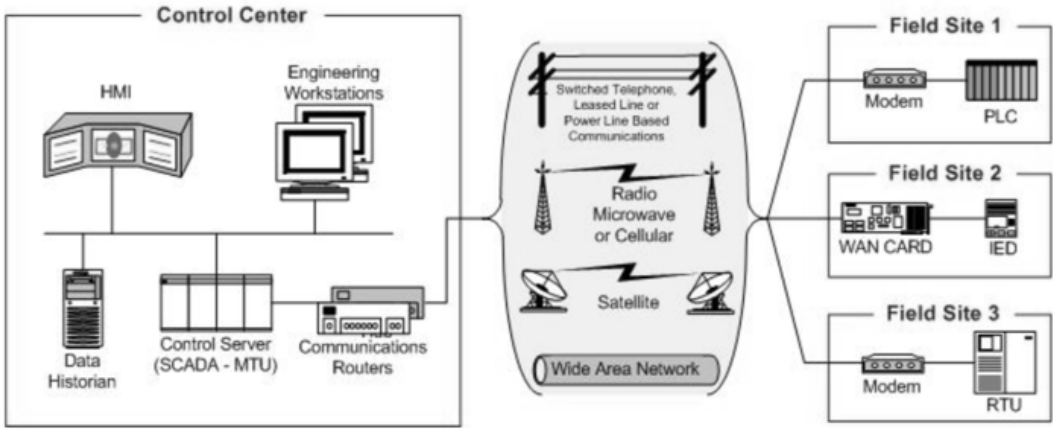

Figure 3. Components and general configuration of a SCADA system. Reprinted from Guide to Industrial Control Systems (ICS) Security (p. 2-6), by Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A, 2015, S*pecial Publication (NIST SP)-800-82 Rev 2*. Used with permission.

SCADA. Supervisory control and data acquisition (SCADA) systems are a type of event-driven ICS that enables centralized data acquisition and control where control of geographically dispersed assets is necessary (Cherdantseva et al., 2016; Obeid & Dhaussy, 2016; Sajid, Abbas, & Saleem, 2016; Stouffer et al., 2015). SCADA systems enable remote management of ICS functions. The utility of SCADA systems has helped propel their growth from disconnected local systems primarily used by engineers to automate plant functions to a fundamental corporate system (Asgarkhani & Sitnikova, 2014).

SCADA systems can remotely control and monitor assets while maintaining a centralized data acquisition model. NIST SP 800-82 offers that this capability enables centralized monitoring and control for any number of inputs and outputs across diverse geographic regions (Stouffer et al., 2015). SCADA systems often include communications equipment such as modems for connectivity to other sites, a control server for data processing, historians for log

collection, and PLCs or remote terminal units (RTUs) that are used to control physical actuators or monitor sensors (Bagri et al., 2014; Obeid & Dhaussy, 2016). This monitoring capability enables remote status reporting of several ICS components. SCADA systems can monitor operating elements such as temperature, fluid levels, vibration, acoustics, surface characteristics, and a host of other parameters (Oborski, 2014).

SCADA systems present a unified picture of data retrieved from data acquisition systems, data transmission systems, and human-machine interfaces (HMI). According to NIST SP 800-82, the collected data is often sent back to a central processing station for monitoring (Stouffer et al., 2015). Based on the alerts/events received, responses can be automated such as technician call-outs or system shutdowns. Additionally, these systems report telemetry data back for analysis to aid in failure prevention and usage statistics.

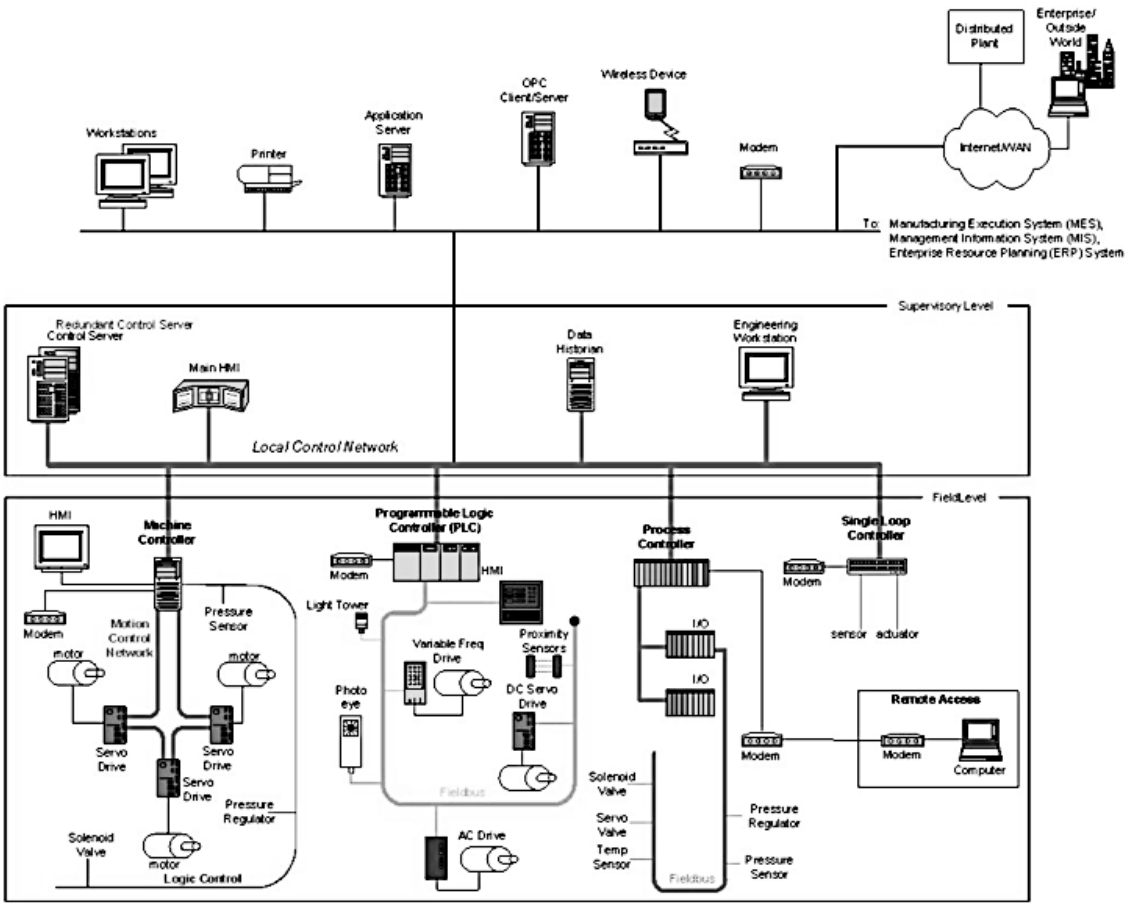

Figure 4. Components and general configuration of a DCS system. Reprinted from Guide to Industrial Control Systems (ICS) Security (p. 2-12), by Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A, 2015, S*pecial Publication (NIST SP)-800-82 Rev 2*. Used with permission.

DCS. NIST SP 800-82 offered that a distributed control system (DCS) uses a variety of host systems to control and process functions within a geographic location such as plants and manufacturing facilities (Stouffer et al., 2015). DCSs utilize a supervisory control-loop to manage the localized controllers required to deliver an industrial objective. Figure 4 depicts an example of a DCS system. This supervisory controller architecture utilizes automated conditional control-loops to ensure that process and control functions maintain defined parameters and

output levels. DCSs are process-oriented systems (Alcaraz & Zeadally, 2015). PLCs are used to maintain the defined tolerances and are responsible for corrections should disruptions occur. Business level views of production systems are provided by connecting these systems to corporate networks. NIST SP 800-82 noted that the distributed nature of a DCS ensures that failures to individual systems minimize disruption to the overall system.

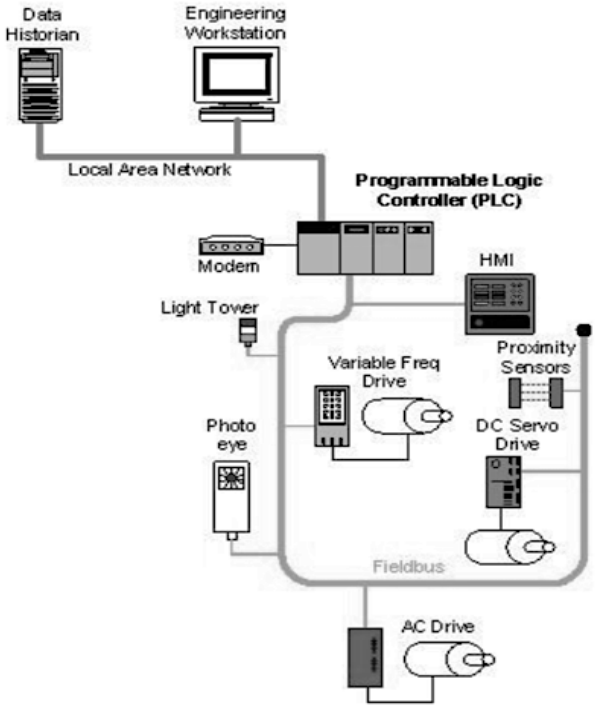

Figure 5. A stand-alone programmable logic controller over a manufacturing process. Reprinted from Guide to Industrial Control Systems (ICS) Security (p. 2-13), by Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A, 2015, S*pecial Publication (NIST SP)-800-82 Rev 2*. Used with permission.

PLCs. A programmable logic controller (PLC) is a microprocessor with programmable memory that is used to control plant processes (Kleinman & Wool, 2014). DCSs and SCADA

systems use PLCs as distributed controllers to manage control loops in hierarchical systems. PLCs collect data as input from sensors, actuators, valves, and a variety of other devices. PLCs operate by scanning inputs against a control-loop and performing actions based on inputs (Aamir et al., 2013). Nawi et al. (2016) offered that PLCs are real-time devices in that outputs must respond to inputs within a defined time frame. PLCs can also serve as standalone controllers for closed-loop control without human intervention as depicted in Figure 5 (Stouffer et al., 2015).

Alphonsus and Abdullah (2016) offered that the scanning and detection function requires that all PLCs have five essential building blocks (a) rack assembly, (b) power supply, (c) programming device, (d) input/out section, and (e) central processing unit (CPU). Alphonsus and Abdullah noted that the blocks performed the following functions

- The rack assembly is a chassis that contains all of the components of a PLC.
- The power supply powers the modules that plug into the chassis.
- The programming device allows an operator to control and enter commands that are processed by the CPU.
- The input/output section is the interface between connected field devices and the CPU.
- The CPU is the brain that controls the logic function of the PLC.

The building blocks combine to create a self-contained unit capable of operating in conjunction with sensors to control an entire manufacturing process. PLC components are typically interconnected using ethernet, radio, or telephone cabling (Janicke et. Al., 2015).

ICS Communication. ICSs work similarly across industries, but there are differences. Based on the industry, systems may need to communicate locally or across geographically dispersed locations. In distribution use cases, communication needs typically span across a

network that covers hundreds of miles. A wide area network (WAN) is best suited to handle communication tasks between geographically dispersed sites. In manufacturing use cases, communication needs remain local to control onsite functions. A local area network (LAN), where bandwidth is more predictable and controlled, is best suited for local network communication needs.

Devices within an ICS network communicate using a variety of communication methods. The communication at lower levels allows for information such as control settings and readings from sensors to be distributed within an ICS network (Ahmed, Obermeier, Sudhakaran, & Roussev, 2017). Serial protocols such as MODBUS, PROFIBUS or DNP3 are used depending on the level of the process. In some cases, these serial protocols are encapsulated in Internet Protocol (IP) and transmitted to other systems over the network. The previously mentioned serial protocols should be constrained where possible due to the lack of security and ease of manipulation. NIST SP 800-82 notes that these protocols should not be allowed to cross from the ICS environment into corporate networks (Stouffer et al., 2015).

Operation Technology and Information Technology

People. One crucial difference between operational and corporate environments is the mindset of the people charged with maintaining and securing technology used to govern the respective environments**.** This mindset difference stems from differences in management practices and use, which ultimately shapes an individual's perception of technology. According to Kuusk et al. (2013), management of information systems in organizations that utilize technologies to control engineering functions is different from that of traditional IT infrastructure systems such as servers, network, and storage because those traditional systems are under the control of a governing body. The engineering control systems are commonly referred to as

operations technology (OT) and are excluded from IT governance. The two environments, OT and corporate IT, are typically separated by the internal customers they support. For example, OT is responsible for supporting internal engineering technology needs such as those found in products plants, manufacturing, or wastewater facilities while IT is responsible for supporting internal corporate technology needs typically found in an enterprise office environment.

Security policy. Aside from differing technology management practices, security policies are also managed differently in ICS environments. Cherdantseva et al. (2016) declared that in ICS environments, integrity and availability come before security. When IT security policies impede operational goals, the business will win as security is not the primary driver. Security approaches in IT environments deliver different results if any when applied to OT (Kuusk et al., 2013). This incompatibility presents an issue when confronted with the current cyber landscape. When ICS and corporate networks connect with different policies and objectives, the potential for mistakes increases significantly if the two environments do not share the same security goals. Additionally, the continuous nature of ICS environments makes timely patching a concern (Ahmed et al., 2012).

Technology. Industrial control systems started off as disconnected systems that were used to manage isolated environments and used proprietary vendor software (Kuusk et al., 2013). Advances in technology continue to change these once disconnected entities into corporate systems. NIST SP 800-82 offered that as ICSs continue to adopt practices that enhance business productivity such as remote access and corporate connectivity, the difference between the computer systems used in corporate and ICS environments becomes increasingly difficult to distinguish (Stouffer et al., 2015). Despite using some of the same systems between corporate and industrial environments, the critical nature of industrial systems mandates that a different

approach to systems management be used (Kuusk et al., 2013). Bustamante, Fuertes, Diaz, and Toulqueridis (2017) offered that the approach used to secure IT systems in corporate environments would be insufficient in an ICS environment.

Several key factors come together to make ICSs different from traditional IT systems. ICSs are time-sensitive and often dependent on connectivity. Minor disruptions in connectivity can result in critical alerts not being processed such as flooding of a wastewater disposal station, an environmental hazard (Stouffer et al., 2015). Additionally, the high-degree of automation in these environments aids in the sensitive nature of these environments. When automated processes fail, preventative actions such as heater shut-off or pump turn-on have the potential for substantial impacts to the surrounding environment (Bambauer, 2014; Stouffer et al., 2015). The result of an IT system going offline is very different from that of an industrial process.

Recent Legislation

In 1998, President Bill Clinton mandated protection of systems that are essential for the continued operation of the economy and government, defined as critical infrastructure, and set up a national Critical Infrastructure Protection program with Presidential Decision Directive 63 (PDD 63) (The White House, 1998). The directive had a defined goal of achieving secure, interconnected systems by 2003 via the establishment of a national notification center and enabling the protection of critical infrastructure. More importantly, the directive noted that specific functions are so critical to the operation of the country that their disruption would impact the well-being of the United States. The directive also set up protected information exchanges between the private sector's Information Sharing and Analysis Center (ISAC) and the public sector's National Information Protection Center (NIPC) to exchange and disseminate discovered

vulnerabilities and threats to industry and the NIPC (He, Devine, Zhuang, 2018). Participation in this exchange was voluntary.

