MEASURING THE STATE OF INDIANA'S CYBERSECURITY

by

James E. Lerums

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Technology

West Lafayette, Indiana

December 2018

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. James E. Dietz
Purdue Polytechnic Institute
Dr. Joseph F. Pekny
College of Engineering
Dr. John A. Springer
Purdue Polytechnic Institute
Dr. Baijian Yang
Purdue Polytechnic Institute

Approved by:

Dr. Kathryne A Newton
Head of the Graduate Program

To my family, past, present, future, here and abroad

ACKNOWLEDGMENTS

I have come to deeply believe that most significant accomplishments are seldom done alone, and it certainly applies to this thesis. First, I would like to express my appreciation and gratitude to the members of my committee for not only their support of this thesis but also for their sage advice and counsel during my classes with them and subsequent endeavors. As my chair, Professor J. Eric Dietz, I thank you for all your spot-on coaching, teaching, and mentoring and the several opportunities with awesome support you have afforded me. Without your government and industry engagements, this thesis would not have had the real world and real time relevance to current events it has. To Professor Baijian Yang, thank you for your keen insights in network security, encouragement, and enabling me to present my first conference paper. To Professor John Springer thank you for sharing your time and providing a very much appreciated sounding board for my thesis statistics ideas. To Professor Joseph Pekny, thank you for your enthusiastic support of the real-world foundation for my thesis. To Professor Connie Justice thank you for your insightful support to include providing "in the nick of time" a solution that focused the Cybersecurity Scorecard and kept it on track.

The topic and data for this thesis would not have been possible without Chetrice Mosley, Cybersecurity Program Director, inviting Purdue to partner with the State of Indiana's Executive Council on Cybersecurity (IECC). Her deep and sustained support along with Noel Lephart's, IECC Program Manager, and the IECC's critical sector and key resource Committees afforded this study invaluable feedback and data. The collaboration proved to be an invaluable opportunity to observe Indiana's incredible public and private cybersecurity team meet the challenges head on.

During the research for this dissertation, I am also very grateful for the support and pleasure of working with Katie Reichart, Graduate Research Assistant, Ben Holmes from Purdue's Academic Technology Department and Daniel Vasquez Carvajal from Purdue's Statistics Consulting Department. Without their thorough and proactive support this dissertation's research and analysis would not have not been available in time to support the Indiana Cybersecurity Strategic Plan published September 2018.

To Professor Eugene Spafford, I can't thank you enough for enabling me to obtain a Ph.D. Beginning before I even applied to Purdue, your insightful, and candid counsel was always there when needed and deepened my understanding in so many aspects of information security. The timeless support from you and Joel Rasmus, Marlene Walls, Jerry Haan, Lori Floyd, Adam Hammer, and Mike Focosi from the Center for Education and Research in Information Assurance and Security (CERIAS) has been invaluable.

Finally, to my greatest supporters, my greatest critics, and advocates, I would like to thank my dear family for their sacrifices, love, and patience they have provided me over the decades.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Critical Infrastructure Sector – is a sector whose assets, networks, systems which could be virtual or physical is so vital to the United States that its destruction or incapacitation would significantly debilitate national security, economic security, public health, or safety or any combination thereof.

Cybersecurity Tools – assessment and standards documentation and/or software that enables organizations to assess, plan, and execute cybersecurity improvements based on their business requirements, risk tolerances, and resources.

Internet of Things – the internet connection of computing devices embedded in everyday objects, which include cameras for baby monitors, household thermostats, cell phones, as well as controls oil refineries or a car painting robot in an automotive plant

Industrial Control System – is a general term that describes several types of controls including a programmable logic controller, distributed control system, and supervisory control and data acquisition systems

Private Organizations – non-government organizations to include sole proprietorships, not for profit, corporations, and limited liability corporations

Public Organizations – government organizations to include state or federal departments and agencies, counties, cities, towns, villages, tribes, and territories

LIST OF ABBREVIATIONS

AWWA	American Water Works Association
CSF	Cybersecurity Framework
CI	Critical Infrastructure
COTS	Commercial Off the Shelf
CSET	Cyber Security Evaluation Tool
DCS	Distributed Control System
DHS	Department of Homeland Security
DoD	Department of Defense
EMA	Emergency Management Agency
EOP	Emergency Operations Plan
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team
IDHS	Indiana Department of Homeland Security
IECC	Indiana Executive Council on Cybersecurity
IED	Intelligent Electronic Device
IoT	Internet of Things
NIST	National Institute of Standards and Technology
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

ABSTRACT

Author: Lerums, James E. PhD
Institution: Purdue University
Degree Received: December 2018
Title: Measuring the State of Indiana's Cybersecurity
Committee Chair: James Eric Dietz

This dissertation introduces a scorecard to enable the State of Indiana to measure the cybersecurity of its public and private critical infrastructure and key resource sector organizations. The scorecard was designed to be non-threatening and understandable so that even small organizations without cybersecurity expertise can voluntarily self-asses their cybersecurity strength and weaknesses. The scorecard was also intended to enable organizations to learn, so that they may identify and self-correct their cybersecurity vulnerabilities. The scorecard provided quantifiable feedback to enable organizations to benchmark their initial status and measure their future progress.

Using the scorecard, the Indiana Executive Council for Cybersecurity launched a Pilot to measure cybersecurity of large, medium, and small organizations across eleven critical infrastructure and key resources sectors. This dissertation presents the analysis and results from scorecard data provided by the Pilot group of 56 organizations. The cybersecurity scorecard developed as part of this dissertation has been included in the Indiana Cybersecurity Strategy Plan published September 21, 2018.

CHAPTER 1. INTRODUCTION

This chapter provides an overview of this research study. This chapter begins with the background to the problem and is followed by the significance of the research, statement of purpose, research questions, assumptions, limitations, and delimitations. Finally, this chapter concludes with a brief overview of the remaining chapters.

1.1 Background

In Symantec's most recent April 2018 Internet Security Threat Report, it noted that between 2015 and 2017 the United States was affected by 303 targeted attacks. This was the most of any country (followed by India with 133 targeted attacks) (Symantec Corporation, 2018). In its 2018 report, the Ponemon Institute reported that the United States had the highest four year average total data breach cost of any nation at $7.91 million (a 7.6% increase from the previous year's $7.35 million) followed by the Middle East with an average total data breach cost of $5.31 million (Ponemon Institute LLC, 2018). Thus, the United States is the global leader suffering from targeted attacks and average total costs of data breaches.

The above targeted attacks and data breaches are not exclusive to private sectors. In Verizon's 2018 Data Breach Investigations Report, the Public Administration sector was recorded with the greatest total cyber incidents and the second most breaches compared to the other twenty private sectors (Verizon, 2018). Given the frequency of daily cyberattacks, State Governors have recognized that cyber threats pose serious risks to the core interests of their states. Generally, they state that a public private partnership and information sharing will be essential for success. While private companies possess most of our nation's capability to detect and defend against cybercrime, only government has the legal authority to pursue and punish the perpetrators (National Governors Association, 2017b).

The required hand in glove partnership between the private and public sectors is required not only for cyber-crime detection, defense, pursuit, and punishment, but also because of the cyber integration of private and public organizations. Not only do

businesses and individuals access public services over the internet (vehicle registration, paying income taxes, etc.) but they also conduct "Business to Business" (B2B) commercial transactions (purchasing, billing, funds transfers, etc.) with each other. Since these transactions occur mostly over the internet, cybersecurity requires a shared effort making it a team sport.

Close collaboration is required for a state's public and private organizations to succeed improving their collective cybersecurity. It requires tracking progress during the planning and execution of collective cybersecurity goals, strategies, objectives, and initiatives. How do you track cybersecurity progress across diverse environments (government, health care, manufacturing, finance, etc.) so all participants understand what they and others must focus on to win? Given small public and private organizations may lack cyber expertise, how do you collect their relevant cybersecurity information?

Attempting to answer these questions is the goal of this research. Its purpose is to provide actionable information to individual organizations, industry alliances, and state and local governments for focusing limited resources to accelerate cybersecurity improvements.

1.2 Significance

Research of several cybersecurity standards, and assessment tools revealed the "state of the art" offers detailed and thorough instruments that small and/or non-information technology organizations across several sectors would be challenged (if even able) to complete. This means there may be thorough and clear cybersecurity status data for many large and some medium size organizations but less for small organizations. Absence of cybersecurity status visibility for small organizations is concerning given, for example, that in the State of Indiana during 2016, 83.3% of its 146,078 establishments had 19 or less employees (U.S. Census, 2016). Additionally, Verizon reported for 2017 58% of the cyber breaches victims were small businesses (Verizon, 2018). This study focused on developing a methodology and collecting actionable cybersecurity information for organizations across all size categories and sectors. The insights contained in this study should help public and private organizations save time by focusing limited resources and attention to improve their collective cybersecurity.

1.3 Statement of Purpose

The purpose of this research was to design, based on best practices, a cybersecurity scorecard from which organizations with or without cybersecurity expertise can self-assess, learn, and initiate focused improvements. By asking standards-based questions the scorecard may lead to insights of cybersecurity vulnerabilities unique to specific critical infrastructure or key resource sectors and/or organization size categories. These insights can aid accelerating real word/real time cybersecurity improvements by mitigating the risk of investing limited resources in the wrong areas.

1.4 Research Questions

The questions central to this research were:

1. Is it possible to develop a cybersecurity scorecard based on identified vulnerabilities and threats, that provides effective actionable information for public and private organizations in the State of Indiana regardless of size or cyber expertise?
2. How well will the cybersecurity scorecard quantitatively identify actionable information that may be unique to organizations in different critical infrastructure sectors and/or size categories?

1.5 Assumptions

The following assumptions were inherent to the pursuit of this study:

1. Effective cybersecurity prevention through identification and protection measures will reduce critical infrastructure cybersecurity incidents more than detection, response, and recovery.
2. Information officially published by industry, government, and academic subject matter experts is accurate and helpful.
3. Vendor specifications for critical infrastructure industrial control systems cybersecurity solutions are accurate and helpful.
4. Cyber threats will continue to evolve, and today's cyber solutions may not suffice for tomorrow.