In 2003, President George W. Bush signed Homeland Security Presidential Directive 7 (HSPD 7) which superseded PDD 63 and added sectors for agriculture and national monuments (The White House, 2003). HSPD 7 was intended to identify, prioritize, and protect these systems. The classification of these networks as critical infrastructure mandated protection for systems processing data on the critical infrastructure networks (CIN). This document reinforced information sharing principles defined in PDD 63. The current list of critical infrastructure sectors is on the Department of Homeland Security's website (Department of Homeland Security [DHS], 2017).

In 2013, President Barrack Obama signed Executive Order 13636 (2013) which spurred the creation of the NIST Cyber Security Framework. The NIST Cyber Security Framework presented owners/operators with a flexible, cost-effective approach that, if followed, would instantiate a comprehensive cybersecurity program (Sedgewick, 2014; Stouffer et al., 2015). The NIST Cybersecurity Framework allowed companies to map existing policies to elements in the framework to fill in any gaps in current approaches. The framework is replete with references to ISA 62443, a series of standards for securing ICSs (Cosman, 2014). The voluntary nature of this legislation is not without issues.

Challenges. Unfortunately, there is much debate regarding the ability of frameworks and directives to drive real change. Additionally, Vos, Tjemkes, Klaver, and Verner (2017) highlighted that the voluntary and partnership dependent relationship defined in CIP directives has less than stellar results. One of the concerns with efforts at consolidating policy into a framework is the inability to enforce recommendations. Shen (2014) argued that despite the

inability to enforce compliance with the NIST Cybersecurity Framework, the benefits come from using the framework as a standard to measure the worthiness of a potential value chain partner's cybersecurity programs.

Smaller ICS companies that do not have cyber programs may find the cost of implementing the framework prohibitive. The Department of Commerce suggested that incentives such as cybersecurity insurance, grants, preference for technical assistance, liability limitation in the event of an attack, and investment recovery are provided to incentivize companies to adhere to the framework (U.S. Department of Commerce, 2013). Hellman (2015) questioned the use of incentives as an effective mechanism to drive compliance and noted that despite federal mandates, incentives, and references ICS environments remain plagued by security vulnerabilities (Hellman, 2015). For reference, ICS-CERT reported a 342% increase in the number of investigated incidents in the Communications CI sector between 2014 (14 incidents) and 2016 (62 incidents) (ICS-CERT, 2014, 2016).

Security Concerns

Gao et al. (2014) attributed some of the security concerns in SCADA environments to the need to save money; thus, the adoption of less secure communication protocols, the use of Ethernet, and canned Microsoft Windows installations together present inherent security flaws that contribute to making SCADA systems susceptible to vulnerabilities. To overcome this limitation, Shahzad et al. (2014b) advocated encrypting the communication protocol itself for protection using public key cryptography. This method would ensure that recipients must possess decryption keys to read the data.

Encryption and authorization mechanisms are needed to ensure secure communications between ICS systems components (Gao et al., 2014). In traditional ICSs, system interactions do

not require authentication to interrupt processes; thus systems changes are not authenticated, and external processes can update system variables. More importantly, enterprise level security receives most of the attention, while process control level and system level security concerns are not addressed and are often the target of most SCADA system attacks (Gao et al., 2014). Additionally, software used to monitor SCADA systems uses legacy programming techniques. NIST SP 800-82 offered that modular programming leads to an endless array of patches that are needed to address vulnerabilities (Stouffer et al., 2015). The increased amount of connectivity and constant patching, combined with a system that cannot withstand sustained outages frames support for an increase in cyber-attacks (Cherdantseva et al., 2016).

PLCs interact directly with devices that control production in the field. Manipulation of a PLC can directly impede an industrial process or offer an avenue to rewrite control functions with devastating consequences. Schuett, Butts, and Dunlap (2014) demonstrated manipulation of a PLC when the authors used repackaged firmware to prevent the PLC's owner from regaining control of the device. The ability to manipulate PLC functions combined with research conducted by Enoiu (2015) that detailed the growing popularity of the five languages used to program PLCs, as defined in IEC 61131-3, PLCs are targeted as much as any other network-connected system. Ahmed et al. (2017) offered that PLCs are "…particularly vulnerable to network attacks…" further stressing the vulnerability of these systems (p.23). Additionally, Abbasi and Hashemi (2016) demonstrated an undetectable attack that manipulated the runtime configuration of the input/output pins that did not require any modification of PLC logic. The attack executed by Abbasi and Hashemi is unique in that unlike attacks that prevent operators from regaining control of the PLC, this attack continues to operate with no known indicators of compromise.

DCSs are equally vulnerable to network attacks. DCSs typically connect to a variety of systems that interconnect via a communication network, making them susceptible to attack (Weerakkody, Liu, Son, & Sinopoli, 2017). Further, corporate desktops are used to monitor and share information on the status of DCSs. NIST SP 800-82 noted that operational views are provided to corporate systems via the network (Stouffer et al., 2015). To illustrate the simplicity of compromising an interconnected DCS, Antonioli, Bernieri, and Tippenhauer (2018) provided a framework for creating a botnet that could be used to map and target a DCS environment undetected. The critical nature of these systems mandates the management of security concerns.

Information Security Management

Information security management in process control environments comes after the need for connectivity is met. At all costs, the business must continue; the need to continue in the face of dynamic changes places pressure on security professionals to secure the business without impeding progress (Istikoma et al., 2015). In ICS environments, information security management's purpose readily conflicts with availability during dynamic business cycles (Kuusk et al., 2013). If an attack fails to happen, it is difficult to justify additional expenditures to protect against security threats that, from the business' point of view, do not exist (Bambauer, 2014).

Expanded connectivity to vendors, supply-chain partners, or the Internet in ICS environments enables the business to be agiler and respond more quickly to dynamic business needs. ICS networks by nature require stability (Cherdantseva et al., 2016). The more connected the environment, the more instability increases. Ilves (2016) noted that the uncontrolled expansion of the Internet mandates more awareness regarding cyber vulnerabilities. The goal of security is counterintuitive to allowing more connectivity akin to the differing goals of traditional business' confidentiality needs versus the availability needs of operational ICS environments

(Ginter, 2013). Operational ICS units desire more connectivity in the ICS environments, yet IT's charge is to make the connection between the two networks more secure. When failures and security incidents happen in business environments, at best information is exfiltrated; in ICS environments, the results are catastrophic, and loss of life and harm to individuals and the economy is at stake (Bambauer, 2014; ISA99, 2017 Kuusk et al., 2013).

Isolation

Companies have realized the importance of ICS since inception and have used various methods to keep them separate from general IT systems where remote access is standard. One such method is the use of air gaps. Byres (2013) offered that in theory, an air gap is a security mechanism that is used to provide physical separation between production and business networks. The theory's fundamental principle works on the assertion that an air gap between the business and critical infrastructure networks would minimize the spread of any viruses. Air gaps are still widely used today as a means of masking connectivity or infrastructure to would-be bad actors (Guri, Monitz, & Elovici, 2017). This method of isolation was once the primary security mechanism for SCADA/ICS networks (Ponomarev, 2015). As an example, Byres (2013) referred to a Siemens Security Advisory, a provider of SCADA systems, which suggested the use of an air gap to mitigate risks discovered in one of its ICSs.

Despite air gaps providing the illusion of actual separation between ICS and business owned networks, patching is an eventuality (Byres, 2013). Without a connection between the business and production networks, engineers will eventually use media transfer devices to download and install patches on an ICS (Bambauer, 2014). It is at this point that the introduction of viruses and other types of malware could occur in critical life safety systems that were previously thought to be separated by an air gap. Byres (2013) insisted that in some cases,

systems are genuinely segmented using air gaps, but the National Cybersecurity and Communication Integration Center (NCCIC) reports that during audits of private companies, air gap networks averaged 11 direct connections between the business network and the ICS network.

Hellmann (2015) took a different approach when considering the danger in using air gaps. While noting vulnerabilities in the SCADA pipeline systems, Hellman offered that even with the use of air gaps and other security measures, SCADA systems can be exploited to gain access to corporate resources as well. Hellman's comments did not oppose extant literature but framed the problem in a different direction. Air gaps that are breached not only present problems to industrial systems, but to any system that is on the other side of the air gap.

Byres (2013) posited that all ICSs connect to the Internet at some point and believing that an air gap will protect your network is far more dangerous than any existing vulnerability. Piggin (2014) posited that the safety of these systems is up to the administrators and recommends locking down systems to prevent exploitation. Despite the focus on securing SCADA systems, these systems are routinely compromised (Bambauer, 2014; Dehlawi & Abokhodair, 2013; Hellmann, 2015). Attacks on these systems can have devastating impacts. Shahzad et al. (2014a) attributed the persistent attacks to the lack of proper authentication scheme for SCADA traffic. Due to the number of persistent attacks that have happened despite an air gap, the practice is losing favor.

Security Incidents

One of the more popular cases describing the futility of air gaps was an attack on Iranian centrifuges reportedly coordinated by the US government and the Israeli government called STUXNET. Initially, the attack was code-named "Operation Olympic Games;" analysts appended the name the STUXNET (Berghel, 2015). STUXNET was used to launch targeted

attacks at PLCs in process control environments and was programmed to resemble standard systems calls, limit infection rates to 3 hosts per system, and to uninstall itself on 12 June 2012 (Karnouskos, 2011). The limit on infection rates aided in masking thus, preventing the system from being detected as a worm that quickly spread to other machines. STUXNET caused the readings of monitoring equipment to report normal conditions when they were, in fact, spinning out of control, setting the Iranian Nuclear Program back years (Bambauer, 2014).

Recent attacks such as STUXNET and its close cousins Flame, Duqu, and Gauss have sparked an interest in protecting ICSs (Bencsath, Pek, Buttyan, & Felegyhazi, 2012). STUXNET received worldwide notoriety as being the first attack used as a cyber-weapon and exposed systems worldwide. The cousins are similar in composition and must be "discovered" versus making their presence known (Bencsath et al., 2012). These attacks are classified as malware and are typically used to disrupt normal operations and steal confidential information.

STUXNET was so effective because the Iranian government never considered the potential for a security breach and trusted in the separation provided by the air gap (Bambauer, 2014). Iranian scientists worked on the issue for years before noticing something was awry. The attack was reportedly spread via the use of USB and is still considered one of the most advanced cyber weapons to date (Bambauer, 2014; Hellmann, 2015). STUXNET has become known in the security industry as the beginning of actual cyber warfare (Bambauer, 2014; Hellmann, 2015; Karnouskos, 2011).

Shamoon malware was used to launch an attack on Saudi Aramco on August 15, 2012: the attack took out 30,000 computers by deleting the master boot record (Dehlawi & Abokhodair, 2013). This attack was unique in that it did not target the process control network or steal information; the focus of this attack was destruction. Fortunately, Saudi Aramco avoided

further destruction by having appropriate controls around their process control environment and, eventually, was able to contain the outbreak. The attacks above are different from generic user attacks in that they were designed to target systems that were previously thought to be safe from the outside world due to their disconnected nature, legacy programming methodology, and the requirement for specialized knowledge of the environment.

Maroochy, a highly publicized attack, was launched by a disgruntled employee, Vitek Boden, that ultimately dumped over 800K liters of raw sewage across 142 pumping stations over an employment dispute in Maroochy Shire, Australia (Brenner, 2013; Tzokatziou et al., 2015). Execution of the attack occurred when the employee used equipment from his employer and used radio commands to open valves that controlled the local sewers. This attack is particularly interesting because it reflects the nature of using remote systems to launch attacks not from some unknown nation-state, but from inside a company by someone with extensive knowledge of a system. Could someone be paid enough to launch a similar attack from the inside? According to Verizon (2016), a similar attack happened in 2016 when hackers used a compromised AS400 system to gain access to ICS controllers in KWC's (a fictitious name) system to release dangerous chemicals into the local water supply. Security holes or insufficient patch management practices take the blame when attacks happen remotely.

HAVEX was another type of attack that targeted SCADA vendors directly. HAVEX has been described as a " general purpose remote access trojan" that is used to infect downloadable software (Maitra, 2015, p. 174). This attack is impressive because it illustrates that any change can introduce another variable in what is otherwise known as a stable environment. Additionally, traditional IT groups tout patching as the key to all security vulnerabilities; this attack added a

new element of downloading an already compromised code that allowed remote execution of commands on systems previously considered to be secure.

A Different Approach

Despite STUXNET receiving the credibility as the first cyber weapon, in 1982, an attack on the Trans-Siberian Pipeline is a more chilling tale of the dangers involved. Thomas Reed, a member of President Ronald Regan's National Security Council, noted that in 1982 the Soviet Union was in search of software to run a pipeline that stretched from Siberia to Eastern Europe. As the U.S. learned of this need for software, they begin working with a Canadian software company that eventually supplied the "enhanced" pipeline software to the Soviet Union that allowed the U.S. to manipulate pump settings and many other parameters (as cited Berghel, 2015, p. 65). This attack disrupted pipeline operations and is believed to have caused one of the biggest non-nuclear explosions ever recorded. The Trans-Siberian Pipeline incident is proof that air gaps only work if environments remain static. Introduction of external components could render the air gap insufficient. Berghel (2015) asserted that the air gaps are misguided approaches that hackers have readily exploited at will for the last 30 years.

Attacks in ICS environments have ranged from completely wiping the hard drives of 30,000 computers at a Saudi Arabian Oil Company to completely shutting down nation state programs such as what happened in Iran and Tibet (Bambauer, 2014; Dehlawi & Abokhodair, 2013). Schiavone, Garg, and Summers (2014) argued that despite advances in detection, technology, and adoption of security frameworks, companies are ill-prepared to deal with cyber-attacks. Organizational changes and rapid fluctuation in business markets ensure dynamic changes play a part in the picture. Schiavone et al. (2014) echoed similar concerns raised by the

seminal work of Hong et al. (2003) when noting the lack of a holistic approach to enterprise security.

Piggin (2014) asserted that despite awareness and diligence in applying safeguards, people are still the weakest link. Piggin went on to note that attacks on personnel can happen outside of the workspace. Personnel must be trained to detect these types of attempts by malicious hackers and know what to do when approached. In the case of STUXNET, it is still unclear how the first virus made it to the initial target. According to Ashenden (2016), the code jumped from the laptop of a maintenance worker to the ICS system. In addition to no longer using air gaps, organizations must now focus on adequately educating users on risky behaviors that increase chances for attack. Piggin went on to suggest that compromising humans is as trivial as compromising system resources.

Ashenden (2016) offered that companies with safety-oriented cultures, as many ICS environments have, try to approach implementing a cybersecurity culture in the same way. The safety culture approach is flawed because a safety culture works toward protecting the end-user; a cybersecurity culture protects an asset that is not as tangible to the end-user. Ashenden (2016) posited that the first step in changing behavior is identifying the undesirable behavior. As an example, the author uses phishing attacks as an example. The common practice of instructing users to not click on suspicious links is easy enough, but the users must have received training to know how to identify suspicious links and suspicious emails. One popular approach is the periodic generation of controlled “suspicious” emails to increase user awareness (Ashenden, 2016). For reference, 26% of incidents reported by ICS-CERT (2016) were email related. In the case of ICS environments, security engineers must be trained in the business use of an ICS

environment and be able to identify exploits possible on vulnerable low-powered devices. Without this knowledge, stopping or mitigating a potential attack becomes next to impossible.

The protocols used in ICS environments and the non-encrypted nature of software make the environment readily susceptible to manipulation. Ashenden (2016) offered that the use of an air gap only forces users to circumvent implemented security measures. As noted in the literature, at some point the air-gapped network is eventually connected to the production environment (Ashenden, 2016; Bambauer, 2014; Hellmann, 2015). Acceptable approaches for consideration, such as those highlighted by ISA99 (2017), will allow limited connectivity to the production network in a controlled manner. This methodology will prevent engineers from circumventing air gap controls and provide a way for engineers to do their jobs efficiently, securely, and without violating security policy. This approach also allows security professionals to focus on internal threats. The notion of an air gap is an approach that is genuinely rooted in attack prevention; this approach does not consider mitigation or the needs of the business. In addition to mitigation, companies should be aware of any potential weaknesses.

Companies must take the time to self-assess their security posture. An internal cybersecurity team could perform the assessment, or have external companies submit bids for an assessment contract; several companies specialize in a variety of penetration (pen) testing and security assessment services (Cherdantseva et al., 2016). The findings from the pen test can be used to firm up any existing gaps in an organization security infrastructure. Piggin (2014) offered a basic ICS checklist for ICS operators that are responsible for the security of the ICS system that includes (a) undertaking open-source searches to identify plant information and remediate/remove accordingly, (b) restricting physical access to the ICS network, and (c) protecting system components from exploitation by applying security patches, disabling unused

ports and services, restricting ICS user privileges, tracking and monitoring audit trails, using antivirus software, and (D) using file integrity software to detect changes in files or when malware is suspected.

Findings

The review of this literature has revealed findings that make it possible to derive where disconnects exist between the constructs of security efficacy, agility, and strategic alignment in ICS environments. Despite numerous efforts to combine legislation that mandates protection of critical infrastructure, the tie-in to business value has purely been from the standpoint of public safety and to a lesser extent the protection of shareholders. Additionally, 87% of ICSs belong to private companies in competitive markets (Stouffer et al., 2015). Few articles have tied security efficacy to the enablement of strategic objectives necessary for private companies to generate additional value. Without this tie-in, information security efforts will solely focus on prevention and mitigation (Tu et al., 2018).

The constant focus on prevention and mitigation is futile (Bambauer, 2014). Industry leaders must shift from a dedicated focus on prevention and mitigation to focusing on strategic enablement in addition to prevention and mitigation as primary components of an information security program. Additionally, the inability of legislation to decrease the number of breaches despite providing a framework coupled with incentives for adoption that do not enhance business value continues to provide barriers to the implementation of voluntary frameworks (Hellman, 2015).

Theoretical Conflicts

The theory of strategic alignment, agility, and integrated security are goals of organizations that wish to compete in global markets (Henderson & Venkatraman, 1993; Hong et

al., 2003; Sambamurthy et al., 2003). Despite agility and strategic alignment being tightly integrated, the concept of security in these dynamic environments requires a concept of measured risk. The longer it takes to assess the risk, the higher the potential to miss market opportunities. Delay puts the concept of security at odds with agility to capitalize on market opportunities. Additionally, businesses can choose to make moves that put the company at risk; without alignment with security strategy, these moves, despite their good intentions, can have lasting consequences (Istikoma et al., 2015; Tu et al., 2018).

In industrial environments, the need to ensure operational and business units are aligned, capitalize on market opportunities, and conduct transactions securely are operational goals that require integration at a much higher level. Cherdantseva et al. (2016) noted the differing perspectives of traditional IT personnel and their operational business counterparts in industrial environments further complicate security of infrastructure that is responsible for the standard of living enjoyed by millions. The theories and assumptions of agility and strategic alignment operate outside of the context of security; the mitigation of concerns becomes difficult without calling attention to a hostile operating environment that did not exist during the creation of these theories.

Primary Conclusions

The findings in the reviewed literature point out that strategic IT/Business alignment is imperative and this alignment governs the use of IT in organizations (Yaokumah & Brown, 2014; Yayla & Hu, 2012). ICS environments have accepted the fact that the systems used to support users and industrial processes are under different governing bodies and often have differing business objectives, but corporate and industrial systems must connect to one another for productivity (Hellman, 2015; Kuusk et al., 2013). Attacks on critical infrastructure segments

are on the rise. Bambauer (2014) noted that attacks are inevitable. Despite the focus on prevention, reports from ICS-CERT (2016) confirmed that the frequency of successful attacks on critical infrastructure has increased. Despite the findings from ICS-CERT, the expansion of ICSs outside of controlled environments continues.

This research has also shown that an organization's ability to quickly utilize IT to sense and respond to competitive actions initiated by competitors is equally relevant in a world where imitation is standard, and customers have unlimited choices (Chakravarty et al., 2013; Martin, 2012; Roberts & Grover, 2012; Zhenhua et al., 2017). Additionally, in specific environments, security, part of an IT governance strategy, can limit the ability of the business to move in an expedited fashion to capitalize on market opportunities (Istikoma et al., 2015; Wu et al., 2015; Yaokumah & Brown, 2014). IT can act as an enabler, but when IT principles interfere with operational aspects, security issues arise (Istikoma et al., 2015; Knijff, 2014).

Critique of Previous Research Methods

The presented studies are not free from errors that may leave readers with additional questions. A common theme is limited applicability of the research findings based on restrictions in geographic distributions (Bahl & Wali, 2014; Garg & Goyal, 2012; Hajikhani & Azadi, 2013; Kumar, Kaur, & GNDU, 2015; Perepletchikov, Ryan, & Tari, 2013; Pretorius & Niekerk, 2015; Vlachos, Minou, Assimakopouos, & Toska, 2011; Yaokumah & Brown, 2014; Yayla & Hu, 2012). The regional relevance means that findings in one study may not be globally applicable, thus failing external validity (Trochim, 2006). Further, some studies omitted data noting whether the assumptions of linearity, normality, homoscedasticity, or multicollinearity were met, bringing into question conclusion validity (Chen, Ramamurthy, & Wen, 2015; Roberts & Grover, 2012; Yayla & Hu, 2012). The omission of the noted items seems to be typical for studies of this type.

Summary

This literature review has discussed a variety of issues about security, agility, and strategic alignment. In ICS environments, these dimensions must now operate together to ensure the business maintains a competitive advantage in addition to protecting the public at large. This chapter discussed different types of ICSs and associated security concerns. Examples of attacks in addition to suggested methods of protecting ICSs provided additional guidance on mitigation of risks. Coverage of gaps in the literature and ethical concerns highlighted traditional thought patterns and concerns that professionals should take into consideration when securing production environments. This chapter provided contributions associated with a study that connects these constructs in ICS environments.

CHAPTER 3. METHODOLOGY

This chapter presents the research methodology used in this study. This study's focus on *what* and the measurable context of *extent* are markers for a quantitative approach. The use of observation and measurement aligns with the post-positivist view and is the philosophy employed in this study. The research goals require the use of closed-ended questions, the collection of data through surveys, and consideration for the hypotheses this study seeks to answer, resulting in a quantitative approach, an approach that will produce the required knowledge.

The remainder of this chapter will outline the focus of this study. The purpose of the study, along with research questions and hypotheses, are provided. The methodology used to frame this study along with the research design will follow. This paper will provide a review of the target population and sample selection process in addition to participant selection and protection methods employed in this study. This section will close with a discussion on the procedures for reviewing reliability and validity of the new instrument along with ethical considerations.

Purpose of the Study

The measurement of the influence of security and agility on strategic alignment in U.S. based ICS environments is the focus of this quantitative study. Bhattacherjee (2012) declared that non-experimental research is a term that is often used to describe research where treatments are not employed such as correlational studies, survey research, and observational research. This study will use a quantitative non-experimental correlational design. This design is appropriate when exploring the relationship between variables without specifying a direction.

Post-positivism centers on the fact that there is a reality outside of what is observed (Creswell, 2013; Trochim, 2006) The philosophical assumptions of this research align with post-positivism (Creswell, 2013). The epistemological assumption is that there is value in the objective and quantifiable knowledge gained by understanding the relationship between the constructs presented in this study and that knowledge is useful. The axiological assumption is that the measurement of agility and security efficacy will objectively inform the strategic alignment model and prove valuable. The ontological assumption is that the constructs of security, agility, and strategic alignment are measurable and the one defined reality is visible to those who observe it. These assumptions lead to a quantitative methodological design, a design that uses objective measurement and analysis, which produces the required knowledge.

Research Questions and Hypotheses

1. What is the extent of the joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments?

   $H_0$1. There is no statistically significant joint relationship between security efficacy, agility, and strategic alignment.

   H_a1. There is a statistically significant joint relationship between security efficacy, agility, and strategic alignment

Sub Questions

Two additional sub-questions will specifically address the relationship between the independent and dependent variables.

2. What is the extent of the relationship between agility and strategic alignment in companies that have industrial control environments?

$H_0$2. There is no statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

H_a2. There is a statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

3. What is the extent of the relationship between security efficacy and strategic alignment in companies that have industrial control environments?

$H_0$3. There is no statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

H_a3. There is a statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

Research Design

This non-experimental correlational design will utilize a quantitative approach that follows post-positivist assumptions (Creswell, 2013; Sekaran & Bougie, 2013). This study used surveys as the primary data collection method. Sekaran and Bougie (2013) posited that survey research, used in descriptive, exploratory, and causal research studies, is prevalent in business inquiries due to the flexibility provided by collecting different types of information. Additionally, Barlett, Kotrlik, and Higgins (2001) offered that survey research is used to gather data that represents or generalizes a population. Several studies using surveys have been conducted on some of the constructs used in this study (Cao et al., 2012; Hajikhani & Azadi, 2013; Pn, 2014; Roberts & Grover, 2012).

This study used surveys to gather data from participants. For this study, participants charged with securing ICS environment provided their views on the constructs of security efficacy, agility, and strategic alignment. Similar correlational studies have used surveys as the

data collection tool (Gerow et al., 2014; Hajikhani & Azadi, 2013). This study utilized industry-specific groups found on Cint for participant solicitation. Cint was used to distribute a link to the survey hosted on SurveyMonkey's servers.

Additionally, three hypotheses evaluate the relationship between variables. Factors in this study highlight a new time-sensitive and insecure landscape that surfaced after the creation of the SAM. This exploratory correlational model will use multiple regression for analysis. The use of is multiple regression is appropriate when several predictor variables are thought to have an impact on the outcome/criterion variable (Bhattacherjee, 2012; Field, 2013; Hoyt, Imel, & Chan, 2008). Awareness of these factors allows for better decision-making in maintaining strategic alignment in ICS environments.

Target Population and Sample

Populations serve a vital role in research. The population is "the group you wish to generalize…" (Trochim, 2006). After identifying the population, sampling is a way to generalize results from that population. Sampling is a method that enhances the quality of inferences about a population (Onwuegbuzie & Collins, 2007). Samples are critical to survey research due to their ability to represent a population; thus, when the sample is representative of the population, the results are generalizable to a broader audience (Mathy, Kerr, & Haydin, 2003; Trochim, 2006).

Population

NIST SP 800-82 recommends that at a minimum, a cross-functional information security team "…should consist of a member of the organization's IT staff, a control engineer, a control system operator, security subject matter experts, and a member of the enterprise risk management staff" (Stouffer et al., 2015, p. 4). The population for this study included industrial and control engineers, technicians, and industrial control operators charged with securing ICS

environments. According to the Bureau of Labor Statistics (2016), this population accounts for a little under 500K positions across multiple industries. Kuusk et al. (2013) offered that companies that use industrial systems often utilize engineers to manage ICSs. The use of engineers to manage these systems is notable in that typical IT classifications may not apply in these environments.

Sample

Strategy. This study utilized a probability-based sampling strategy. Random sampling was used to select the participants in this study. Random sampling is a method that "occurs when each sampling unit in a defined population has an equal chance of being selected" (Teddlie & Yu, 2007, p. 79) This study exercised a single-stage sampling strategy. Random sampling, a well-known method, allows for generalization to a larger population (Creswell, 2013; Teddlie & Yu, 2007; Trochim, 2006).

Frame. Trochim (2006) offered that the sample frame is the accessible part of a population that a researcher can use for a study. The sample frame for this study came from Cint's database of participants in various industrial sectors. Cint's database included 563 participants that work in ICS environments such as manufacturing, energy, and municipalities across the United States.

Size. The sample size is an essential consideration in quantitative studies (Barlett et al., 2001; Trochim, 2006). Sample size determines the number of responses needed to represent the desired population at a given power. According to Cohen (1992a), knowledge of the sample size allows adjustment "… to attain the desired power for the specified significance and hypothesized ES" (p. 156). Estimation of the sample size becomes possible when the following values are

known: (a) alpha/significance, (b) power, and (c) effect size (Cohen, 1992a, 1992b; Trochim, 2006).

Inclusion and Exclusion Criteria. Hoertel, Chevance, and Limosin (2017) offered that inclusion and exclusion criteria are characteristics that participants must own for inclusion or exclusion from a study. An active role in securing ICS environments was the primary inclusion criteria for this study. Screening questions aided in filtering participants based on age and length of relevant experience in securing ICS environments. Exclusion criteria for this study included participants less than 18 years of age or participants with less than two years of experience securing ICS systems.

Power Analysis

Current research suggests that acceptable values for significance and power are 0.05 and 0.8 respectively (Cohen, 1992b; Trochim, 2006). The proposed model for this study evaluates the impact of predictors, security efficacy and agility, on the outcome variable of strategic alignment. A priori power analysis of sample size was conducted using information based on selected values for a power of .95, an effect size of .15, and an alpha value of 0.05. The application G*Power3 was used to model the numbers and provided a minimum sample size of 97 (Faul, Erdfelder, Buchner, & Lang, 2009).

Procedures

Participant Selection

One of the primary challenges associated with random sampling is the ability of the sample to be purely random. According to the Bureau of Labor Statistics (2016), the market reported the following positions and growth statistics (a) Water and Waste Water Operators 114K positions with 6% growth (b) Power Plant Operators, Distributors, and Dispatchers 60K

and 6% decline (c) Industrial Engineers 241K with no growth (d) Industrial Engineering Technicians 66.5K. In this case, a truly random sample becomes cost-prohibitive, so the populations were flagged using Cint's pool of candidates. Further complicating data collection is the fact the control/process engineers and their IT counterparts have different titles due to IT and OT having different organizational objectives even within the same company (Kuusk et al., 2013). The selection of a broader population, via Cint's collection tool, to include enterprise risk management staff and IT (Stouffer et al., 2015), as a part of a cross-functional team, ensured inclusion of qualified participants.

Protection of Participants

Creswell (2013) offered that the disclosure of sensitive information may harm participants. To ensure participant protection, respondents entered data anonymously over an encrypted tunnel between the participant's host machine and SurveyMonkey's servers. Respondents that did not meet qualification criteria were thanked for their time and redirected out of the survey. All respondents provided consent regarding disclosure of survey results. For the security of participants, all collected data is stored on encrypted media under the control of this researcher for at least seven years. This survey did not collect organization data. This measure offers an additional layer of protection for participants and the companies that employ them. For example, contrary responses that impact shareholder confidence, are not able to be traced back to an organization. Additionally, this also prevents the findings in the survey from being used to launch attacks against organizations.

Data Collection

The process of collecting data for this research used an online survey hosted by SurveyMonkey. The initial phase of data collection began with creating the pilot and actual

surveys on SurveyMonkey's servers. Cint was used to solicit participants who matched the target audience of ICS security professionals. Publishing of the final survey link to respondents in Cint's pool of ICS experts occurred after modifications were made based on field and pilot studies.