5. Increasing number of cyber attackers may be a factor to the increasing number of annual cyber incidents.
6. As a utility's industrial control systems cyber vulnerabilities are decreased, some or most cyber attackers will migrate to easier and more lucrative targets.
7. Many if not all industrial control system vendors are working to improve the cybersecurity of their systems, but their solutions are works in process with some vendors leading others.
8. Pilot group members voluntarily, accurately, and without reservation answered scorecard questions.
9. Pilot group members understood scorecard questions.
10. There is risk self-scoring done by participating organizations may differ from scoring conducted by external third-party cybersecurity experts.

1.6 Limitations

The following limitations were inherent in the pursuit of this study:

1. Cybersecurity threats and vulnerability information in this study was limited to publicly available industry, federal, state, and academic open source information as of November 2018.
2. Indiana public and private organizations providing scorecard data were not randomly selected
3. Organization size category definitions for each Indiana critical infrastructure and key resource sectors were determined by the Committees for those sectors independently from each other and may not identical.
4. The sizes categories determination for the organizations that participated in this study was made by the sector Committees for those organizations.
5. There is score inflation risk in the data analyzed in this study given submitted scorecards were based on organizations' self-assessments.
6. The industrial control systems vendors referenced in this paper are not inclusive of all the industry vendors and their mention should not be considered an endorsement by the author or Purdue University.

7. The location of the number of employees (total, information technology personnel, and cybersecurity personnel) was left to the discretion of the organizations submitting the scorecard. For some organizations the employees were exclusively in Indiana exclusively, other organizations counted employees both in Indiana and elsewhere.

1.7 Delimitations

The following delimitations were inherent in the pursuit of this study:

1. Organizations that participated in voluntarily submitting scorecards were known to the sector Committees of the Indiana Executive Council on Cybersecurity Committees.
2. Scorecard responses received were limited by the time available to collect the data from May to September of 2018.
3. Time and resources available limited the number of referenced vendor industrial control systems cybersecurity solutions.

1.8 Organization

This thesis provides five major chapters and appendices. Chapter 2 provides an overview on the fundamentals of critical infrastructure sectors, information technology, industrial control systems and their inherent cyber vulnerabilities. It then discusses tools for increasing cyber security, cybersecurity resource considerations, and potential external factors affecting cybersecurity.

Chapter 3 provides an overview to the motivation and desired outcomes on which the cybersecurity scorecard used in this study was based and describes the methods, procedures and how the scorecard was designed and employed to collect the data.

Chapter 4 describes the analysis and results from the data collected.

Chapter 5 contains a summary of this document, a discussion of the results, and recommendations for future research.

CHAPTER 2. LITERATURE REVIEW

2.1 Overview

To better understand the challenges and benefits of assessing cybersecurity it is important to discuss the definition and importance of critical infrastructure sectors and the challenges in making their information technology and industrial control systems cybersecure. This chapter provides an overview of critical infrastructures, their industrial control systems, cyber-physical attacks, cybersecurity tools, resource considerations, and additional factors that may affect cybersecurity.

2.2 Critical Infrastructures

The United State has identified sixteen critical infrastructure sectors with physical or virtual assets, systems, or networks consider so vital that their incapacitation or destruction would have grave effects on security, national economic security, national public health, or safety, or any combination thereof (The White House, 2013b). The infrastructure sectors include the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communications systems we rely on to stay in touch with friends and family. The following is a list of all the critical infrastructure sectors:

Chemical
Commercial Facilities
Communications Sector
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services Sector
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Water and Wastewater Systems

Significant damage or disruptions of a critical infrastructure could result in potentially catastrophic and cascading consequences. For example, a disruptive cyber-attack on a water utility would have life, safety, and health consequences when fire hydrants fail during a fire, and hospital's operations are impaired

2.3 Fundamentals of Critical Infrastructure Industrial Control Systems

Presidential Decision Directive 63 of May 1998 established the need for protecting the nation's cyber-supported infrastructure sectors which includes, but are not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private (Clinton, 1998). The critical infrastructure is characterized by physical, cyber, geographic, and logical interdependencies and interacting components between sectors (Hentea, 2008).

In addition to traditional information technology, industrial control systems support several critical infrastructure sectors. Industrial controls systems (ICS) is a general term that encompasses several types of controls systems including Programmable Logic Controllers (PLC), distributed control systems (DCS), supervisory control, and data acquisition (SCADA) systems (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015). Control systems can be used in several industry sectors to include manufacturing and distribution. Use of manufacturing controls can be generally categorized for use in process-based and discrete-based manufacturing. Process-based manufacturing industries typically utilize either continuous manufacturing processes or batch manufacturing processes. Continuous manufacturing such as used in oil refineries or chemical distillation plants run continuously even during transitions for making different grades or products. Batch manufacturing such as used in food production has distinct processing steps for a given quantity of material with the possibility of brief steady state operations within intermediate steps. Discrete manufacturing such as used in producing mechanical or electronic parts typically conducts a series of steps on a single device to create the final product.

Distribution industries such as natural gas pipelines, water distribution, and electrical power grids use industrial control systems geographically dispersed often over thousands of square miles. While the actual controls used in manufacturing and

distribution industries are very similar in operation they differ in their environmental deployment. Manufacturing industries usually operate within a confined factory or plant-site with communications riding over a local area network (LAN) with robust and high-speed performance. Distribution industries require long-distance communications over wide-area networks (WAN) and are subject to communication challenges such as delays, and data loss posed by the various communications media required. The various network types also introduce different security controls and challenges (Stouffer et al., 2015). Although a distribution industrial control system may use a LAN and PLCs like a manufacturing control system it has the added complexity of a WAN as shown in Figure 2.1 to connect the Control Center to its Field Sites.

A distribution SCADA system as depicted in Figure 2.1 has several components that perform specific functions (Kambic, Smith, & Yang, 2013; Stouffer et al., 2015).

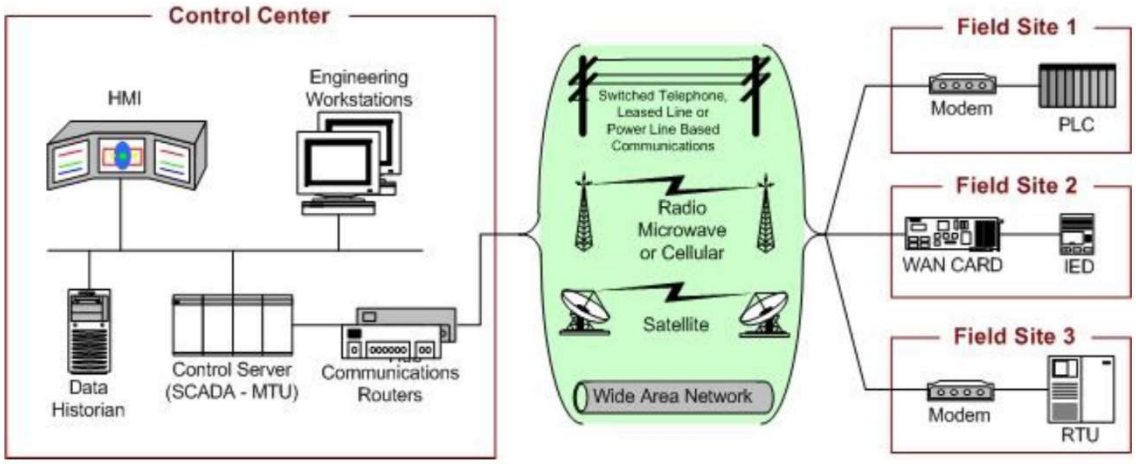

Figure 2.1 Distribution SCADA Systems (Stouffer et al., 2015)

They include:

1. SCADA Master (MTU for Master Terminal Unit) - sends control commands and receives status data from remote terminal units (RTUs), intelligent electronic devices (IEDs), and programmable logic controllers (PLCs). The term “Master” is derived from the protocol given the SCADA initiates the commands, and the RTUs, PLCs, and IEDs respond as slaves.
2. Human Machine Interface (HMI) - provides a graphic display and interface for operators. HMI can either be a hardware/software solution, or a software

application running on industry standard hardware and operating system (such as Microsoft Windows). HMI is sometimes called MMI for Man Machine Interface.

3. Programmable Logic Controller (PLC) – is a solid-state device designed to replace previously used electrical relays using ladder logic. PLCs have migrated from being programmed with ladder logic programming hardware terminals to software applications with intuitive interfacing. PLCs provide core functionality for SCADA operations, but in situations requiring minimal inputs, outputs, and processing intelligent electronic devices can be used.
4. Remote Terminal Unit (RTU) – are generally deployed in field sites and provide remote monitoring and control capability at unattended field sites. RTUs support various communication means to include Public Switched Telephone Network (PSTN), fiber optic cable, and radio/Microwave. For some sites PLCs or IEDs can be used in lieu of RTUs.
5. Application Servers – provide a variety of services in the Control Center to include data processing functions, real time operational process control, and maintaining historical data (for analysis, forecasting, training, accounting, etc.).
6. I/O Servers – provide the communications front end to the system for data acquisition and responsible for collecting, buffering, and providing PLC, RTU, and IED process information.
7. Intelligent Electronic Devices (IED) – solid state technology has enabled various devices such as protective relays to communicate directly with a control server without a PLC or RTU. Local programming IEDs can provide a level of fault-tolerance in case communications to the master fail (Stouffer et al., 2015).

As shown in the generic control system architecture of Figure 2.2 control systems operations networks are usually integrated with the business enterprise network and potentially with external customers and vendors on the internet.