Participation in the survey automatically directed respondents to a link that included a description of the study, terms, detailed instructions, statement of informed consent, confidentiality agreement, and a description of any associated risks. For this study, 97 responses provided the needed power. A target number of 185 responses, twice the number needed, was considered for this survey to account for incomplete responses. Once the target number of completed surveys had been reached, by exiting the survey at completion, Cint closed the survey and data collection ceased.

Several screening questions served to ensure participants had the requisite experience and did not belong to a protected group. Primary demographic data such as gender, length of experience with ICS, age group, company size, and industry served to help identify patterns amongst respondents. Three instruments were used to collect and measure data on the constructs of security efficacy, agility, and strategic alignment. Once the collection deadline passed, an export of the data into IBM's SPSS Version 24 followed. Collected responses were subjected to appropriate statistical procedures for testing relationships amongst variables, in this case, correlation and multiple regression. The survey took an average of 3 minutes to complete.

Data Analysis

Before analysis, screening of the data was necessary before making any statistical assumptions. Mertler and Vannatta (2013) outlined four reasons for screening data. The first reason identified data accuracy as a goal. This principle highlights the nature of statistical

programs to provide data based on submitted data, without regard for the accuracy of the data. The next purpose is to assess the impact and ways to deal with missing or incomplete data. Participants in survey research may tire of the survey or unintentionally incorrectly code a response resulting in incomplete data (Meade & Craig, 2012). The impact of extreme outliers can create problems such as skewing the results of otherwise valid responses (Tabachnick & Fidell, 2007). Bagozzi and Yi (2012) echoed the concern for outliers and noted that sound established practices must guide the exclusion of outliers. The last reason, the one most recognizable in research, is to meet the assumptions of normality, linearity, and homoscedasticity.

Given the non-experimental nature of this study, there is a long-standing debate regarding the validity of parametric testing on ranked data. With Likert data, rank ordering prioritizes responses, but the distance between groups is not consistent. For example, it is not easy to quantify whether the distance between "disagree" and "somewhat disagree" is the same as the distance between "neutral" and "agree." Menard (2010) noted that ordinal data, due to its non-scalar manner, are difficult to analyze. Leung (2011) posited that "the summed scale score may still be of the interval type, for the sum may be insensitive to the violation of interval assumption at item level" (Leung, 2011, p. 413). Leung noted this approach assumes the instrument has been previously validated using a reliability measure such as Cronbach's Alpha. This study used summed scaled scores to conduct testing. Additionally, Carifio and Perla (2007) noted that Likert data, if using a 5 to 7 point scale, will hold for using parametric analyses. Norman (2010) highlighted that over 80 years of empirical data support the ability of parametric statistics to be robust against common violations with ordinal data.

This study called for a new instrument that uses established measures for the constructs of security efficacy, agility, and strategic alignment. A Bivariate Correlation was performed

using Pearson's Correlation coefficient to see to what extent the degree of the relationship is between the independent and dependent variables. Multiple regression, using hierarchical selection, was used to determine to what extent the independent variables can be used to predict the dependent variable and secondarily, to explain causation. Multiple regression, using hierarchical selection, was utilized based on its ability to allow the researcher to determine the order in which predictor values were added to the regression equation (Hoyt et al., 2008).

Instruments

When conducting research that measures values, reliability and validity of the instrument are two fundamental values to review when finding an instrument fit for use in research (Tavakol & Dennick, 2011). Reliability is the ability of a measurement method to produce the same result consistently. Bhattacherjee (2012) offered an example that compares the consistency of guessing one's weight versus using a scale to produce the same result. The scale is going to produce a more accurate consistent result.

Validity

Foddy (1998) noted that due to "…comprehension difficulties, inadequate response options, and inadequate specification of response frameworks…" some survey respondents will answer a question without full comprehension of the question. Poorly worded questions contribute to the incidence of outliers and have the potential to skew results. One way to add clarity to questions and measurement relevance is to conduct field testing with a panel of experts (Gehlbach & Brinkworth, 2011). The new instrument was field tested, to enhance validity, by seven industry experts that possessed 10+ years of experience securing ICSs used in energy, water treatment, and manufacturing environments. The field test panel provided feedback on the properties of face validity, readability, wording, ability to stress participants, and appropriateness

for job type for this instrument. For example, one panelist noted an issue with the progression of the Likert-scale. Another panelist suggested clarifying questions seven and eleven. After making the requested updates, the survey was sent out for pilot testing.

Pilot testing, a critical part of the research process, provides a method for testing the survey instrument against a smaller population within the sample frame to detect scale functionality, estimate response rate, and identify design issues (Bhattacherjee, 2012; Gehlbach & Brinkworth, 2011; Johanson & Brooks, 2010). Pilot participants were selected using the same process as participants from the main group. Cint provided the audience pool and sent participants a link to the pilot survey hosted on SurveyMonkey's servers. The pilot test ran for one week where 15 participants, who would have fit the profile on the main study, were given the opportunity to pilot the instrument. Respondents were asked to provide additional feedback in free text form at the end of each section. Analysis of comments did not lead to further enhancement of this instrument. For this study, completed surveys returned Cronbach's α of .96 for ITBS and .97. The measures of agility and security efficacy produced observed Cronbach's α of .90 and .93 respectively and remain unchanged (see Table 1).

Table 1. *Reliability Statistics*

Variable	Cronbach Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
ITBS	.963	.968	5
BSIT	.971	.976	5
AG	.905	.911	5
SE	.934	.940	6

Reliability

There are many types of reliability measures, but the most frequently used is for the internal consistency of a group of items to measure the same concept developed by Doctor Lee Cronbach (Trochim, 2006). Dr. Lee Cronbach developed Alpha to represent the internal consistency of a scale (Cronbach, 1951). The test results range from 0 to 1 with 0 showing no relationship between items and the closer to 1 a measure is, the likelihood of measuring the same concept increases (Tavakol & Dennick, 2011). Additionally, when the reliability coefficient is squared, the error can be attained by subtracting the squared number from 1. Typically, acceptable values for Cronbach's α are 0.70 and above (Cortina, 1993; Nunnally, 1975).

Huang (2012) created an instrument to measure strategic alignment, IT management sophistication, and perceived IT importance. From this study, this researcher only included the questions for the measurement of strategic alignment. Strategic alignment is measured using five questions to address IT/Business alignment (ITBS) while five questions are used to measure Business/IT alignment (BSIT). The survey utilized a seven-point Likert scale (1 – strongly disagree to 7 – strongly agree). The original study noted Cronbach's α numbers of .84 for ITBS and .92 for BSIT.

Patrakosol and Lee (2009) created a survey instrument to measure the constructs of IT agility and performance. From this study, this researcher only included the questions for the measurement of agility. The survey utilized a seven-point Likert scale (1 – strongly disagree to 7 – strongly agree). The original study noted a Cronbach's α of .90 for IT agility.

Kankanhalli et al. (2003) developed a survey instrument to measure the efficacy of information security efforts. The constructs of top management support and IS security effectiveness were measured. From this study, this researcher only included the questions for the

measurement of IS security effectiveness. The survey utilized a seven-point Likert scale (1 – strongly disagree to 7 – strongly agree). Normalization of the questions occurred to enhance clarity for information security professionals across a broad range of industries. The original study noted a Cronbach's α of .93 for security efficacy.

Ethical Considerations

The pressure put on security professionals to keep pace with the business when dealing with critical infrastructure presents some fundamental ethical concerns. Primarily, given that the security industry has well documented the risk of attacks in these environments as well as our inability to prevent stated attacks is the continued deployment of these systems despite security concerns ethical? Bambauer (2014) highlighted the potential for loss of life and environmental harm and provided examples of the results when ethical concerns are not known or overlooked. Second, the very classification of these systems as critical infrastructure places them in a unique category apart from business IT systems via PPD 21.

The need for security to set the stage for business transactions is now a requirement with the recent push for connected services in these environments. Additionally, according to Cherdantseva et al. (2016), the confidentiality, integrity, availability triad governs IT systems on corporate networks; in ICS environments safety, reliability, and resiliency aspects come before confidentiality. Unfortunately, the lack of confidentiality in these systems makes them vulnerable to attack. By making security the base foundation upon which business/IT relationships exist, protection of assets becomes inherent.

The topic of security efficacy in process control environments is currently front of mind for companies that use these systems. Recent attacks have nations and organizations alike on high alert (Kaiser, 2015). Given the sensitivity of the potential results, care must be taken to

protect the identity respondents and the companies that employ them. Griffiths (1995) provided a variety of examples of ethics violations in his work regarding responsible research. The validity of gathered data must be maintained to avoid tainting the results of future research efforts (Mathy et al., 2003). Before publishing, consideration of the potential impact on the companies that survey respondents work for is necessary. The protection of participant identity and any associated organizational data are primary concerns for ethical research.

The small size of the ICS sector makes it easy to determine potential contributors just by revealing organizational data. As an additional layer of protection for participants, SurveyMonkey allows anonymous data entry where email and IP address collection are disabled. Additionally, Cint provides an option to disable the collection IP address and email information of respondents in their participant pools. Although it is impossible to secure all data transmitted over the Internet, connections to SurveyMonkey utilize 256-bit encryption ciphers. With this level of encryption, eavesdropping becomes more difficult, elevating the level of security while taking part in the survey. This survey did not collect organizational data to protect the identity of corporations. For example, negative responses linked to identifiable organizations, have the potential to impact shareholder confidence in addition to making a company a potential target of future attacks due to identified weaknesses in the survey. The measures discussed aided in avoiding adverse effects on survey respondents or the companies for which they worked.

Summary

This chapter provided a review of the methodology and constructs used to shape this study. This chapter expanded on the purpose of the study along with providing research questions and hypotheses that were used to guide this study. The methodology of the study was defined followed by a discussion regarding the research design. This chapter also provided a

review of the target population and sample along with measures taken to ensure reliability and validity of the newly created instruments. This chapter closed with ethical considerations. Respondent demographics and a detailed analysis of the data collected will follow in Chapter 4. Chapter 5 provides conclusions on collected data and recommendations for future analysis.

CHAPTER 4. RESULTS

This chapter presents the data analyzed for the relationships described in Chapter 3. This chapter provides data on the relationship between the variables security efficacy (SE), agility (ITA), and strategic alignment (STA) in this correlational non-experimental study. This chapter starts with a review of the background of the study. A description of the sample provides insight into the demographics of the participants in this study. Demographic data precedes a discussion regarding the statistical test used to test the stated hypotheses. This chapter concludes with a summary of the provided information.

Background

This quantitative non-exploratory study evaluated two predictor variables, security efficacy and agility, and one outcome variable, strategic alignment. Prior chapters reviewed vital components of this research such as the problem this research seeks to solve, existing literature on the constructs security efficacy, agility, and strategic alignment, and relevant data regarding the methodology. This chapter will expand on the methodology provided in the previous chapter with statistical analysis. Analysis of the data was conducted using IBM's SPSS Statistics Version 24.

Description of the Sample

The target population for this study included security professionals charged with securing U.S. based ICS environments. The inclusion of multiple industries helps to gain a better picture of security practices outside of specific industries, thus allowing the results to be more generalizable across the ICS community. Inclusion criteria for this study required participants to be 18 years of age or older and have at least two years of experience securing ICS environments.

Tables 2, 3, and 4 display the frequency tables for years of experience, gender, and age group of respondents. Of the participants that completed the study, 31% had more than 5 years of experience with 41% having 3 years or less. The highest percentage of respondents had less than 4 years of experience securing industrial control/SCADA environments; this is not surprising as about three-fourths of those responding were under 40 years of age. Many of the participants, 51%, were in the 30 – 39 age range with the 60 or older group rounding out the bottom of the frequency table at 5%. Most respondents were male (79.4%).

Table 2. *Years of Experience Securing Industrial Control/SCADA Environments*

	Frequency	Percent	Cumulative Percent
2 – 3 yrs.	44	41.1	41.1
4 – 5 yrs.	30	28.0	69.2
>5 yrs.	33	30.8	100.0
Total	107	100.0	

Table 3. *Gender of Respondent*

	Frequency	Percent	Cumulative Percent
Male	85	79.4	79.4
Female	22	20.6	100.0
Total	107	100.0	

Table 4. *Age Group of Respondent*

	Frequency	Percent	Cumulative Percent
18 - 29	27	25.2	25.2
30 -39	54	50.5	75.7
40 -49	12	11.2	86.9
50 -59	9	8.4	95.3
60 or older	5	4.7	100.0
Total	107	100.0	

Table 5 demonstrates that small or moderately-sized companies employ a significant percentage of respondents. Six of ten respondents work for companies with less than 1,000 employees. The respondents' industry included cities (19.6%), energy companies (16.8%), manufacturing (37.4%), or some other organization/company (26.2%) (see Table 5).

Table 5. *Number of Employees in Company*

	Frequency	Percent	Cumulative Percent
< 500	26	24.3	24.3
501 - 1000	37	34.6	58.9
1001 - 5000	32	29.9	88.8
5000 - 10000	5	4.7	93.5
>10000	7	6.5	100.0
Total	107	100.0	

Table 6. *Respondent's Industry*

	Frequency	Percent	Cumulative Percent
City or Municipality	21	19.6	19.6
Energy	18	16.8	36.4
Manufacturing	40	37.4	73.8
Other	28	26.2	100.0
Total	107	100.0	

Figure 6 displays respondent's highest level of education. Nearly four of ten respondents (38.3%) earned a bachelor's degree as his or her highest degree. Only 10.3% of respondents attained a high-school diploma or equivalent.

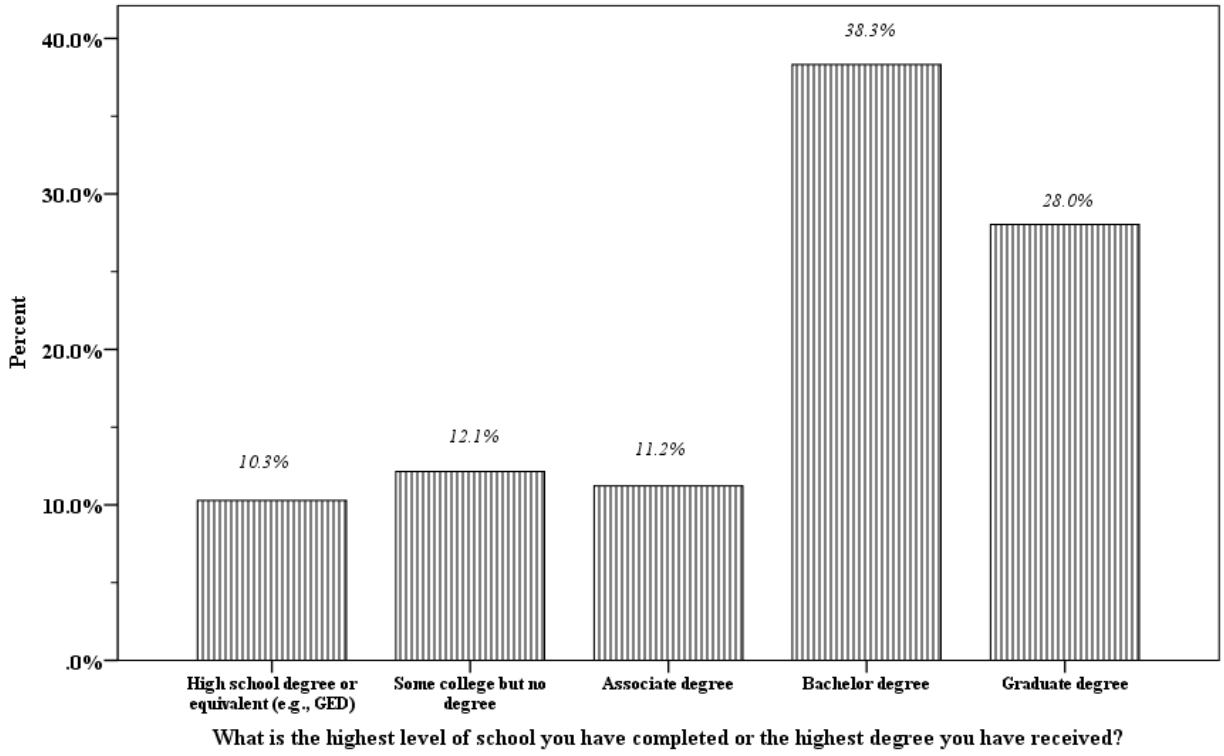

Figure 6. *Highest level of education*

Assumptions

Before conducting tests on multivariate data, verifying the assumptions of normality, linearity, and homoscedasticity is a required step to ensure results provide the quality necessary to fit a linear model (Field, 2013; Laerd, 2013; Tabachnick & Fidell, 2007). Despite this, the violation of normality has been shown to be a non-factor in the ability of regression to perform estimation (Berry & Feldman, 1985). Further, for this study, bootstrapping is used to account for non-normality and outliers in the regression model. As outlined in Field (2013), bootstrapping makes all the standard assumptions of OLS regression including normality and homoscedasticity of the errors in estimation. Bootstrapping corrects these violations of the standard regression

model and produces more accurate conclusions (Field, 2013). The assumption of multicollinearity no longer stands when the tolerance is less than .20 or when VIF is greater than 5 (Garson, 2012) or more than 10 (Field, 2013). Table 8 displays the VIF values for the predictor variables. In this model, there is no multicollinearity; therefore, the assumption of multicollinearity holds.

Table 7. *Test of Normality*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Agility	0.201	107	0.000	0.866	107	0.000
Security Efficacy	0.181	107	0.000	0.848	107	0.000
Strategic Alignment	0.144	107	0.000	0.874	107	0.000

Note. a. Lilliefors Significance Correction

Table 8. *Multicollinearity Statistics*

Model	Collinearity Statistics	
	Tolerance	VIF
Agility	0.608	1.645
Security Efficacy	0.608	1.645

Table 9. *Pearson Correlations: Strategic Alignment by Agility and Security Efficacy*

			STA	AG	SE
Pearson Correlation			1	.545**	.601**
Sig. (2-tailed)				0.000	0.000
N			107	107	107
Bootstrap[c]	Bias		0	0.000	-0.010
	Std. Error		0	0.083	0.090
	BCa 95% Confidence Interval	Lower		0.368	0.394
		Upper		0.694	0.743

Note. **. Correlation is significant at the 0.01 level (2-tailed).

Correlation analysis

Pearson's *r* was used to measure the degree of the linear relationship amongst the variables. Values can range from + 1.00 to -1.00 where a value that equals .00 represents no linear relationship (Tabachnick & Fidell, 2007). The closer the value is to 1 or -1, a stronger relationship exists. Additionally, Field (2013) offered significance values below .05 indicate a statistically significant relationship. In Table 9, all values indicate a strong correlation between strategic alignment, agility, and security efficacy.

Regression Analysis

This study attempted to assess the impact of the predictor variables on the outcome variable. Multiple regression, using hierarchical selection was selected to regress the predictors against the outcome variable based on the absence of literature on the defined relationships. Three research questions were developed to explore the relationships.

Hypothesis Testing

RQ1. What is the extent of the joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments

$H_0$1: There is no statistically significant relationship between security efficacy, agility, and strategic alignment.

H_a1: There is a statistically significant relationship between security efficacy, agility, and strategic alignment.

To determine the appropriate model to use, tests of normality were performed for the total strategic alignment scores (see Table 7). Table 7 cautions against the use of traditional multiple regression with non-normal distributions, $D(107) = .144$, $p=.000$, is significantly non-normal. For the variables in this study, Appendix B contains the histograms and P-P plots used to identify patterns within distributions. Appendix B confirms that the data has a negative skew. Appendix C contains the box plots used to identify outliers within the data. Appendix C indicates outliers exists across all constructs.

Table 10. *Regression Model Summary*

					Change Statistics				
Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	R^2 Change	F Change	df1	df2	Sig. F Change
1	.545[a]	0.297	0.290	3.88225	0.297	44.383	1	105	0.000
2	.639[b]	0.408	0.397	3.57863	0.111	19.573	1	104	0.000

Note. a. Predictors: (Constant), AG, b. Predictors: (Constant), SE, c. Dependent Variable: STA

According to Table 10, the regression analysis shows that agility $F((1, 105) = 44.383, p < .000)$ and security efficacy $F((1, 104) = 19.573, p < .000)$ are significant. The null hypothesis

is rejected, and the alternate is accepted. As you can see in Table 10, regression results indicate an overall model of two predictors (security efficacy and agility) that significantly predicts strategic alignment [$R^2 = .408$, $R^2_{adj} = .397$, $F(2, 104) = 35.903$, $p < .000$]. This model accounted for 40.8% of variance in strategic alignment in U.S. based ICS environments.

Table 11. *Coefficients*

Model		B	SE B	ß	t	Sig.
1	(Constant)	32.884	3.459		9.506	0.000
	Sum of AG	0.854	0.128	0.545	6.662	0.000
2	(Constant)	22.554	3.952		5.706	0.000
	Sum of AG	0.434	0.152	0.277	2.865	0.005
	Sum of SE	0.653	0.148	0.428	4.424	0.000

RQ2. To what extent is the relationship, if any, between agility and strategic alignment in companies that have industrial control environments?

$H_0$2: There is no statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

H_a2: There is a statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

The second research question tests whether there was a statistically significant relationship between agility and strategic alignment in companies that have industrial control environments. Table 9 contains the results of the Pearson correlation between agility and strategic alignment in companies that have industrial control environments. The null hypothesis is rejected and alternate hypothesis accepted indicating that agility is significantly correlated with

strategic alignment, $r = .545$ [.368, .694], $p = .000$. The relationship is considered significant and positive in that as the level of agility increased, levels of strategic alignment increased. The regression analysis in Table 9 Model 1 shows that agility $F((1, 105) = 44.383, p < .000)$ is significant in predicting the outcome variable and has the most significant impact on strategic alignment (ß = .545, $p<.001$) as shown in Table 11. Table 10 reflects that agility accounts for 29.7% of the variance in strategic alignment and is the most significant predictor of strategic alignment.

RQ3. To what extent is the relationship, if any, between security efficacy and strategic alignment in companies that have industrial control environments?

$H_0$3: There is no statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

H_a3: There is a statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

The third research question tests whether there was a statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments. Table 9 contains the result of the Pearson correlation between security efficacy and strategic alignment in companies that have industrial control environments. The null hypothesis is rejected and alternate hypothesis accepted that security efficacy is significantly correlated with strategic alignment, $r = .601$ [.394, .743], $p = .000$. The regression analysis in Table 10 Model 2 shows that security efficacy $F((1, 104) = 19.573, p < .000)$ is significant at predicting strategic alignment but has the least amount of influence on strategic alignment (ß = .428, $p<.001$) as shown in Table 11. Additionally, given that the confidence intervals do not

cross 0, the relationship is positive. The model reflects that security efficacy is responsible for 11.1 % of the variance in strategic alignment.

Summary

The purpose of this quantitative non-exploratory correlational study was to determine the relationship between security efficacy, agility, and strategic alignment in U.S. based ICS environments. Additionally, security efficacy and agility were regressed against strategic alignment to determine their ability to predict strategic alignment. The first research question (H1) attempted to determine the extent to which a joint relationship existed between security efficacy, agility, and strategic alignment. Research question (RQ1) showed that the regression of the predictor variables of security efficacy and agility against strategic alignment, the predictors accounted for 40.8% of the variance in strategic alignment in ICS environments. The analysis results concluded that there is a significant positive relationship at each step of the model between the predictors, security efficacy and agility, and the outcome variable, strategic alignment. That significance means that the model accurately predicts strategic alignment.

The second research question (RQ2) attempted to determine the extent to which a relationship existed between agility and strategic alignment in US-based ICS environments. The analysis results concluded that there is a significant positive relationship between agility and strategic alignment in ICS environments. Additionally, agility can predict strategic alignment and accounts for 29.7% of the variation in the model.

The third research question (RQ3) attempted to determine the extent to which a relationship existed between security efficacy and strategic alignment in US-based ICS environments. The analysis results concluded that there is a significant positive relationship between security efficacy and strategic alignment in ICS environments. The model showed that

security efficacy can predict strategic alignment and accounts for 11.1% of the variation in the model.

This chapter has provided a review of the background of the study. A description of the sample provided insight into the demographics of the ICS community. This chapter also discussed statistical tests used to validate the stated hypothesis. Data were tested using correlation and multiple regression. This chapter also provided a review of the results and research questions along with a summary.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

In this quantitative correlational study, the researcher utilized gaps in the literature to identify a research problem that explores the relationship between security efficacy, agility, and strategic alignment in ICS environments located in the United States. This chapter will provide a summary of the research study that includes a discussion of the results, conclusions, limitations, and recommendations for further research.

Summary of the Results

The primary focus of this study was to gather perceptions on security efficacy, agility, and strategic alignment from security professionals charged with securing ICS environments in the U.S. The positioning of the constructs of security efficacy and agility as predictors for the construct of strategic alignment in ICS environments is vital for this study. This positioning is vital as strategic alignment in ICS environments has a direct impact on the bottom line. As noted in previous sections, there is a great deal of literature on the constructs in this study. Strategic alignment is touted for its ability to ensure IT meets the needs of the business (Gerow et al., 2015; Yaokumah & Brown, 2014). Agility is required to ensure competitive actions initiated by competitors generate products with newer capabilities that enhance market positioning (Chakravarty et al., 2013; Sawas & Watfa, 2015). Security efficacy is required to ensure intellectual property stays within the organization, and to secure business transactions in a digital world (Istikoma et al., 2015; Schiavone et al., 2014).

Before conducting this research, little empirical data existed about the relationship between the need for technology professionals to rapidly deploy ICS systems to maintain alignment and the challenges faced by information security professionals to adequately secure

these deployed environments. To model the relationship, this researcher used the following questions and hypotheses to guide this study.

1. What is the extent of the joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments?

   $H_0$1. There is no statistically significant joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments.

   H_a1. There is a statistically significant joint relationship between security efficacy, agility, and strategic alignment in companies that have industrial control environments.

Sub Questions

Two additional sub-questions specifically addressed the relationship between the independent and dependent variables.

2. To what extent is the relationship, if any, between agility and strategic alignment in companies that have industrial control environments?

   $H_0$2. There is no statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

   H_a2.There is a statistically significant relationship between agility and strategic alignment in companies that have industrial control environments.

3. To what extent is the relationship, if any, between security efficacy and strategic alignment in companies that have industrial control environments?

   $H_0$3. There is no statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

   H_a3.There is a statistically significant relationship between security efficacy and strategic alignment in companies that have industrial control environments.

This research has shown that agility and security efficacy have a positive and predictive relationship with strategic alignment. Responding quickly to competitive actions initiated by competitors does not decrease security efficacy when the business and IT are strategically aligned.

The literature covered in this study spanned the theories of strategic alignment, IT agility, and integrated system theory. These theories are linked as IT agility helps the business utilize IT investments to manage competitive actions initiated by competitors, essentially, the application of IT agility as a differentiator in a flooded market. Security adds a new dynamic to strategic alignment as it secures business transactions in an increasingly insecure, fast-paced digital arena. This theoretical context provided the foundation for this study.

Discussion of the Results

A survey was used to collect the data for this study. The survey instrument was created using approved instruments from pre-existing instruments to cover the constructs of security efficacy (Kankanhalli et al., 2003), agility (Patrakosol & Lee, 2009), and strategic alignment (Huang, 2012). The instrument contained 30 questions (see Appendix A) based on a seven-point Likert scale ranging from (*1 - strongly disagree to 7 - strongly agree)*. The first two questions were qualifiers followed by five questions that provided additional demographic data.

The sample contained energy companies (16.8%), municipalities (19.6%), manufacturing companies (37.4%) and many other (26.2%) industries. Data collected from the respondents were correlated and regressed to determine the strength and direction of the relationship and to assess the predictive capabilities of security efficacy and agility on strategic alignment using a combination of statistical tests. Significant positive correlations were noted between agility and strategic alignment, $r = .545$ [.368, .694], $p = .000$ and security efficacy and strategic alignment,

r = .601 [.394, .743], p = .000. Additionally, it was noted that the predictive capabilities of security efficacy and agility together account for 40%, agility having the most significant impact at 29.7%, of the variation in strategic alignment with security efficacy F ((1, 104) = 19.573, p < .000) and agility F ((1, 105) = 44.383, p < .000) showing significant predictive capabilities.

Conclusions Based on the Results

This study revealed several key findings. The relationship between security efficacy and strategic alignment suggests that as security efficacy increases, strategic alignment increases. The positive relationship between agility and strategic alignment pairs well with the existing literature regarding agility supporting the business during rapid business transactions or when the markets shift, and the resultant increase is in firm performance (Coltman, Tallon, Sharma, & Queiroz, 2015; Gerow et al., 2015). The joint relationship between security efficacy, agility, and strategic alignment now provides insight into how security efficacy can strengthen strategic alignment. These findings provide a basis for security professionals in ICS environments to add enhancing strategic alignment to their focus alongside prevention and risk mitigation.

Limitations

The data in this study only applies to U.S. based ICS environments. ICS environments exist globally, and attacks on ICS environments occur in an incentive-based fashion focusing solely on identified vulnerabilities (Bambauer, 2014). Additionally, the lack of a standard governing body between IT and OT departments, as noted by Kuusk et al. (2013), within an organization limits the applicability of this study to environments structured in this fashion. Another item worth noting is the relatively short amount of time in ICS by over 40% of respondents. Additionally, this study also assumed a degree of strategic alignment existed before this study taking place. The degree of strategic alignment has an impact on agility, thus an

impact on the effectiveness of security controls. Adhering to the recommendations in this research will not shield a company from a determined intruder.

As previously mentioned, the findings in this study can only speak to the observed relationships between the constructs. The data collected only measured relative perceptions of the participants' view of the constructs. Respondent bias in truthfully answering sensitive questions also plays a role in the validity of results. Several other factors play into attacks and the ever-increasing frequency of such events. This study only addresses the influence security efficacy has on strategic alignment and does not mention how to improve security efficacy.

Implications for Practice

The SAM is more than 25 years old. The business landscape and technology that existed during the creation of the SAM has drastically changed due to advancements in technology and increased global competition in ICS environments (Aravind et al., 2013; Oborski, 2014; Zhenhua et al., 2017). Despite the changes in technology, the model is still highly desired in businesses today. Additionally, the use cases for interconnecting ICSs for expansion and enhanced monitoring capabilities continue to enable the completion of strategic objectives for companies that use this technology (Cherdantseva et al., 2016). The practice of connecting ICSs to hostile environments such as the Internet, a practice discouraged by NIST SP 800-82, continues to transform into accepted practice, while cyber threats headline the news with a continuous string of massive data breaches that plague modern communication (Bambauer, 2014; Stouffer et al., 2015). Increased scope and monitoring needs of the environments continue to drive the demand for more connectivity. The strategic alignment model existed before cyber threats routinely made front page news and sponsored cyber warfare became commonplace. Asgarkhani and Sitnikova

(2014) referenced the delicate balance associated with attaching a critical insecure ICS to an environment, the Internet, not designed with security in mind.