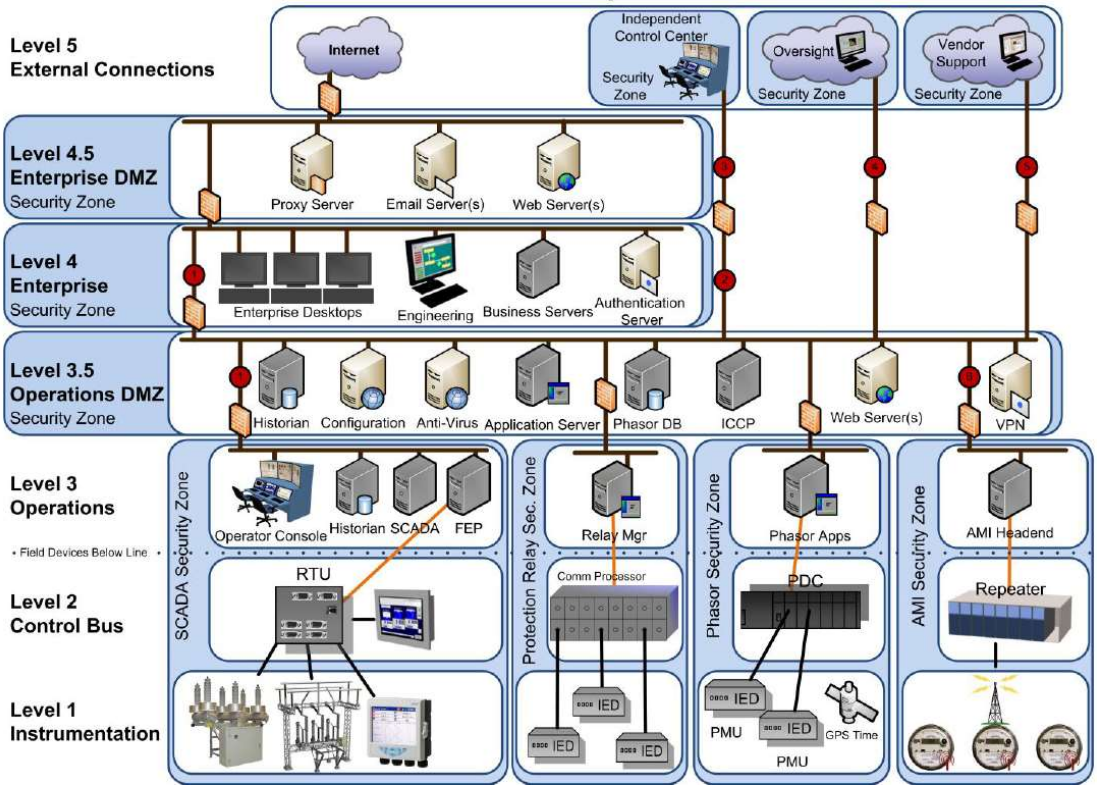

Figure 2.2 Control System Architecture (Mahan, Fluckiger, & Clements, 2011)

Critical infrastructure organizations are under constant pressure to do more with less. Facility owners and operators look at integrating their industrial controls' operational networks with their business networks as a means for improving efficiency and productivity given financial, operational, and compliance restrictions limit their other options. Unfortunately, several of the automation and control systems on operational networks today are often a combination of legacy systems. These legacy system were planned with a life span of twenty to thirty years and were initially designed and installed for reliability and speed and without cyber security considerations (Stouffer et al., 2015).

2.4 Cyber-Physical Attacks

In addition, control systems have evolved from isolated proprietary hardware/software solutions in the 1970's to open systems that include commercial off the shelf (COTS) personal computers, operating systems, TCP/IP communications, and internet access. In other words, industrial control systems that run our critical

infrastructure systems, like our electrical distribution grid (with a required greater than 99.99% operational up time), transportation, and water utilities have gained a significantly increased attack surface and have become vulnerable to the same attacks as the rest of the enterprise (Hentea, 2008). The term cyber-physical attacks is used for cyber-attacks on critical infrastructures that can have an adverse physical impact (Loukas, 2015).

The Department of Homeland Security's Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) fiscal 2015 report noted ICS cyber incidents increase 20% (i.e. from 245 to 295). Between 2014 and 2015 the ICS-CERT reported cyber incidents for manufacturing increased from 69 to 97 (49% increase) and for water distribution from 14 to 25 (79% increase) (DHS ICS-CERT, 2014, 2015). An example of critical infrastructure control systems' vulnerability took place on December 23, 2014 when over 220,000 Ukrainian customers lost power for over five hours due to a cyber-attack. The cyber-attack began months earlier with phishing emails that included BlackEnergy 3 malware infected Microsoft Word and Excel files and ended with the energy utilities' industrial control systems used to shut down 30 substations, and disablement of systems restoration uninterruptable power supplies, and corruption of various utility systems with KillDisk malware (Zetter, 2016a, 2016b).

Cyber-physical attacks threats continue. On March 15, 2018 the Department of Homeland Security issued Alert TA-18-074A. The Alert noted that since at least March 2016, U.S. critical infrastructure sectors (to include energy, nuclear, water, aviation, and critical manufacturing) have been targeted by Russian government cyber threat actors (Carcano, 2018; U.S. Computer Emergency Readiness Team, 2018)

2.5 Tools for Increasing Critical Infrastructure Cybersecurity

Given the increasing attacks on critical infrastructure information technology and industrial control systems, this section looks at tools available to enable a critical infrastructure organization to increase its cybersecurity.

During 2003 President Bush released "The National Strategy to Secure Cyberspace". Included among several short and long term goals was for the Office of

Science and Technology Policy to develop and update an annual federal research and development agenda to address several priorities to include intrusion detection, internet infrastructure security, applications security, communications security (including SCADA systems encryption and authentication) (The White House, 2003). During 2013 President Obama issued Executive Order 13636 which directed the development of a framework to reduce cyber risks to critical infrastructure ("The Cybersecurity Framework") (The White House, 2013a).

As a result of the 2003 National Strategy to Secure Cyberspace, and the 2013 Executive Order 13636, significant academic research and coordinated Federal government and private sector efforts resulted in standards and assessment tools to empower a critical infrastructure organization to increase its cyber security.

2.5.1 Standards

As directed by Executive Order 13636 through the Secretary of Commerce, the National Institute of Standards and Technology (NIST) led the development of the Cybersecurity Framework (CSF). After ten months of collaborative discussion with more than 3,000 security professionals NIST published on February 2014 the "Framework for Improving Critical Infrastructure Cybersecurity" (NIST, 2014; PwC, 2014). Assembled from standards, guidelines, and practices that have worked in industry, the CSF provides organization and structure to multiple approaches to cyber security.

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of an organization's risk management process. The CSF consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers (NIST, 2014).

1. The Framework Core is a set of cybersecurity activities, outcomes, and information references common to all critical infrastructure sectors, and provides detailed guidance for developing specific organizational Profiles.
2. The Framework Profiles help organizations align their cybersecurity activities with their business requirements, risk tolerance, and resources.

3. The Framework Tiers provide a mechanism for organizations to view cybersecurity risk and the processes to manage that risk. Tiers can range from Partial (Tier 1) to Adaptive (Tier 4) with the higher tier numbers requiring a greater investment of resources and effort, but in turn providing greater cybersecurity.

As shown in Figure 2.3 the Framework Core is organized in a listing of Functions, and Categories.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 2.3 Framework Core Functions and Categories (NIST, 2014)

Each Function Category in turn has Subcategories, and Information References (i.e. standards) as shown in Figure 2.4.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Figure 2.4 Framework Category's Subcategories and References (NIST, 2014)

To summarize the Cybersecurity Framework provides an organization a repeatable process leveraging best practices (i.e. standards, guidelines, and processes) to increase and maintain its cybersecurity based on its business requirements, risk tolerances, and resources.

2.5.2 Assessment Tools

There are several public and private assessment tools to enable organizations to understand their cybersecurity status that are based on the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2018a). An example is the Industrial Control Systems – Cyber Emergency Response Team's (ICS-CERT) Cyber Security Evaluation Tool (CSET). CSET provides a systematic, disciplined, and repeatable approach for an organization to evaluate its security posture. It is a free downloadable software tool for Microsoft Windows personal computers that guides users through a step by step process to evaluate industrial control systems and information

technology security practices. Users can select from a portfolio of recognized industry and government standards and recommendations what is appropriate for their operations.

CSET helps users assess their operational and informational systems cybersecurity practices through a series of detailed questions about their systems components and architectures as well as operational policies and procedures based on accepted cybersecurity standards. Once the questionnaires are completed, CSET produces charts and reports showing areas of strength and weakness, and a prioritized recommendations list for increasing cybersecurity (DHS ICS-CERT, 2016).

ICS-CERT recommends using CSET with a cross functional team as follows:

1. Select Standards - Users can select one or more government and industry recognized cybersecurity standards. CSET will generate questions specific to those requirements.
2. Determine Assurance Level - The security assurance level (SAL) is determined by responses to potential consequences of an effective cyber-attack on an ICS organization, facility, system, or subsystem. The SAL can be selected or calculated and provides a recommended level of cybersecurity rigor necessary to protect against worst-case events.
3. Create the Diagram – Users can create a diagram from scratch or import an existing MS Visio diagram into CSET's graphical user interface. Users can then define cybersecurity zones, critical components, and network communication paths.
4. Answer the Questions – CSET then generates questions using the network topology, selected security standards, and SAL as its basis. To assist with the questions CSET provides help through supplemental text, and additional resources.
5. Review Analysis and Reports – CSET provides an Analysis dashboard with interactive graphs and tables that present assessment in both summary and detailed form. Professionally designed reports can be printed to facilitate coordination, communications, and synchronization with management and staff members.

2.5.3 Vendors' Solutions

Industrial control systems vendors like GE, Modicon, and Rockwell Automation have noted the increased infrastructure cybersecurity requirements and are building greater cybersecurity capabilities into their respective products (General Electric, 2012; Rockwell Automation, 2013; Schneider Electric, 2015). An example of this is the collaborative effort between Rockwell Automation, CISCO, and Panduit to educate their shared customers and offer new products with integrated cybersecurity features. To address new and legacy industrial control systems without cybersecurity capabilities, companies like Schweitzer Engineering Laboratories provide cybersecurity components and engineering solutions (Bartman & Carson, 2015). Critical infrastructure organizations can now begin to find industrial controls cybersecurity options that didn't exist only a few years ago.

To summarize, we have covered the fundamentals of critical infrastructure industrial control systems and how they were initially designed for speed, and reliability on isolated networks and without cybersecurity in mind. Subsequently industrial control systems and their operational networks have increasingly become more cyber vulnerable as they have been connected to the internet for remote access and integrated with enterprise networks to improve business efficiency and productivity. We also learned that as a result of increased governmental and private collaborative hard work, critical infrastructure organizations now have available robust tools to assess and increase their cyber security posture, based on their business requirements, risk tolerances, and resources. In addition, industrial control systems vendors and their partners are offering industrial control components with cybersecurity options that simply didn't exist just a few years ago. However, despite the availability of cybersecurity tools, and vendor solutions over the past several years there has not been a decline in critical infrastructure cyber-attacks over the same period. The following sections of this chapter address several challenges improving cybersecurity.

2.6 Challenges to Improving Cybersecurity

This section provides an overview to cybersecurity resource considerations that challenge improving cybersecurity, to include cost-benefit analysis. The methods described in this section will be challenged with the difficulty of precisely quantifying the risks and consequential costs of cybersecurity threats that are constantly changing.

2.6.1 Identifying Cybersecurity Resource Considerations

Determining cybersecurity costs for one's personal notebook may be as simple as the cost of purchasing and maintaining up to date anti-virus software and a virtual private network service. Determining the costs for increasing the cybersecurity of a state's water critical infrastructure sector is more complex given differences in various utility companies' systems, personnel, organizations, funding resources, federal and state regulatory compliance, etc. One approach to ensuring the various elements of potential cybersecurity costs are examined and identified is to leverage the U.S. Department of Defense's DOTMLPF-P methodology.

DOTMLPF-P is an acronym for Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy. When preparing to execute a significant, complex, and difficult goal or objective the Department of Defense (DoD) uses DOTMLPF-P to analyze all the elements required for success and identify capability gaps that need to be addressed (Defense Acquistion University, 2016).

Figure 2.5 below translates the "definitional intent" of DoD's DOTMLPF-P Elements to Cybersecurity Functional Areas to make them relevant for capability gaps analysis of cybersecurity for critical infrastructures.

Each of the Cybersecurity Functional Areas; Procedures, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Regulations will require resources. However, the resources required for each Functional Area may be covered by different entities. For example, for the Procedures Cybersecurity – Functional Area, which includes the NIST Cybersecurity Framework and the Cybersecurity Evaluation Tool (CSET) have been developed and are maintained by the Federal Government.

DOTMLPF-P - Elements			Cybersecurity - Functional Areas	
Element	**Definition**		**Functional Area**	**Definition**
Doctrine	how missions are conducted	→	Procedures	processes, guidelines, standards
Organization	combination of organizations, i.e. Departments & Agencies	→	Organization	organization of the public & private voluntary coalition
Training	tactical preparation	→	Training	degrees and/or certification
Materiel	available equipment, testers, spares, "off the shelf" items	→	Materiel	Industrial controls systems hardware and software
Leadership	leader's preparations at all levels to execute mission	→	Leadership	preparation of senior private & government executives
Personnel	availability of qualified personnel	→	Personnel	availability of qualified personnel
Facilities	real estate, industrial facilities	→	Facilities	real estate, industrial facilities
Policy	department and agency policies that affect the above	→	Regulations	federal and state regulations and codes that affect the above

Figure 2.5 DOTMLPF-P Elements to Functional Areas Translation

Consequently, this means that neither a state government nor its critical infrastructure organizations may need to resource any cybersecurity frameworks guidance and evaluation research and publications. However, for the Materiel Functional Area, each organization will need to fund their own hardware, software, networking, and integration required to cybersecure its unique information technology and/or industrial controls systems. By examining each Cybersecurity – Functional Area for gaps, the cybersecurity resources required to address those gaps can be identified and reduce the risk that a cost is overlooked.

2.6.2 Cybersecurity Costs -Benefit Analysis

For other than the vendors of cybersecurity products or services, cybersecurity is a consideration or "necessary evil" required to successfully pursue organizational goals and objectives. Consequently, resources required for cybersecurity are likely to come at the expense of other investments and operational requirements that may impact primary goals and objectives.

Cost-benefit analysis is an economic principal that can be used to efficiently manage cybersecurity resources (Loeb & Gordon, 2006). Cost-benefit analysis compares

the cost of an activity versus its benefit to help decide how to efficiently allocate scarce resources among competing requirements. From a cybersecurity context, a cost-benefit analysis enables you to compare the costs of various cybersecurity options and determine their benefits. If the benefits exceed the costs of the additional cybersecurity costs, then it is worthwhile to make the cybersecurity investments. However, if the cybersecurity investment costs exceed the benefits, then those investments should be curtailed. In other words, additional cybersecurity doesn't always result in an organization being better off.

Once the costs of cybersecurity activities are captured by reviewing the Cybersecurity – Functional Areas, the next step is to determine the benefits of those cybersecurity activities. The benefits associated with cybersecurity activities are derived from the cost savings (i.e. cost avoidance) that results from preventing cybersecurity breaches (Loeb & Gordon, 2006). With both the cost and benefits of cybersecurity activities, a cost-benefit analysis can be conducted to determine how much to invest in cybersecurity.

An example of the monetary consequences of one type of cybersecurity breach can be made using research data published by the Ponemon Institute in its 2018 report. Ponemon reported that the per capital cost of an energy company records data breach was $167 (Ponemon Institute LLC, 2018). That means if an electric utility company suffers a records breach for its 59,880 customers the total monetary remediation cost would be approximately $10,000,00 ($167/per capita x 59,880 customers = $9,999,960). Ponemon Institute's per capita costs include legal, forensic analysis, lost customers, opportunity, and other costs.

Given a potential data breach, calculating the right cybersecurity investments requires variables affecting potential cost savings and include (1) the potential losses associated with the information breaches, (2) the probability that a particular breach will, occur, and (3) the productivity associated with specific investments, which can be used to determine the reduction in the probability of potential losses (Loeb & Gordon, 2006).

Table 2.1 depicts a table showing the interaction between all these variables for four different levels of organizational investment in cybersecurity technologies, training, procedures etc. which offer different levels of risk reduction.

The table illustrates that if nothing is done (Option A) a $10,000,000 potential loss without cybersecurity and an occurrence probability of .75 has an expected loss of $7,500,000. If the organization invests $650,000 (Option B) in cybersecurity and reduces the occurrence probability to .50 the expected loss is 5,000,000 and the incremental net benefit (i.e. cost avoidance) is $1,850,000. The table then shows how additional cybersecurity investments of $1,300,000 (Option C), $1,950,000 (Option D), and $2,600,000 (Option E) result in incremental net benefits of $350,000, $50,000, and -$250,000 respectively.

Table 2.1 How Much to Invest in Cybersecurity (Loeb & Gordon, 2006)

Option	(1)	(2)	(3)	(4) = (2) x (3)	(5) = (1) + (4)	(6)	(7)	(8) = (6) - (7)
	Investment Level	Total Potential Loss from Cybersecurity Breach without Investment	Probability of Loss at Each Investment Level	Expected Loss at Each Investment Level	Total Expected Cybersecurity Costs = Investment Costs + Expected Loss from Breaches	Incremental Benefits from Increase in Investment Level (reduction in expected loss, i.e. reduction in column 4 values with additional investment)	Incremental Level of Investment (increase in investment levels, i.e. increasein column 1 values)	Incremental Net Benefit of Increase in Investment Level
A	$ -	$ 10,000,000	0.75	$10,000,000	$ 7,500,000	Not Applicable	Not Applicable	Not Applicable
B	$ 650,000	$ 10,000,000	0.50	$ 5,000,000	$ 5,650,000	$ 2,500,000	$ 650,000	$ 1,850,000
C	$ 1,300,000	$ 10,000,000	0.40	$ 4,000,000	$ 5,300,000	$ 1,000,000	$ 650,000	$ 350,000
D	$ 1,950,000	$ 10,000,000	0.33	$ 3,300,000	$ 5,250,000	$ 700,000	$ 650,000	$ 50,000
E	$ 2,600,000	$ 10,000,000	0.29	$ 2,900,000	$ 5,500,000	$ 400,000	$ 650,000	$ (250,000)

Given that even though the investment of $2,600,000 reduced occurrence probability to 0.29, the cost-benefit analysis revealed the return for the additional investment dollars became a negative $250,000, indicating the organization's best security investment level is $1,950,000 (Option D).

2.6.3 Additional Issues that May Affect Improving Cybersecurity

After confirming a positive cost benefit analysis to investing in cybersecurity activities identified by reviewing the Cybersecurity – Functional Areas there may be additional factors that may still make cybersecurity improvements difficult. Below are a few examples of additional issues that need to be resolved before cybersecurity improvements can be made.

2.6.3.1 Regulated Rate Pricing

Indiana as do many other states has the Indiana Utility Regulatory Commission which is an administrative agency that hears evidence in cases filed before it and makes decisions based on evidence presented in those cases. The Commission is required by state statute to make decisions in the public interest to ensure the utilities provide safe and reliable service at just and reasonable rates ("Indiana Utility Regulatory Commission," 2017).

Consumers (i.e. voters) depend and expect predictable (and economical) services from regulated monopolies such as power, water, communications, transportation, etc. Consequently, regulated critical infrastructure organizations cannot suddenly and unilaterally raise their rates to cover cybersecurity capital and operational expenses.

2.6.3.2 Critical Infrastructures Organization Sizes

Research of Purdue Business Library's OneSource Global Business 2016 database revealed for Indiana water supply companies (NAIC 22131) the average annual revenue per employee is $250,000 and the number of employees for each company listed. Figure 8 depicts the number of companies by number of employees and shows that most of Indiana water utility companies have five or less employees (188 of the 325 (57.8%)).

The resource implication of small company size on cybersecurity is the difficulty a small company will have in funding an additional employee to install, operate, and maintain the company's cybersecurity in addition to capital expense of new cybersecurity technology. A locally or state regulated water utility company can't simply and quickly increase the number of customers to increase its revenues by at least $250,000 to cover the annual labor and burden of an extra employee for cybersecurity.