With the results of this study, information security professionals can now be aware of the relationship between security efficacy and strategic alignment. For ICS environments, security and data confidentiality are secondary concerns (Cherdantseva et al., 2016). Given security efficacy's ability to enhance strategic alignment, an opportunity exists to derive benefits beyond risk prevention and mitigation. The conversation now is changed from the need for security to solely prevent and mitigate attacks (Bambauer, 2014; Tu et al., 2016), to a more meaningful conversation that enhances an organization's ability to derive value out of existing investments via strategic enablement. Risk prevention and mitigation no longer have to be the only factor of an effective security program; now security can stand alongside agility as a strategic enabler.

Making the connection between security efficacy, agility, and strategic alignment may alleviate some of the pressure experienced when information security needs to quickly respond to business demands (Istikoma et al., 2015). Yaokumah and Brown (2014) offered that more research is needed to show how organizational leaders can improve strategic alignment between the business and information security. The information security community could benefit by no longer being an inhibitor to the business, but an enabler. This research has shown that having agility within IT does not correlate with a decreased level of strategic alignment. The relationship between the constructs suggests that security along with agility can positively influence strategic alignment.

Recommendations for Further Research

Based on the findings future research should address the separation of IT and security management practices as they relate to ICS environments. This research has shown that agility

and security efficacy increase strategic alignment. Given that agility and security efficacy are significant predictors of strategic alignment, a study is needed to address the degree of strategic alignment when no governing body exists across the disciplines of IT and Operations Technology (OT) in ICS environments. Does the lack of a governing body between ICS Security and IT Security increase the attack surface for attackers?

Additionally, 69% of participants in this study had less than four years of experience. Additional research should address expanding the research sample to include more experienced and certified professionals. Research should also be conducted to highlight the impact of the different management practices and the role of leadership between IT and OT, as outlined by Kuusk et al. (2013), on security efficacy in ICS environments. Ashenden (2016) highlighted the importance of people/culture in security practice. An additional area of research should explore the human element to include background, compensation, ICS security certification and training, and recruitment practices and their impact on security efficacy in ICS environments.

Conclusion

Consistent with existing research, agility and strategic alignment are tightly integrated. Researchers have long declared agility is as remarkable as strategic alignment when operating in dynamic environments. Additionally, the observation of the relationship between security efficacy and strategic alignment shows that security efficacy is also a strategic enabler. It is possible to operate highly dynamic, transaction-based business environments in a secure fashion without negatively impacting the business. The continued practice of conducting business over the Internet introduces tremendous business opportunities and exposure to customers across the globe. With the increased exposure comes risks of cybercriminals to disrupt business and cause environmental harm. Given the current trend of ICS environments enabling additional

connectivity, security efficacy not only acts as a prevention and risk mitigation mechanism, but it can also enable continued business growth securely and responsibly.

REFERENCES

Aamir, M., Poncela, J., Uqaili, M., Chowdhry, B., & Khan, N. (2013). Optimal design of remote terminal unit (RTU) for wireless SCADA system for energy management. *Wireless Personal Communications, 69*(3), 999-1012. http://dx.doi.org/10.1007/s11277-013-1060-9

Abbasi, A., & Hashemi, M. (2016). *Ghost in the PLC designing an undetectable programmable logic controller rootkit via pin control attack*. Paper presented at Black Hat Europe 2016, London, UK.

Ahmed, I., Obermeier, S., Naedele, M., & Richard III, G. G. (2012). SCADA systems: Challenges for forensic investigators. *Computer* (12), 44-51. https://dx.doi.org/10.1109/mc.2012.325

Ahmed, I., Obermeier, S., Sudhakaran, S., & Roussev, V. (2017). Programmable logic controller forensics. *IEEE Security & Privacy, 15*(6), 18-24. Retrieved from https://ieeexplore.ieee.org/servlet/opac?punumber=8013

Al Hamadi, H. M. N., Yeun, C. Y., & Zemerly, M. J. (2013). A novel security scheme for the smart grid and SCADA networks. *Wireless Personal Communications, 73*(4), 1547-1559. http://dx.doi.org/10.1007/s11277-013-1265-y

Alcaraz, C., Lopez, J., Zhou, J., & Roman, R. (2011). Secure SCADA framework for the protection of energy control systems. *Concurrency & Computation: Practice & Experience, 23*(12), 1431-1442. http://dx.doi.org/10.1002/cpe.1679

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. http://dx.doi.org/10.1016/j.ijcip.2014.12.002

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal, 26*(3), 236-248. http://dx.doi.org/10.1057/sj.2013.14

Almalawi, A., Yu, X., Tari, Z., Fahad, A., & Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *Computers & Security, 46*(0), 94-110. http://dx.doi.org/10.1016/j.cose.2014.07.005

Alphonsus, E. R., & Abdullah, M. O. (2016). A review on the applications of programmable logic controllers (PLCs). *Renewable and Sustainable Energy Reviews, 60*, 1185-1205. Retrieved from https://www.journals.elsevier.com/renewable-and-sustainable-energy-reviews

Anh, P. D., & Chau, T. D. (2010). Component-based design for SCADA architecture. *International Journal of Control, Automation, and Systems, 8*(5), 1141-1147. http://dx.doi.org/10.1007/s12555-010-0523-y

Antonioli, D., Bernieri, G., & Tippenhauer, N. O. (2018). Taking control: Design and implementation of botnets for cyber-physical attacks with cpsbot. Retrieved from https://arxiv.org/pdf/1802.00152.pdf

Apol, P. S., Hadiwidjojo, D., Djumahir, Rahayu, M., & Sarno, R. (2013). Information technology productivity paradox: A resource-based view and information technology strategic alignment perspective for measuring information technology contribution on performance. *Journal of Theoretical & Applied Information Technology, 53*(3), 541-552. Retrieved from https://www.jatit.org/

Aravind Raj, S., Sudheer, A., Vinodh, S., & Anand, G. (2013). A mathematical model to evaluate the role of agility enablers and criteria in a manufacturing environment. *International Journal of Production Research, 51*(19), 5971-5984. https://dx.doi.org/10.1080/00207543.2013.825381

Asgarkhani, M., & Sitnikova, E. (2014). *A Strategic Approach to Managing Security in SCADA Systems.* Paper presented at the 13th European Conference on Cyber Warfare and Security. Retrieved from https://www.researchgate.net/profile/Andrew_Liaropoulos/publication/264337838_Proceedings_of_the_13th_European_Conference_on_Cyber_Warfare_and_Security/links/53d904af0cf2e38c6331db58.pdf#page=37

Ashenden, D. (2016). The human shield. *The Chemical Engineer, 896,* 22-25. Retrieved from https://www.thechemicalengineer.com/features/the-human-shield/

Bagozzi, R. P., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science, 40*(1), 8-34. http://dx.doi.org/10.1007/s11747-011-0278-x

Bagri, A., Netto, R., & Jhaveri, D. (2014). Supervisory control and data acquisition. *International Journal of Computer Applications, 102*(10). https://dx.doi.org/10.5120/17848-8797

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry. *Information Management & Computer Security, 22*(1), 2-23. http://dx.doi.org/10.1108/IMCS-01-2013-0002

Bambauer, D. E. (2014). Ghost in the network. *University of Pennsylvania Law Review, 162*(5), 1011-1091. Retrieved from https://www.pennlawreview.com/

Barlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal, 19*(1), 43. Retrieved from https://aisnet.org/members/group_content_view.asp?group=89777&id=170352&terms=sigosra/journal.html

Bencsath, B., Pek, G., Buttyan, L., & Felegyhazi, M. (2012). The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet, 4*(4), 971-1003. http://dx.doi.org/10.3390/fi4040971

Berghel, H. (2015). A farewell to air gaps, part 1. *Computer* (6), 64-68. https://dx.doi.org/10.1109/mc.2015.179

Berry, W., & Feldman, S. (1985). *Multiple regression in practice.* Retrieved from http://methods.sagepub.com/book/multiple-regression-in-practice

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. Retrieved from http://scholarcommons.usf.edu/oa_textbooks/3

Boell, S. K., & Cecez-Kecmanovic, D. (2010). Literature reviews and the hermeneutic circle. *Australian Academic & Research Libraries, 41*(2), 129-144. https://doi.org/10.1080/00048623.2010.10721450

Brenner, J. F. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the Atomic Scientists, 69*(5), 15-20. http://dx.doi.org/10.1177/0096340213501372

Byres, E. (2013). The air gap: SCADA's enduring security myth. *Communications of the ACM, 56*(8), 29-31. http://dx.doi.org/10.1145/2492007.2492018

Campos, J. T. G. A. A., Santos, C. C. R., de Souza, C. H. F., & da Silva, R. M. (2013). *Design of reconfigurable manufacturing control applied in a material handling production system using petri nets*. IFAC Proceedings Volumes, 46(24), 499-504. https://dx.doi.org/10.3182/20130911-3-br-3021.00087

Cao, Q., Baker, J., & Hoffman, J. J. (2012). The role of the competitive environment in studies of strategic alignment: A meta-analysis. *International Journal of Production Research, 50*(2), 567-580. https://dx.doi.org/10.1080/00207543.2010.538742

Carifio, J., & Perla, R. J. (2007). Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes. *Journal of Social Sciences, 3*(3), 106-116. https://doi.org/10.3844/jssp.2007.106.116

Chabukswar, R., & Sinopoli, B. (2015). *Secure detection with correlated binary sensors*. Paper presented at the American Control Conference. https://dx.doi.org/10.1109/acc.2015.7171934

Chakravarty, A., Grewal, R., & Sambamurthy, V. (2013). Information technology competencies, organizational agility, and firm performance: Enabling and facilitating roles. *Information Systems Research, 24*(4), 976-997. https://dx.doi.org/10.1287/isre.2013.0500

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems, 55*(3), 11-19. https://doi.org/10.1080/08874417.2015.11645767

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cybersecurity risk assessment methods for SCADA systems. *Computers & Security, 56*, 1-27. https://dx.doi.org/10.1016/j.cose.2015.09.009

Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854-864. https://doi.org/10.1109/jiot.2016.2584538

Cohen, J. (1992a). A power primer. *Psychological Bulletin, 112*(1), 155-159. http://dx.doi.org/10.1037/0033-2909.112.1.155

Cohen, J. (1992b). Statistical power analysis. *Current directions in psychological science, 1*(3), 98-101. https://doi.org/10.1007/0-387-26528-7_4

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. *Journal of Information Technology, 30*(2), 91-100. http://dx.doi.org/10.1057/jit.2014.35

Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defense triage process. *Computers & Security, 70*, 467-481. https://doi.org/10.1016/j.cose.2017.07.009

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*(1), 98. https://doi.org/10.1037//0021-9010.78.1.98

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

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334. https://dx.doi.org/10.1007/bf02310555

Cuenca, L., Boza, A., & Ortiz, A. (2011). An enterprise engineering approach for the alignment of business and information technology strategy. *International Journal of Computer*

Integrated Manufacturing, 24(11), 974-992. http://dx.doi.org/10.1080/0951192X.2011.579172

Cvejic, R., Markovic, A., & Cvejic, R. (2014). Supervisory control (SCADA) systems and their implementation in the high voltage plants. *Annals Of The Oradea University. Fascicle of Management and Technological Engineering, XXIII (XIII), 2014/3*(3). https://doi.org/10.15660/auofmte.2014-3.3069

Davenport, T. H., & Short, J. E. (1990). The new industrial engineering: Information technology and business process redesign. *Sloan Management Review, 31*(4), 11-27. Retrieved from https://sloanreview.mit.edu/

Dehlawi, Z., & Abokhodair, N. (2013). *Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident.* Paper presented at the Intelligence and Security Informatics. https://doi.org/10.1109/isi.2013.6578789

Department of Homeland Security. (2014). *ICS-CERT Year in Review*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf

Department of Homeland Security. (2016). *ICS-CERT Year in Review*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

Department of Homeland Security. (2017). Critical Infrastructure Sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

Drnevich, P. L., & Croson, D. C. (2013). Information technology and business-level strategy: Toward an integrated theoretical perspective. *MIS Quarterly, 37*(2), 483-509. https://doi.org/10.25300/misq/2013/37.2.08

Enoiu, E. P. (2015). Programming languages popularity and implications to testing programmable logic controllers. *PeerJ PrePrints*. http://dx.doi.org/10.7287/peerj.preprints.879v1

Exec. Order No. 13636, 3 C.F.R. 33 (2013).

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods, 41*(4), 1149-1160. https://doi.org/10.3758/brm.41.4.1149

Field, A. (2013). *Discovering statistics using IBM SPSS statistics (4th. ed)*. Thousand Oaks, CA: Sage.

Foddy, W. (1998). An empirical evaluation of in-depth probes used to pretest survey questions. *Sociological Methods & Research, 27*(1), 103-133. http://dx.doi.org/10.1177/0049124198027001003

Fowler, F. J. (2009). *Survey research methods* (4th Ed.). Thousand Oaks, CA: Sage.

Furukawa, M., Hirobayashi, S., & Misawa, T. (2014). A study on the "flexibility" of information systems (Part 3): MIS flexibility planning scheme for IT/business strategy alignment. *International Journal of Business and Management, 9*(6), 88-97. https://dx.doi.org/10.5539/ijbm.v9n6p88

Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Philip Chen, C. L. (2014). SCADA communication and security issues. *Security & Communication Networks, 7*(1), 175-194. http://dx.doi.org/10.1002/sec.698

Garg, A., & Goyal, D. P. (2012). Striving towards strategic alignment in SMEs: An empirical analysis. *Journal of Advances in Management Research, 9*(1), 77-95. http://dx.doi.org/10.1108/09727981211225662

Garson, G. D. (2012). *Testing statistical assumptions*. Asheboro, NC: Statistical Associates Publishing.

Gehlbach, H., & Brinkworth, M. E. (2011). Measure twice, cut down error: A process for enhancing the validity of survey scales. *Review of General Psychology, 15*(4), 380-387. https://doi.org/10.1037/a0025704

Gerow, J. E., Grover, V., Thatcher, J., & Roth, P. L. (2014). Looking toward the future of IT–business strategic alignment through the past: A meta-analysis. *MIS Quarterly, 38*(4), 1159-1186. https://doi.org/10.25300/misq/2014/38.4.10

Gerow, J. E., Thatcher, J. B., & Grover, V. (2015). Six types of IT-business strategic alignment: an investigation of the constructs and their measurement. *European Journal of Information Systems, 24*(5), 465-491. https://doi.org/10.1057/ejis.2014.6

Ghani, A. T. A., & Zakaria, M. S. (2013). Business-IT models drive businesses towards better value delivery and profits making. *Procedia Technology, 11*, 602-607. https://dx.doi.org/10.1016/j.protcy.2013.12.234

Ginter, A. (2013). Securing industrial control systems. *Chemical Engineering, 120*(7), 30-35. Retrieved from http://www.chemengonline.com/

Gitzel, R., Schmitz, B., Fromm, H., Isaksson, A., & Setzer, T. (2016). Industrial services as a research discipline. *Enterprise Modelling and Information Systems Architectures, 11*(4). Retrieved from https://emisa-journal.org/emisa

Goepp, V., & Avila, O. (2015). An extended-strategic alignment model for technical information system alignment. *International Journal of Computer Integrated Manufacturing, 28*(12), 1275-1290. https://dx.doi.org/10.1080/0951192X.2014.964774

Gonzalez-Benito, J., & Lannelongue, G. (2014). An integrated approach to explain the manufacturing function's contribution to business performance. International Journal of Operations & Production Management, 34(9), 1126-1152.

Griffiths, P. A. (1995). *On being a scientist: Responsible conduct in research (2nd Ed.)*. Washington, DC: National Academies Press. https://doi.org/10.17226/4917

Guri, M., Monitz, M., & Elovici, Y. (2017). Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack. *ACM Transactions on Intelligent Systems and Technology, 8*(4), 1-25. http://dx.doi.org/10.1145/2870641.

Hajikhani, A., & Azadi, A. (2013). Strategic alignment analysis between IT-business strategies. *Interdisciplinary Journal of Contemporary Research In Business, 5*(1), 528-536. Retrieved from http://ijcrb.webs.com/

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis, 38*(2), 215-225. https://doi.org/10.1111/risa.12878

Hellmann, H. (2015). Acknowledging the threat: Securing United States pipeline SCADA systems. *Energy Law Journal, 36*(1), 157-178. Retrieved from https://www.eba-net.org/felj/energy-law-journal/

Henderson, J. C., Rockart, J. F., & Sifonis, J. G. (1987). Integrating management support systems into strategic information systems planning. *Journal of Management Information Systems, 4*(1), 5-24. https://dx.doi.org/10.1080/07421222.1987.11517783

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4. https://dx.doi.org/10.1147/sj.1999.5387096

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243. https://dx.doi.org/10.1108/09685220310500153

Hoertel, N., Chevance, A., Limosin, F. (2017). *Inclusion and Exclusion Criteria and Psychological Research*. Thousand Oaks, CA: Sage.

Hoyt, W. T., Imel, Z. E., & Chan, F. (2008). Multiple regression and correlation techniques: Recent controversies and best practices. *Rehabilitation Psychology, 53*(3), 321-339. http://dx.doi.org/10.1037/a0013021

Huang, L. K. (2012). The impact of IT management sophistication on perceived IT importance in strategic alignment. *The Journal of Computer Information Systems, 53*(2), 50-64. Retrieved from https://www.tandfonline.com/toc/ucis20/current

Ilves, T. H. (2016). The consequences of cyber attacks. *Journal of International Affairs, 70*(1), 175-178,111. Retrieved from https://jia.sipa.columbia.edu/

ISA99 (2017). ISA-62443-1-1 - Security for industrial automation and control systems: Models and concepts. Retrieved from http://isa99.isa.org/Public/Series/Documents/ISA-62443-1-1-Public.pdf

ISA99 (2004). Manufacturing and control systems security part 1: Models and terminology. Retrieved from http://isa99.isa.org/

Ismail, S., Sitnikova, E., & Slay, J. (2014). *Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study*. Paper presented at the 11th Fuzzy Systems and Knowledge Discovery. https://dx.doi.org/10.1109/FSKD.2014.6980976

Istikoma, Bt Fakhri, N. F., Qurat ul, A., & Ibrahim, J. (2015). Information security aligned to enterprise management. *Middle East Journal of Business, 10*(1), 62-66. https://doi.org/10.5742/mejb.2015.92601

Janicke, H., Nicholson, A., Webber, S., & Cau, A. (2015). Runtime-monitoring for industrial control systems. *Electronics, 4*(4), 995-1017. https://dx.doi.org/10.3390/electronics4040995

Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: Sample size for pilot studies. *Educational and Psychological Measurement, 70*(3), 394-400. http://dx.doi.org/10.1177/0013164409355692

Kaiser, R. (2015). The birth of cyberwar. *Political Geography, 46*, 11-20. https://doi.org/10.1016/j.polgeo.2014.10.001

Kankanhalli, A., Teo, H.H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154. https://doi.org/10.1016/s0268-4012(02)00105-6

Karnouskos, S. (2011). *Stuxnet worm impact on industrial cyber-physical system security.* Paper presented at the IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. https://doi.org/10.1109/iecon.2011.6120048

Knijff, f. M. v. d. (2014). Control systems/SCADA forensics, what's the difference? *Digital Investigation, 11*(3), 160.

Kruger, C. J., & Noxolo Mama, M. (2012). Incorporating business strategy formulation with identity management strategy formulation. *Information Management & Computer Security, 20*(3), 152-169. https://dx.doi.org/10.1108/09685221211247271

Kumar, K., Kaur, P., & GNDU, A. (2015). A generalized process of reverse engineering in software protection & security.

Kuusk, A., Koronios, A., & Gao, J. (2013). *Overcoming integration challenges in organisations with operational technology.* Paper presented at the 24th Australasian Conference on Information Systems. https://doi.org/10.1109/iecon.2011.6120048

Laerd (2013). Ordinal regression using SPSS statistics. Retrieved from https://statistics.laerd.com/spss-tutorials/ordinal-regression-using-spss-statistics.php

Lee, O. K. D., Xu, P., Kuilboer, J.-P., & Ashrafi, N. (2016). Idiosyncratic Values of IT-enabled Agility at the Operation and Strategic Levels. *Communications of the Association for Information Systems, 39*, 242-266. https://doi.org/10.17705/1cais.03913

Leung, S.-O. (2011). A comparison of psychometric properties and normality in 4-, 5-, 6-, and 11-point likert scales. *Journal of Social Service Research, 37*(4), 412-421. http://dx.doi.org/10.1080/01488376.2011.580697

Logan, B. (2015). Pandora's net. *Mechanical Engineering, 137*(1), 28-33. https://doi.org/10.1115/1.2015-jan-1

Lowry, P. B., & Wilson, D. (2016). Creating agile organizations through IT: The influence of internal IT service perceptions on IT service quality and IT agility. *The Journal of Strategic Information Systems, 25*(3), 211-226. https://dx.doi.org/10.1016/j.jsis.2016.05.002

Maitra, A. K. (2015). Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems & Decisions, 35*(1), 169-182. http://dx.doi.org/10.1007/s10669-014-9520-7

Martin, P. G. (2012). The need for enterprise control. *InTech, 59*(6), 12-14,16,18. Retrieved from https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/

Mathy, R. M., Kerr, D. L., & Haydin, B. M. (2003). Methodological rigor and ethical considerations in Internet-mediated research. *Psychotherapy: Theory, Research, Practice, Training, 40*(1-2), 77. https://doi.org/10.1037/0033-3204.40.1-2.77

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological Methods, 17*(3), 437-455. http://dx.doi.org/10.1037/a0028085

Menard, S. (2010). *Logistic regression: From introductory to advanced concepts and applications*. https://doi.org/10.4135/9781483348964

Mertler, C. A., & Vannatta, R. A. (2013). Advanced and multivariate statistical methods (5th ed.). Los Angeles, CA: Pyrczak.

Nawi, I., Aisham, B., Pauline, O., & Jaffery, N. (2016). Review on system operation of auto-feeder for door panel production using programmable logic controller. *ARPN Journal of Engineering and Applied Sciences, 11*, 5326-5330. Retrieved from http://www.arpnjournals.com/jeas/

Neitzel, L., & Huba, B. (2014). Top ten differences between ICS and IT cybersecurity. *InTech, 61*(3), 12-18. Retrieved from https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education, 15*(5), 625-632. https://dx.doi.org/10.1007/s10459-010-9222-y

Nunnally, J. C. (1975). Psychometric Theory - 25 Years ago and now. *Educational Researcher, 4*(10), 7-21. https://doi.org/10.2307/1175619

Obeid, F., & Dhaussy, P. (2016). RITA secure communication protocol: application to SCADA. *Computer Science & Information Technology, 6*(15), 1-12. https://dx.doi.org/10.5121/csit.2016.61504

Oborski, P. (2014). Developments in integration of advanced monitoring systems. *International Journal of Advanced Manufacturing Technology, 75*(9-12), 1613-1632. https://dx.doi.org/10.1007/s00170-014-6123-x

Onwuegbuzie, A. J., & Collins, K. M. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report, 12*(2), 281-316. Retrieved from https://nsuworks.nova.edu/tqr/

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems, 18*, 26-45. http://dx.doi.org/10.1016/j.accinf.2015.06.001

Patrakosol, B., & Lee, S. M. (2009). IT capabilities, interfirm performance, and the state of economic development. *Industrial Management & Data Systems, 109*(9), 1231-1247. http://dx.doi.org/10.1108/02635570911002298

Perepletchikov, M., Ryan, C., & Tari, Z. (2013). An analytical framework for evaluating service-oriented software development methodologies. *Journal of Software, 8*(7), 1642-1659. http://dx.doi.org/10.4304/jsw.8.7.1642-1659

Pieters, W., Dimkov, T., & Pavlovic, D. (2013). Security policy alignment: A formal approach. *Systems Journal, IEEE, 7*(2), 275-287. http://dx.doi.org/10.1109/JSYST.2012.2221933

Piggin, R. (2014). Industrial systems: Cyber-security's new battlefront. *Engineering & Technology, 9*(8), 70-74. https://doi.org/10.1049/et.2014.0810

The White House. (1998). *Presidential decision directive - Critical infrastructure protection*. Retrieved from http://fas.org/irp/offdocs/pdd/pdd-63.pdf

The White House. (2003) *Homeland security presidential directive - Critical Infrastructure Identification, Prioritization, and Protection.* Retrieved from https://fas.org/irp/offdocs/nspd/hspd-7.html

The White House. (2013) *Presidential policy directive -- Critical infrastructure security and resilience*. Retrieved from http://fas.org/irp/offdocs/ppd/ppd-21.pdf

Wu S.P.J., Straub, D. W., & Liang, T.P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly, 39*(2), 497-A497. Retrieved from https://doi.org/10.25300/misq/2015/39.2.10

Pn, S. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security, 22*(5), 450-473. https://doi.org/10.1108/imcs-05-2013-0035

Ponomarev, S. (2015). *Intrusion Detection System of industrial control networks using network telemetry* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Thesis Global database. (3664531)

Pretorius, B., & Niekerk, B. V. (2015). *Cyber-Security and Governance for ICS/SCADA in South Africa*. Paper presented at the proceedings of 10th International Conference on Cyber Warfare and Security*,* Kruger National Park, South Africa.

Renaud, A., Walsh, I., & Kalika, M. (2016). Is SAM still alive? A bibliometric and interpretive mapping of the strategic alignment research field. *The Journal of Strategic Information Systems, 25*(2), 75-103. https://dx.doi.org/10.1016/j.jsis.2016.01.002

Roberts, N., & Grover, V. (2012). Leveraging information technology infrastructure to facilitate a firm's customer agility and competitive activity: An empirical investigation. *Journal of Management Information Systems, 28*(4), 231-270. https://dx.doi.org/10.2753/mis0742-1222280409

Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. Special Publication (NIST SP)-800-53 Rev 4.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access, 4*, 1375-1384. http://dx.doi.org/10.1109/ACCESS.2016.2549047

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly, 27*(2), 237-263. https://doi.org/10.2307/30036530

Sardana, D., Terziovski, M., & Gupta, N. (2016). The impact of strategic alignment and responsiveness to market on manufacturing firm's performance. *International Journal of Production Economics, 177*(1), 131-138. https://doi.org/10.1016/j.ijpe.2016.04.018

Sauer, C., Yetton, P. W., & Alexander, L. (1997). *Steps to the future: Fresh thinking on the management of IT-based organizational transformation.* San Francisco, LA: Jossey-Bass Inc.

Sawas, M., & Watfa, M. (2015). The impact of cloud computing on information systems agility. *Australasian Journal of Information Systems, 19*. https://dx.doi.org/10.3127/ajis.v19i0.930

Sedgewick, A. (2014). Framework for improving critical infrastructure cybersecurity, version 1.0. NIST-Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework

Schiavone, S., Garg, L., & Summers, K. (2014). Ontology of information security in enterprises. *Electronic Journal of Information Systems Evaluation, 17*(1), 71-87. Retrieved from http://www.ejise.com/main.html

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill building approach*. West Sussex, United Kingdom: John Wiley & Sons.

Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS Quarterly, 37*(2), 565-590. https://doi.org/10.25300/misq/2013/37.2.11

Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014a). A review: Industrial control system (ICS) and their security issues. *American Journal of Applied Sciences, 11*(8), 1398-1404. https://doi.org/10.3844/ajassp.2014.1398.1404

Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014b). *Industrial control systems (ICS) vulnerabilities analysis and SCADA security enhancement using testbed encryption*. Retrieved from: http://dl.acm.org/citation.cfm?doid=2557977.2558061

Shanks, G., Bekmamedova, N., & Willcocks, L. (2013). Using business analytics for strategic alignment and organisational transformation. *International Journal of Business Intelligence Research, 4*(3), 1-15. http://dx.doi.org/10.4018/ijbir.2013070101

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Journal of Internet Law, 18*(6), 3-6. Retrieved from https://lrus.wolterskluwer.com/store/product/journal-of-internet-law/000000000010015615

Siurdyban, A. (2014). Understanding the IT/business partnership: A business process perspective. *Information Systems Frontiers, 16*(5), 909-922. http://dx.doi.org/10.1007/s10796-012-9388-3

Smaczny, T. (2001). Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations? *Management Decision, 39*(10), 797-802. https://doi.org/10.1108/eum0000000006521

Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security. *Special Publication (NIST SP)-800-82 Rev 2*.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston, MA: Pearson.

Tallon, P. P., & Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model. *MIS Quarterly, 35*(2), 463-486. https://doi.org/10.2307/23044052

Tallon, P. P., Queiroz, M., Coltman, T. R., & Sharma, R. (2016). Business process and information technology alignment: Construct conceptualization, empirical illustration, and directions for future research. *Journal of the Association for Information Systems, 17*(9), 563-589. https://doi.org/10.17705/1jais.00438

Tan, F. T. C., Tan, B., Wang, W., & Sedera, D. (2016). IT-enabled operational agility: An interdependencies perspective. *Information & Management, 54*(3) http://dx.doi.org/10.1016/j.im.2016.08.001

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55. http://dx.doi.org/10.5116/ijme.4dfb.8dfd

Taveras, P. (2013). Scada live forensics: Real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal*. Retrieved from https://eujournal.org/index.php/esj

Teddlie, C., & Yu, F. (2007). Mixed methods sampling. *Journal of Mixed Methods Research, 1*(1), 77-100. http://dx.doi.org/10.1177/2345678906292430

Thao, T.-P., Molla, A., & Peszynski, K. (2012). Enterprise systems and organizational agility: A review of the literature and conceptual framework. *Communications of the Association for Information Systems, 31*, 167-193.