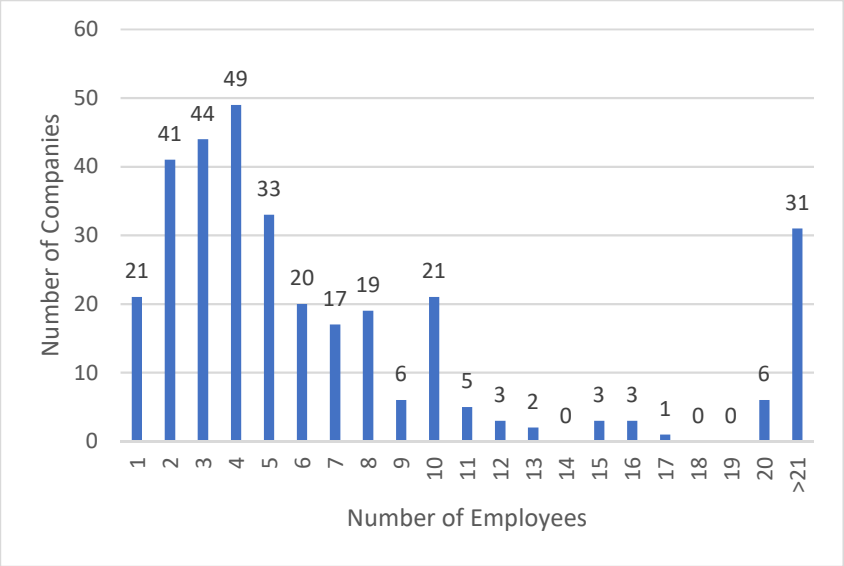

Figure 2.6 Number of IN Water Utility Companies Based on Number of Employees

Whereas a large or very large Indiana water utility company has the "economic flexibility" to fund a cybersecurity headcount, the same does not apply to over half of Indiana's water utility companies due to their small size.

Figure 2.7 shows how small companies are further economically constrained when addressing cybersecurity costs given their higher average annual operating costs per capita versus those of larger companies.

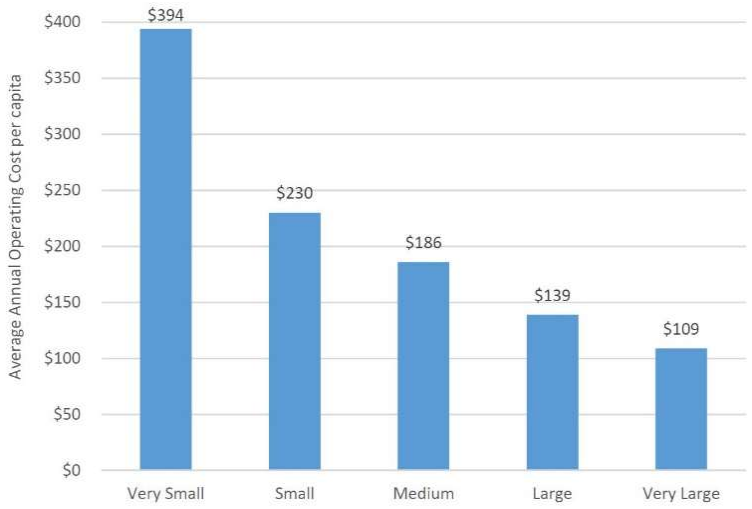

Figure 2.7 Annual per Capita Operating Cost (Indiana Finance Authority, 2016)

Issues affecting cybersecurity improvements like those listed above may be systemic and require support from industry or government. These improvements (changes) and are not easily resolved individually by critical infrastructure organizations.

2.7 Summary

This chapter provided an overview of cybersecurity as it pertains to critical infrastructure sectors. The purpose of this dissertation is to solely focus on assessing the cybersecurity of those sector organizations in order to reduce their vulnerabilities to cyber-attacks. We learned how several critical infrastructures depend on industrial control systems, on which a cyber-attack can have physical consequences to include loss of electricity or water, and explosions in hazardous environments. This chapter discusses how the availability of cybersecurity standards, assessment tools, and vendor solutions have not significantly decreased reported cyber-physical attacks on critical infrastructure organizations. The results of this review of literature provided confirmation of the importance and relevance of the questions posed in this study. The challenges to improving cybersecurity include:

1. Identifying all the relevant resource considerations
2. Conducting a cost-benefits analysis to determine the best cybersecurity investments
3. and Quickly identifying and resolving any additional issues that may hamper cybersecurity improvements

Given the challenges listed above a cybersecurity assessment process based on current and emerging threats is necessary in order to focus limited resources and time to accelerate cybersecurity improvements. This chapter sets the foundation and the basis to address the significance and need for this research.

CHAPTER 3. METHODS AND PROCEDURES

3.1 Overview

The methodology and procedures in this study were developed to answer the research questions with academic rigor, integrity and required anonymity and support the Indiana Cybersecurity Strategy Plan. By combining this study with the State of Indiana's cybersecurity efforts opened the opportunity for this study to collect and analyze real world / real time data while simultaneously assisting with the State's cybersecurity. This chapter will begin with reviewing the research questions and describing how they relate to the Indiana Cybersecurity Strategy Plan. It is followed with background to the State of Indiana's Cybersecurity Scorecard initiative, the Scorecard's design process (study design), participants, recruitment procedures, data collection procedure, and analysis. The following chapter will discuss the scorecard response demographics, and analysis and results from the Scorecard's answers data.

3.2 Research Questions

The questions central to this research were:

1. Is it possible to develop a cybersecurity scorecard based on identified vulnerabilities and threats, that provides effective actionable information for public and private organizations in the State of Indiana regardless of size or cyber expertise?
2. How well will the cybersecurity scorecard quantitatively identify actionable information that may be unique to organizations in different critical infrastructure sectors and/or size categories?

The above questions are aligned with the Indiana Cybersecurity Strategic Plan's Cybersecurity Scorecard's deliverable description that it "will not only provide key indicators to users, but also can be used to directly quantify the effectiveness of the Council" (Governor Eric J. Holcomb, 2018). Answers to both research questions could provide "key indicators to users". If the Scorecard is used to collect data before and after

the Council implements cybersecurity initiatives, then it could "quantify the effectiveness of the Council" if the Scorecard effectively measures key indicators.

3.3 The State of Indiana's Cybersecurity Scorecard Initiative Background

During April 2016, in an effort to build a robust cybersecurity team, Indiana's then Governor Michael Pence directed the formation of the Indiana Executive Council on Cybersecurity (IECC) (Pence, 2016). On January 2017 his successor Governor Eric Holcomb's Executive Order continued the IECC (Holcomb, 2017). The IECC is composed of:

1. Senior State Leadership (to include the Executive Director of Department of Homeland Security, Attorney General, Chief Information Officer, Adjutant General of the Indiana National Guard, and Superintendent of Indiana State Police (or their designees)),
2. the Chief Information Officers from Purdue and Indiana Universities,
3. Senior Executives from critical infrastructure and key resource sectors (to include Information Technology, Communications, Energy Sector, Healthcare and Public Health, Defense Industrial Base, Financial Services, and Water/Wastewater), and
4. Federal cybersecurity experts stationed in Indianapolis, Indiana (to include the Federal Bureau of Investigation, Department of Homeland Security, and Secret Service).

In August of 2017 Governor Holcomb further demonstrated Indiana's commitment to cybersecurity by signing along with thirty eight State governors the National Governors Association's (NGA) "A Compact to Improve State Cybersecurity" (National Governors Association, 2017a). In September 2017, the Indiana Executive Council on Cybersecurity (IECC) completed version 4 of its Charter, which identifies its roles and responsibilities (Indiana Executive Council on Cybersecurity, 2017). As per its Charter, the IECC is responsible for establishing and maintaining a strategic framework that defines high-level cybersecurity goals for the State which in turn generated cybersecurity initiatives during January of 2018.

One of those initiatives, led by the State of Indiana's Director of Cybersecurity Programs, Chetrice Mosley, included developing and implementing a Cybersecurity Scorecard, in partnership with Purdue University.

At a minimum, Mosely (C. Mosley, personal communication, February 14, 2018) directed:

1. The Cybersecurity Scorecard identify the different cybersecurity vulnerabilities in organizations by size (large, medium, and small) and IECC Charter critical infrastructure and key resource sectors (Indiana Executive Council on Cybersecurity, 2017).
2. The Scorecard encourage voluntarily completion by owners or managers of organizations of all sizes who may not have in-house cybersecurity expertise (e.g. town government, non-profit, garage, legal, dry cleaning, medical, construction, etc.).
3. The Scorecard be non-threatening, understandable and educational to encourage organizations to self-assess and learn so that they may self-correct areas they identified on their own (C. Mosley, personal communications, March 7, 2018).
4. The Scorecard provide a quantifiable measure that can be used to compare Scorecard results before and after cybersecurity initiatives, resources, and deliverables are provided to measure the effectiveness of the same.

In addition to the above Scorecard requirements the following assumptions were made:

1. The Cybersecurity Scorecard is intended to accelerate effective and efficient actions that outpace the growth of cyber threats.
2. Over time the Scorecard will need to be updated predicated on successes, subsequent objectives, and evolving threats.
3. Indiana organizations have matured beyond using the Cybersecurity Scorecard as an awareness tool (given the frequent news regarding evolving cybersecurity threats and their consequences).

4. The Cybersecurity Scorecard will provide actionable information while accessing the needs for deliverables and reports from government, industry, academia individually or collectively
5. Participation will be voluntary, and data collection will likely require statistical sampling since participation may not be 100%.

Given the desired voluntary participation in the Scorecard's data collection, the risk of wasting participants' resources was identified (e.g. time, money, and/or political will). To preclude that risk the Scorecard design requires data collection that mitigates:

1. Vague findings that fail to identify necessary improvements
2. Only identifying non-feasible improvements (due to constrained time, money, and/or political will)
3. Insufficient who, what, where, when, why, or how details that preclude the focus for using limited resources and/or making rapid improvements

3.4 Designing the Cybersecurity Scorecard (Study Design)

With the above requirements in mind the State of Indiana and Purdue University reviewed public, proprietary, state, and national scorecards to identify best practices that may be used for Indiana's Cybersecurity Scorecard. The publicly available scorecards that were reviewed included:

1. Baldridge Cybersecurity Excellence Builder (Baldridge, 2017)
2. The State of Michigan's - CySAFE IT Security Assessment Tool (State of Michigan, 2018)
3. The Department of Homeland Security's in Partnership with the Multi-State Information Sharing and Analysis Center's - The Nationwide Cyber Security Review (Department of Homeland Security and Multi-State Information Sharing and Analysis Center, 2018)
4. Center for Information Assurance and Security – Community Cyber Security Maturity Model (The Center for Infrastructure Assurance and Security, n.d.)
5. The National Institute of Standards' – Cyber Security Framework (National Institute of Standards and Technology, 2014)

6. The National Cybersecurity and Communication Integration Center's - Cyber Security Evaluation Tool (National Cybersecurity and Communications Integration Center, 2017)

Scorecards were reviewed for government, industry, and/or commercial cybersecurity standards already required of Indiana organizations. Voluntary completion of Indiana's Cybersecurity Scorecard questions is easier if an organization has already answered similar questions in compliance with their legal and/or industry requirements. If the Scorecard asks standards-based questions a small organization will need to abide by in the future, it could save that organization compliance time later.

Indiana's cybersecurity requires a collaborative effort and basing the Scorecard on an applicable standard that crosses public and private sectors enables a common language for identifying vulnerabilities and cybersecurity solutions. A standard that is referenced in several of the reviewed scorecards is the National Institute of Standards and Technology – Cybersecurity Framework (NIST-CSF) (National Institute of Standards and Technology, 2014). In the reviewed scorecards listed above the NIST-CSF is referenced in all except for the Community Cyber Security Maturity Model (The Center for Infrastructure Assurance and Security, n.d.).

Basing the Indiana Cybersecurity Scorecard on the NIST-CSF standard could benefit Indiana's State, Local, Tribal, and Territorial governments should they participate in the Nationwide Cyber Security Review (NCSR) (Department of Homeland Security and Multi-State Information Sharing and Analysis Center, 2018). Sponsored by the U.S. Department of Homeland Security, the NCSR is based on the NIST-CSF and is a no-cost, voluntary, anonymous, self-assessment designed to measure gaps and capabilities in governments' cybersecurity programs (Department of Homeland Security and Multi-State Information Sharing and Analysis Center, 2018). The NCSR evaluates cybersecurity nationally and provides metrics and actionable information to individual State, Local, Tribal, and Territorial government respondents.

As a policy framework of computer and network guidance the NIST-CSF enables public and private organizations to assess and improve their ability to prevent, detect, and respond to cyber-attacks. Basing the State's Cybersecurity Scorecard on the NIST-CSF offers the following potential advantages:

1. Large private and public organizations would find the Scorecard questions in line with compliance requirements they have likely met (i.e. avoiding unnecessary or duplicative work).
2. The NIST-CSF provides a framework from which the unique regulatory or industry standards can be aligned. In other words, the unique requirements specific to various sectors such as Energy utilities or Healthcare organizations have been identified for each using the NIST-CSF framework. This supports closer to apples to apples cybersecurity comparison between diverse public and private critical infrastructure and key resource sectors.
3. Scorecard questions that align with the NIST-CSF could help the State of Indiana and its Local, Tribal, and Territorial governments answer questions for the Nationwide Cyber Security Review.

The NIST-CSF's Framework Core component was selected to develop the Scorecard's questions. The Core was selected because it is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure and key resource sectors. By organizing industry standards, guidelines, and practices, the Core facilitates organizational communications of cybersecurity activities from the executive suite to the implementation/operations level (National Institute of Standards and Technology, 2018b).

The Framework Core begins with five continuous and concurrent Functions (Identify, Protect, Detect, Respond, and Recover) that provide a high-level and strategic view of an organization's lifecycle management of its cybersecurity risk. It provides additional details for the Functions from 22 underlying Categories. The Categories in turn are supported with additional details with 98 underlying Subcategories. The Subcategories describe discrete outcomes which are matched with Informative References (i.e. industry standards, guidelines, and practices), as shown in Figure 3.1 (National Institute of Standards and Technology, 2018b).

Figure 3.1 NIST-CSF Functions, Categories, Subcategories, and Info References

The organization and level of detail provided by the Framework Core's Subcategories, shown above, enables organizations to thoroughly assess their cybersecurity status and to decide how to correct identified vulnerabilities (based on their cybersecurity risk requirements and resources). If each Subcategory is addressed as a Cybersecurity Scorecard question, it would result in 98 questions. Large and some medium size organizations are likely to be staffed with personnel who have the expertise and time to address most if not all the Categories and Subcategories. Several of the questions based on Categories and Subcategories would be challenging if not impossible to answer for a principal or operator of a small garage, nursery, law office, or other non-information technology organizations.

Making the Cybersecurity Scorecard useable for small Indiana businesses is important for the following reasons:

1. Verizon reports that for 2017 58% of the cyber breaches victims were small businesses (Verizon, 2018).
2. Ponemon and Keeper Security reported September of 2017 that cyber-attacks on small and medium businesses increased over twelve months, from 55 percent to 61 percent (for the six hundred businesses Ponemon reviewed) (Keeper Security, 2017).

3. Ponemon and Accenture reported 2017 that the average cybercrime cost for a small company per enterprise seat is $1,726 versus $436 for a large company. In other words, the cybercrime cost per seat for a small company is nearly four times the cost for a large company (Accenture and Ponemon Institute, 2017).
4. The Council of Economic Advisors reported February 2018 to the Executive Office of the President that "A firm's security flaw can put its customers, suppliers, and corporate partners at risk…..sophisticated adversaries often target small and medium-sized companies as means to gain foothold on the interconnected business ecosystems as a supply chain attack" (The Council of Economic Advisers, 2018). In other words, cyber breached small companies can become gateways for successfully breaching their larger customers as in the case of Home Depot (The Council of Economic Advisers, 2018).
5. For the State of Indiana, the U.S. Census reported of the 146,078 establishments recorded in the 2016 Census, 83.3% of them had 19 or less employees (U.S. Census, 2016).

If primarily large, some medium, and few if any small organizations complete the Cybersecurity Scorecard its usefulness for increasing Indiana's cybersecurity will be limited. To enable small Indiana organizations to complete the Scorecard, the Director of Indiana's Cybersecurity Program directed the Scorecard have no more than twenty questions written with minimal jargon so that it may be understandable to a non-technical office manager (C. Mosley, personal communications, March 7, 2018).

Given the number of NIST-CSF Categories and Subcategories that could be used for Scorecard questions the first step was to select the most important outcomes. To screen for the most relevant Categories and Subcategories , the "areas of focus" from the Department of Defense's Cybersecurity Implementation Plan were selected (Department of Defense, 2016b). The Department of Defense (DoD) developed its Cybersecurity Implementation Plan based on cyber incidents, inspections, and investigations that revealed many incidents uncovered were possible in part due to simple mistakes. Given small organizations are more likely to make simple mistakes due to their cyber expertise, the DoD's "areas of focus" were used to customize the Framework Core for the

Scorecard questions. In fact, the NIST Cybersecurity Framework was designed to be flexible so that its use can be customized given organizations have unique risks, and different threats, vulnerabilities, risk tolerances, and budgets (National Institute of Standards and Technology, 2018b). The DoD's four "areas of focus" are:

1. Ensuring Strong Authentication – How are users logging into systems and devices?
2. Hardening Devices – Are devices and systems properly configured and updated?
3. Reducing the Attack Surface – How many devices need to be connected to the internet and are they properly configured?
4. Detecting and Responding to Potential Intrusions – Can cyber defenders do their jobs?

The above "areas of focus" were used to customize the number of Categories from 22 to 16 and Subcategories from 98 to 51 and aligned as shown in Figure 3.2. Please note NIST-CSF version 1.0 (National Institute of Standards and Technology, 2014) was used to develop the Cybersecurity Scorecard since the Scorecard was developed before version 1.1 was released April 16, 2018 (please note the NIST-CSF version 1.1 does not invalidate existing version 1.0 uses (National Institute of Standards and Technology, 2018b)).

FOCUS AREA	FUNCTION	CATERGORY	SUBCATEGORY
2. Hardening Devices	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1 Physical devices and systems within the organization are inventoried
			ID.AM-2 Software platforms and applications within the organization are inventoried
			ID.AM-3 Organizational communication and data flows are mapped
			ID.AM-4 External information systems are catalogued
			ID.AM-5 Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
			ID.AM-6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
1. Ensuring Strong Authentication (Identities and credentials are managed for authorized devices and users)		Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated
			ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
			ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
			ID.BE-4: Dependencies and critical functions for delivery of critical services are established
			ID.BE-5: Resilience requirements to support delivery of critical services are established
1. Ensuring Strong Authentication (Identities and credentials are managed for authorized devices and users)		Governance (ID.GV): The policies, procedures, andprocesses to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established
			ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
			ID.GV-4: Governance and risk management processes address cybersecurity risks
2. Hardening Devices		Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-3: Threats, both internal and external, are identified and documented
			ID.RA-4: Potential business impacts and likelihoods are identified
			ID.RA-6: Risk responses are identified and prioritized
1. Ensuring Strong Authentication (Identities and credentials are managed for authorized devices and users)	PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-2: Physical access to assets is managed and protected
			PR.AC-3: Remote access is managed
1. Ensuring Strong Authentication (Identities and credentials are managed for authorized devices and users)		Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained
			PR.AT-2: Privileged users understand roles & responsibilities
			PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
			PR.AT-4: Senior executives understand roles & responsibilities
1. Ensuring Strong Authentication		Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected
			PR.DS-2: Data-in-transit is protected
2. Hardening Devices			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
1. Ensuring Strong			PR.DS-4: Adequate capacity to ensure availability is maintained
1. Ensuring Strong Authentication (Identities and credentials are managed for authorized devices and users)		Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained
			PR.IP-3: Configuration change control processes are in place
			PR.IP-4: Backups of information are conducted, maintained, and tested periodically
			PR.IP-6: Data is destroyed according to policy
			PR.IP-7: Protection processes are continuously improved
			PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
			PR.IP-10: Response and recovery plans are tested
			PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
2. Hardening Devices		Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least privilege
			PR.PT-4: Communications and control networks are protected
3. Reducing the Attack Surface		Disconnect all unused outward (to the public internet devices (PR-TBD)	TBD
4. Detecting and responding to potential intrusions	DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events
			DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
			DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
			DE.CM-8: Vulnerability scans are performed
4. Detecting and responding to potential intrusions		Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
			DE.DP-2: Detection activities comply with all applicable requirements
4. Detecting and responding to potential intrusions	RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event
4. Detecting and responding to potential intrusions		Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained
			RS.MI-2: Incidents are mitigated
			RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
4. Detecting and responding to potential intrusions	RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event
4. Detecting and responding to potential intrusions		Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed
			RC.CO-2: Reputation after an event is repaired
			RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Figure 3.2 "Areas of Focus" Customized Categories and Subcategories

(Department of Defense, 2016a; National Institute of Standards and Technology, 2014)

Sixteen Categories were selected for the focus of the Scorecard's questions given the objective was to keep the total number of questions to 20 or less. The text for the selected Categories was checked for readability and as written scored at the college graduate readability level with the Flesch-Kincaid Grade Level (20.9), The SMOG Index (17.5), Automated Readability Index (21.5), and Linsear Write Formula (20.9). To make the questions more understandable the IECC's Strategic Resources Working Group composed of members with and without cybersecurity expertise reviewed the selected Categories and rewrote them into plain English questions. The rewritten plain English questions improved readability into the range of eleventh grade to college level with the Flesch-Kincaid Grade Level (13.2 / college), The SMOG Index (11.2 / eleventh grade), Automated Readability Index: (12 / twelfth grade), and Linsear Write Formula (11.4 / eleventh grade). To increase readability a few of the Category focus areas resulted in more than one Scorecard question resulting in the Scorecard having a total of twenty-two non-demographic questions. The Strategic Resources Working Group added seven demographic questions to bring the final total of Scorecard questions to twenty-nine. The first two demographics questions are to identify the organization submitting the Scorecard.