Trochim, W. M. (2006). The research methods knowledge base (2nd Ed). Retrieved from http://www.socialresearchmethods.net/kb/

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis. *Information & Computer Security*, *26*(2), 150-170. https://doi.org/10.1108/ics-06-2017-0042

Turel, O., Liu, P., & Bart, C. (2017). Board-level information technology governance effects on organizational performance: The roles of strategic alignment and authoritarian governance style. *Information Systems Management, 34*(2), 117-136. https://doi.org/10.1080/10580530.2017.1288523

Tzokatziou, G., Maglaras, L. A., Janicke, H., & He, Y. (2015). Exploiting SCADA vulnerabilities using a Human Interface Device. *International Journal of Advanced Computer Science and Applications, 6*(7), 234-241. https://doi.org/10.14569/ijacsa.2015.060731

U.S. Department of Commerce (2013). *Recommendations to the president on incentives for critical infrastructure owners and operators to join a voluntary cybersecurity program*. Retrieved form https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf

Vos, P., Tjemkes, B., Klaver, M., & Verner, D. R. (2017). Enhancement of public-private partnerships within critical infrastructure protection programs. *Critical Infrastructure Protection Review*, 19. Retrieved from https://www.criticalinfrastructureprotectionreview.com/

Verizon (2016). Data breach investigations report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Vlachos, V., Minou, M., Assimakopouos, V., & Toska, A. (2011). The landscape of cybercrime in Greece. *Information Management & Computer Security, 19*(2), 113-123. http://dx.doi.org/10.1108/09685221111143051

Weerakkody, S., Liu, X., Son, S. H., & Sinopoli, B. (2017). A graph-theoretic characterization of perfect attackability for secure design of distributed control systems. *IEEE Transactions on Control of Network Systems*, *4*(1), 60-70. https://doi.org/10.1109/acc.2016.7525076

Wu, S. P., Straub, D. W., & Liang, T. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and it managers. *MIS Quarterly, 39*(2), 497. https://doi.org/10.25300/misq/2015/39.2.10

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Business Systems, Governance & Ethics, 9*(2), 50-65. https://dx.doi.org/10.15209/jbsge.v9i2.718

Yang, L. R. (2013). Key practices, manufacturing capability and attainment of manufacturing goals: The perspective of project/engineer-to-order manufacturing. *International Journal of Project Management, 31*(1), 109-125. https://dx.doi.org/10.1016/j.ijproman.2012.03.005

Yayla, A. A., & Hu, Q. (2012). The impact of IT-business strategic alignment on firm performance in a developing country setting: Exploring moderating roles of environmental uncertainty and strategic orientation. *European Journal of Information Systems, 21*(4), 373-387. http://dx.doi.org/10.1057/ejis.2011.52

Zhenhua, Y., Jie, O., Sisi, L., & Xia, P. (2017). Formal modeling and control of cyber-physical manufacturing systems. *Advances in Mechanical Engineering, 9*(10). doi:10.1177/1687814017725472

STATEMENT OF ORIGINAL WORK

Academic Honesty Policy

Capella University's Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.

Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person's ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others' work through proper citation and reference. Use of another person's ideas, including another learner's, without proper reference or citation constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else's ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University's Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

Statement of Original Work and Signature

I have read, understood, and abided by Capella University's Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Learner name and date Devecchio Turner 07/23/18

APPENDIX A. SURVEY INSTRUMENT RESEARCHER-CREATED

1. Click Agree/Disagree to continue/exit
2. How many years of experience do you have securing industrial control or SCADA environments?
3. Are you 18 or older [] Yes []No
4. Please select your age group [] 18-29 []30-39 []40-49 []50-59 []60 or older
5. Please select your gender []Male []Female
6. How many people are employed by your company? []<50 []51 – 250 [] 251 – 1001 []1000 - 10000 []>10000
7. Please select your industry [] City or Municipality []Energy []Manufacturing []Other
8. What is the highest level of school you have completed or the highest degree received?

Business-IT Strategy Alignment - Identify the extent to which IT supports the business in these functions	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
9. IT supports the business by reflecting business plan missions							
10. IT supports the business by reflecting business plan goals							
11. IT supports the business by supporting business strategies							
12. IT supports the business by recognizing external business environmental forces							
13. IT supports the business by reflecting business resource constraints							

IT-Business Strategy Alignment- Identify the extent to which the business is aligned to IT in these functions	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
14. The business supports IT by reflecting the information systems (IT) plan							
15. The business supports IT by referring to specific information systems (IT) applications							
16. The business supports IT by referring to the information systems (IT) plan							
17. The business supports IT by utilizing the strategic capability of information systems (IT)							
18. The business supports IT by having reasonable expectations of information systems (IT)							

IT Capability	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
19. Flexible electronic links exist between IT and partner organizations							
20. IT infrastructure can quickly adapt to new tasks							
21. There are very few identifiable IT bottlenecks between IT and partner organizations							
22. Various forms of electronic data received from partners are assimilated and utilized quickly within IT							
23. Information is shared seamlessly between IT and partners, regardless of location							

Information Security Effectiveness	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
24. Security measures in your organization have an overall deterrent effect							
25. Security measures in your organization have an overall preventative effect							
26. Security measures in your organization are effective in protecting hardware							
27. Security measures in your organization protect software							
28. Security measures in your organization protect data							
29. Security measures in your organization protect computer services							

APPENDIX B. HISTOGRAMS AND P-P PLOTS

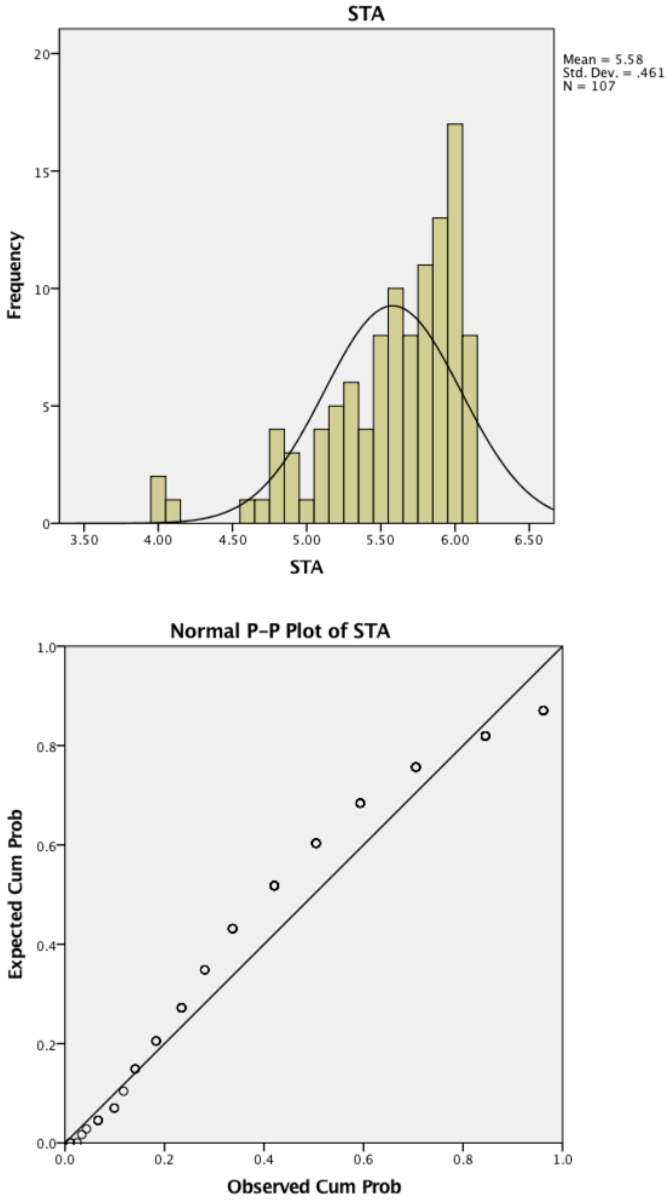

Figure B1. Strategic alignment histogram and P-P plot

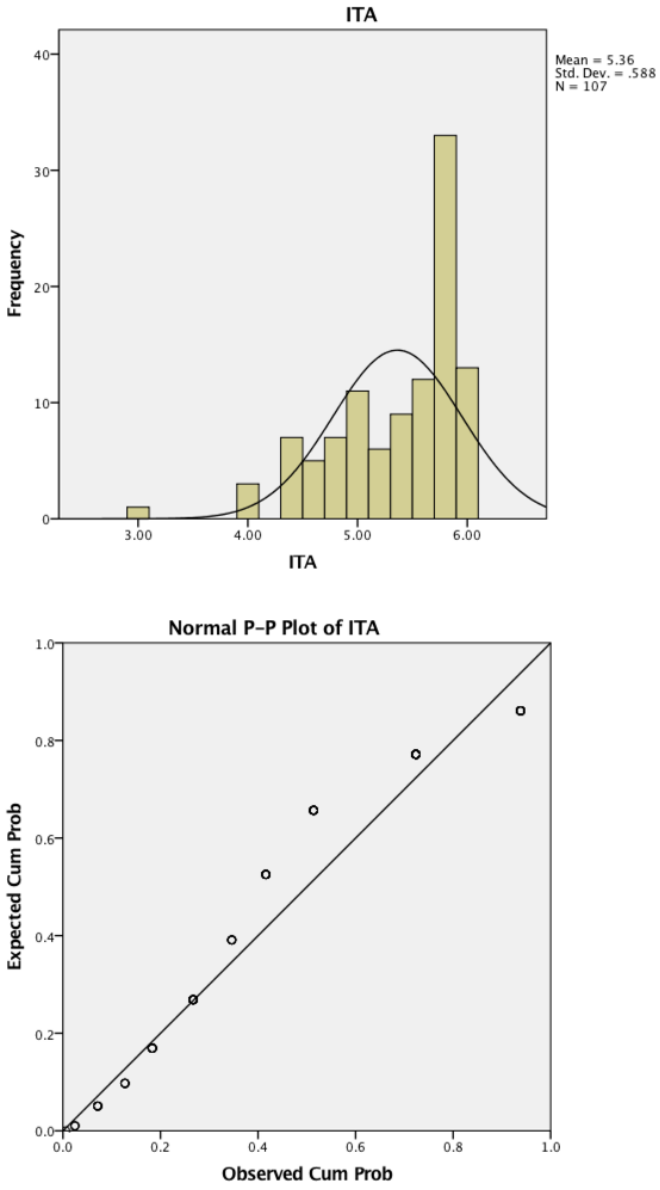

Figure B2. Agility histogram and P-P plot

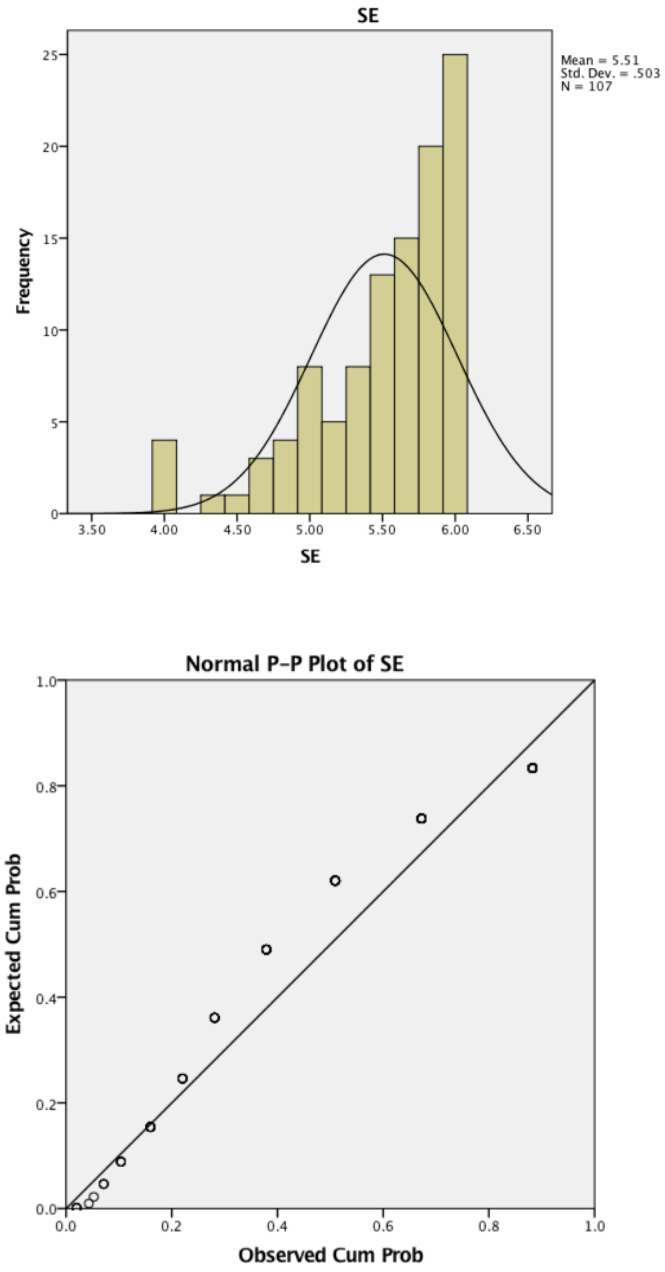

Figure B3. Security efficacy histogram and P-P plot

APPENDIX C. EXPLORATORY BOX PLOT

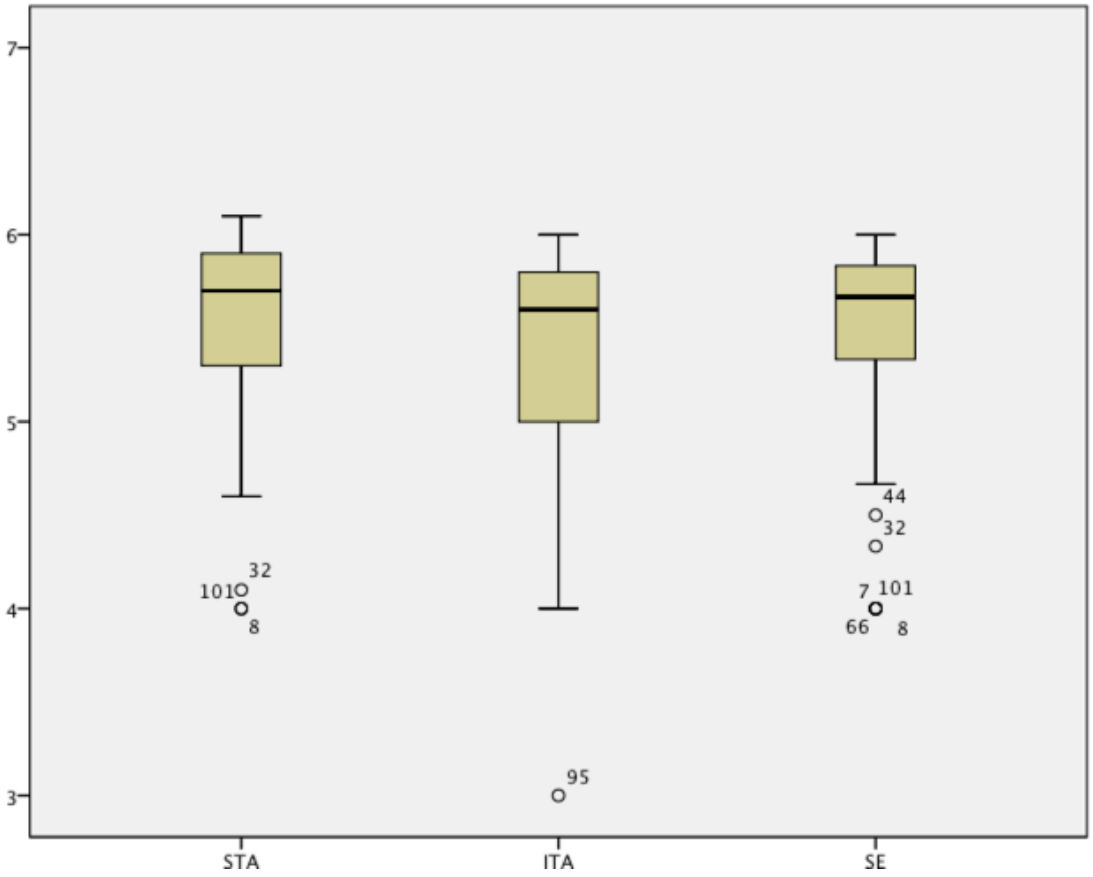

Figure C1. Exploratory box plot