Two Likert Scales were used to obtain quantifiable data from the Scorecard and make the questions non-threatening and answers applicable to different sectors and organization sizes. For 15 questions a respondent could answer: I don't know (0), Strongly Disagree (1), Disagree (3), Neither Agree or Disagree (3), Agree (4), or Strongly Agree (5). For seven questions a respondent could answer: I don't know (0), Never (1), Almost Never (2), Occasionally/Sometimes (3), Almost Every Time (4), or Every Time (5). The values adjacent to each answer option were used to score each question and with a total of 22 scoreable questions a Scorecard could have a total score ranging from 0 to 110. The Scorecard questions with answer types are shown in Table 3.1.

Table 3.1 Final Indiana Cybersecurity Scorecard Questions

Scorecard Question	Answer Type
Name of Organization	Text
Your E-Mail Address	Text
How many employees are there in your organization (full and part time)?	Numerical
How many employees have information technology related duties?	Numerical
How many employees have cybersecurity related duties?	Numerical
Does your organization outsource your information technology needs?	Yes / No
Does your organization outsource your cybersecurity needs?	Yes / No
Our organization values cybersecurity	Disagree / Agree
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	Disagree / Agree
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	Disagree / Agree
Our business/organization model influences the way we approach cybersecurity.	Disagree / Agree
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	Disagree / Agree
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	Disagree / Agree
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	Disagree / Agree
We have system checks in place to make sure that our data is not compromised or changed.	Disagree / Agree
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	Disagree / Agree
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	Disagree / Agree
Our cybersecurity technology (such as antivirus, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	Disagree / Agree
We have a process in place to address a cyberthreat.	Disagree / Agree
We have a cyber emergency response plan in place to address a cyberattack on our organization	Disagree / Agree
If we were impacted by a cyber emergency (e.g. ransomware), we know how our organization would recover our data and/or operational systems.	Disagree / Agree
After a cyberthreat or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	Disagree / Agree
Our executive leadership receives periodic status, physical, and cybersecurity updates	Never / Every Time
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	Never / Every Time
We provide our employees cybersecurity awareness and/or training.	Never / Every Time
We protect our business and customer information so that only the employees that need to see it, can.	Never / Every Time
We would know if our cybersecurity technology detected a cyberthreat.	Never / Every Time
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	Never / Every Time
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	Never / Every Time

3.5 Participants and Recruitment Process

Before asking thousands of Indiana organizations to use the Cybersecurity Scorecard, a Pilot group was selected to test the Scorecard. The Pilot test consists of three stages:

1. Use the Cybersecurity Scorecard to identify cybersecurity shortfalls on which to focus resources and deliverables for cybersecurity improvements. This was conducted from May through September of 2018.
2. Provide focused cybersecurity resources and deliverables (i.e. tools) and time to implement them. Those tools may differ based an organization's sector and size. For example, a large water utility may need to cyber harden its industrial controls while a small retailer may need to increase its point of sale cybersecurity training. This will take place during the fall of 2018 and through early spring of 2019.
3. Use the 2018 Cybersecurity Scorecards to measure changes in cybersecurity. This is currently scheduled for March of 2019.

For the Pilot each of the ten IECC Charter critical infrastructure and key resource sector Committees were each asked to nominate one large, two medium, and three small volunteer organizations to use the Scorecard (Indiana Executive Council on Cybersecurity, 2017). The number and size of volunteer organizations requested for the Pilot was based on an estimate of how may volunteers would be available and statistically significant sample sizes were not a consideration. The Committees nominated volunteer organizations from the Communications, Defense Industrial Base, Elections, Energy, Finance, Government Services, Healthcare, K-12 Education, Local Government, and Water and Wastewater sectors. In addition, six Business organizations were added to the Pilot for an initial total of 66 participants (to total 11 large, 22 medium, and 33 small organizations).

Anonymity was designed into the data collection and analysis and reporting process to increase candor in the results and address concerns Pilot members may have about revealing their cybersecurity weaknesses to hackers and litigation risks.

3.6 Data Collection Procedure

The Scorecard was initially delivered to the Pilot group of 66 organizations via email using Qualtrics, an academic online data collection and analysis tool. The invite to complete the Scorecard was from Indiana's Director of Cybersecurity Programs, and participants could choose to complete the Scorecard online or download the Scorecard as a PDF file, print it, complete it, and either post or email it. Approximately 28 organizations responded to the Qualtrics email and completed the Scorecard online. Chetrice Mosley also personally emailed the Scorecard as a fillable PDF file attachment to participants that may not have received the Qualtrics emails because of spam filters on their respective mail servers.

Participation of respondents from the different sectors varied and additional organizations were invited to submit their Scorecard input. In total 60 Scorecards were received via email, postal mail and online submission. Postal and emailed Scorecard responses were entered in Qualtrics and aggregated with the online submissions for data analysis.

3.7 Data Analysis

All Scorecard entries were checked for completeness and clarity regardless how they were collected in Qualtrics (online submission, email, or postal mail). Complete and unambiguous Scorecards data was afterwards exported from Qualtrics to Excel to prepare it for statistical analysis using IBM SPSS. Preparation in Excel included anonymizing participants and sector identifications, converting descriptive answers to numerical values (e.g. "Yes" to "1" and "No" to "2"), converting Likert Scale choices numerical values (e.g. "Strong Agree (5)" to "5") and eliminating Qualtrics survey tracking fields (e.g. "Start Date", "End Date", "Status", etc.). Once the data was coded in Excel it was imported into IBM SPSS statistical analysis software.

SPSS was used for data analysis to obtain descriptive statistics that included the mean, medium, standard deviation, range (i.e. maximum and minimum) and sample size. SPSS was also used for analysis of variables (ANOVA) and scatterplot analysis to identify relationships among variables and determine if multicollinearity assumptions

were violated. SPSS ANOVA results were used in SAS for Windows to conduct the power procedure to determine the sample sizes required to ensure statistical significance in the results.

The data collection and analysis process designed and used for the first stage of the Scorecard Pilot was designed to scale from data collection and analysis for less than one hundred participants to thousands when the Pilot is successfully completed. Purdue University's Qualtrics capability can support surveying over five thousand participants a day.

3.8 Validity and Reliability

Peer review and auditing was used to check for validity and reliability of this study. The logic, factual soundness, and cogency of the study was reviewed with the researcher's chair, committee member, the statistics department consultant and Indiana's Director of Cybersecurity Programs. Reliability checking was done by verifying the survey data by more than one individual and documenting and critically reviewing data coding procedures.

CHAPTER 4. ANALYSIS AND RESULTS

4.1 Overview

The analysis and results that follows is from the data collected from 56 useable Scorecards, with each Scorecard providing data from three numerical scale questions and 24 questions with numerical ordinal questions. The analysis will begin with a review of the Scorecard's Pilot group's demographics followed by analysis of the scorecard data that supports the research questions:

1. Is it possible to develop a cybersecurity scorecard based on identified vulnerabilities and threats, that provides effective actionable information for public and private organizations in the State of Indiana regardless of size or cyber expertise?
2. How well will the cybersecurity scorecard quantitatively identify actionable information that may be unique to organizations in different critical infrastructure sectors and/or size categories?

Based on data available from the scorecards the following questions were analyzed in order to address the research questions.

1. How do questions rank by scores?
2. Does ranking of questions ranked by size differ?
3. Does ranking of questions by sector differ?
4. How do organization sizes rank by scores?
5. How do sectors rank by scores?
6. Does Information Technology Outsourcing Affect Scores?
7. Does Cybersecurity Outsourcing Affect Scores?

4.2 Survey Demographics

Sixty Scorecards (90% of the Pilot Group participation objective of 66) were received June through September of 2018. After following the data coding procedure in Appendix D data from 56 useable Scorecards remained. Two scorecards were incomplete and two were duplicative as shown in Step 2. (2) and 2. (12) in Table 4.1.

The names of all participating organizations were anonymized with randomly generated response identification numbers by Qualtrics online survey application.

Table 4.1 Scorecard Data Coding Log

Step 2.(2)	Hid R_1JVp61eHQzMw3ry given "FALSE" Status (i.e. didn't complete Scorecard)
	Hid R_21vKHuilJlWLHSX Given Sum of Scores doesn't Equal TTL
Step 2.(11)	For R_Z91RXekL9d79V4Z changed ~50,000 Eployees to 50,000 and ~9,000 IT to 9,000
	For R_OMZt8QkSPxTOTkJ changed all IT to 42 and 3-March Cybersecurity to 3 (Qualtrics Input was
	For R_3j6Sp4uETMMtJH7 changed over 200,000 employees to 200000, over 50,000 IT to 50000 and over 1,000 Cybersecurity to 1000
	For R_3POjmlSHFuzJNad changed 60,000+ employees to 60,000, "unknown" IT to "blank", and "Many" Cybersecurity to "blank"
	For R_2VaPYu5klLWv4BZ changed approx. 5,000 employees to 5000, approx. 140 IT to 140, approx. 6 (dedicated) to 6
	For R_301v7TYCDwwVTaR changed 22 FT employees to 22, 2 but very limited IT to 2,
	For R_28YVQIAryYBUnJD changed ~500 employees to 500, ~20 IT to 20, and ~7 to 7
	For R_2xXoahSNqWi1kmq changed 1000+ employees to 1000
	For R_3D2cQc2MOayGDxp changed ~1300 employees to 1300
	For R_VVke1pl8zwwXhOp changed 475+ employees to 475
	For R_2Yol5PEt1H4j1Gs changed 425+ employees to 425
Step 2.(12)	Hid R_3hrNlOw7L0UiTq4 given R_3fBpdrkkllCVfdJ input for Same Organization
	Counted R_1go7sCIJvQGzKlB for Elections and not for Local Government (he was listed twice in Audit Log)

The 56 scorecards provided data from eleven critical infrastructure and key resource sectors organizations. Five sectors represented public organizations in Government Services (State), K-12 Education, Local Government, Election, and Water and Wastewater. Six sectors represented private organizations in Business, Communications, Energy, Finance, and Healthcare. Table 4.2 lists all the sectors with the public sectors in green cells and private sectors in blue cells.

Table 4.2 Public and Private Sectors

Indiana Critical Infrastructure and Key Resource Sectors	
Business	Government Services
Communications	Healthcare
Defense Industry	K-12 Education
Election	Local Government
Energy	Water and Wastewater
Finance	

Of the 11 sectors only two submitted the requested scorecards with one for a large organization, two for medium organizations and three for small organizations in their respective sector as requested. Seven sectors submitted less than the requested six scorecards and two sectors submitted more than six scorecards. Given the Pilot Group

participation objective of 66 organization (six for each sector) the 56 useable scorecards represented an 85% participation with public organization scorecards providing an 87% participation (of 30 organizations) and private organizations providing 83% participation (of 36 organizations) as depicted in Table 4.3 (the percentages are for administratively measuring participation and not used for statistical analysis). The participating sector names were anonymized with randomly assigning letters

Table 4.3 Useable Scorecard Participation

		Anonymized Critical Infrastructure or Key Resource Sectors												
		A	B	C	D	E	F	G	H	I	J	K	Total	% Participation
Size	Large	1	1	1	1	1	1	1	1		1		9	82%
	Medium	2	1		1	2	2	1	1	1	1	1	13	59%
	Small	4	3	8	3	3	3	3	3	2	1	1	34	103%
	Total	7	5	9	5	6	6	5	5	3	3	2	56	85%
% Participation		117%	83%	150%	83%	100%	100%	83%	83%	50%	50%	33%	85%	

Total % of Public Participation	87%
Total % of Private Participation	83%

4.3 Analysis Questions

The analysis questions listed below use the numerical values from the scorecard's Likert scale questions as the dependent variable called score(s). Higher scores represent a greater confidence or frequency in conducting specified cybersecurity measures. Low scores represent lack of knowledge, lower confidence or infrequent conduct of cybersecurity measures. The independent variables will be questions, organization size category, sector, insourcing vs outsourcing information technology or cybersecurity support, number of total employees, number of information technology employees, and number of cybersecurity employees.

4.3.1 How Do Questions Rank by Scores?

By ranking the questions by the mean scores from all fifty-six participating organizations in ascending order (low scores to high scores) it is possible to identify the NIST CSF Category areas where the Pilot Group collectively indicated the lowest knowledge, confidence, or frequency in conducting the specified cybersecurity measures. The Scorecard questions with the lowest mean scores are the question which received the

lowest confidence score from all 56 respondents and indicates the most vulnerable NIST-CSF Category.

For example, in Table 4.4 the Scorecard questions with the lowest mean score of 3.09 (on a scale of 1 to 5 with 5 being the best score) is “22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software”.

The letters “(DE.CM)” at the beginning of the question identify that it is related to the NIST-CSF “Detection” Function and its “Security Continuous Monitoring” Category (from Figure 2.3). Identifying the NIST-CSF’s Function and Category for low scoring question further identifies the desired outcomes and informative references required to address the low scores (i.e. cybersecurity vulnerability areas).

Identifying the questions with the lowest scores identifies on which cybersecurity vulnerabilities to focus limited resources to rectify first.

Table 4.4 Ranking of Questions by Scores

	Mean	Median	Std. Deviation
22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	3.09	3.00	1.599
13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our organization.	3.57	4.00	1.360
18. (PR.AT) We provide our employees cybersecurity awareness and/or training.	3.68	3.50	1.266
12. (RS.MI) We have a process in place to address a cyberthreat.	3.79	4.00	1.275
21. (PR.AC & PR.PT) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	3.80	5.00	1.721
16. Our executive leadership receives periodic status, physical, and cybersecurity updates.	3.82	4.00	1.011
4. (ID.BE) Our business/organization model influences the way we approach cybersecurity.	3.89	4.00	1.021
10. (PR.IP) As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	3.93	4.00	1.024
20. (DE.DP) We would know if our cybersecurity technology detected a cyberthreat.	3.96	4.00	0.990
5. (ID.GV) When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	3.98	4.00	0.944
17. (ID.AM) We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	3.98	4.00	1.120
8. (PR.DS) We have system checks in place to make sure that our data is not compromised or changed.	4.00	4.00	1.062
3. (ID.AM) We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	4.09	4.00	1.100
14. (RC.RP) If we were impacted by a cyber emergency (e.g. ransomware), we know how our organization would recover our data and/or operational systems.	4.09	4.00	1.180
9. (PR.AC) Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	4.16	4.00	0.968
7. (PR.IP) We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	4.29	4.00	0.803
6. (ID.RA) We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	4.45	4.00	0.570
11. (PR.PT) Our cybersecurity technology (such as antivirus, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	4.45	5.00	0.711
15. (RC.CO) After a cyberthreat or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	4.46	5.00	0.687
19. (PR.AC) We protect our business and customer information so that only the employees that need to see it, can.	4.48	5.00	0.687
1. Our Organization values cybersecurity	4.50	5.00	0.688
2. (ID.AM) We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	4.57	5.00	0.657

4.3.2 Does Ranking of Questions by Size Differ?

This question is for determining if the low scoring questions (i.e. cybersecurity vulnerabilities) for large, medium, and small organizations are the same or differ. This is important because increasing cybersecurity for a large organization of thousands of personnel is more complex than for a small organization of less than twenty.

Of the five lowest scoring questions for each organizational size categories Table 4.5 identifies only two questions (questions 22 and 13) that large, medium, and small organizations have ranked as their lowest five scoring questions. Large and small organizations both list question 21 in the lowest five questions, and medium and small organizations list question 12. Only in the case of question 22 for large and small organizations does it rank identically (i.e. the lowest scoring of all questions). Based on Table 4.5 the difference in lowest scoring questions between large, medium, and small organizations indicates their vulnerabilities are not identical

Table 4.5 Ranking of Questions by Size

Low to High Question Scores Rankings for Large Size Organizations	Mean	Low to High Question Scores Rankings for Medium Size Organizations	Mean	Low to High Question Scores Rankings for Small Size Organizations	Mean
22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	2.56	4. (ID.BE) Our business/organization model influences the way we approach cybersecurity.	3.69	22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	2.94
21. (PR.AC & PR.PT) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	3.44	22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	3.85	13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our organization.	3.35
17. (ID.AM) We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	3.78	10. (PR.IP) As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	3.92	18. (PR.AT) We provide our employees cybersecurity awareness and/or training.	3.35
3. (ID.AM) We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	3.89	13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our organization.	3.92	16. Our executive leadership receives periodic status, physical, and cybersecurity updates.	3.59
13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our	3.89	5. (ID.GV) When we make a decision in our organization that involves legal, operational, technological, or	4.08	12. (RS.MI) We have a process in place to address a cyberthreat.	3.62
20. (DE.DP) We would know if our cybersecurity technology detected a cyberthreat.	3.89	12. (RS.MI) We have a process in place to address a cyberthreat.	4.08	21. (PR.AC & PR.PT) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	3.68

4.3.3 Does Ranking of Questions by Sectors Differ?

This question is for determining if the low scoring questions (i.e. cybersecurity vulnerabilities) for the 11 different sectors are the same or differ. This is important because increasing cybersecurity for a Finance organization with its office automation is different than for an Energy organization with its industrial control systems.

Given there are eleven different sectors for purposes of this question only sectors A and E will be used as a comparison example. Of the six lowest ranking questions in sectors A and E only two questions (22 and 21) were identified for both sectors, and they differ in ranking between sectors. Between sectors A and E four of their six (66%) of their lowest ranking questions differ (A's non-matching questions are 13, 18, 8, and 10, and E's questions are 7, 3, 5, and 17). Based on Table 4.6 the difference in lowest scoring questions between sectors A and E indicates their vulnerabilities are not identical.

Table 4.6 Ranking of Questions by Sector

Low to High Question Scores Rankings for Sector A	Mean	Low to High Question Scores Rankings for Sector E	Mean
22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	2.71	7. (PR.IP) We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	3.57
13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our organization.	2.86	3. (ID.AM) We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	3.57
18. (PR.AT) We provide our employees cybersecurity awareness and/or training.	2.86	5. (ID.GV) When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	3.71
21. (PR.AC & PR.PT) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	3.00	17. (ID.AM) We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	4.00
8. (PR.DS) We have system checks in place to make sure that our data is not compromised or changed.	3.14	22. (DE.CM) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.	2.71
10. (PR.IP) As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	3.29	21. (PR.AC & PR.PT) Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	3.00

4.3.4 How do Organization Sizes Rank by Scores?

Given Verizon reports that for 2017 reported 58% of the cyber breach victims were small businesses (Verizon, 2018) this question is for determining if large, medium, and small organizations differ in their cybersecurity scores (i.e. vulnerability). Table 4.7 ranks small organizations with the lowest mean score of 86.35 out of a possible 110 and medium organizations with the highest mean score of 94.85 for a difference of 8.5 points.

Table 4.7 Organization Size Groups Scores Statistical Descriptives

	N	Mean	Std. Deviation	Minimum	Maximum
Small	34	86.35	13.946	60	109
Large	9	90.78	15.746	67	110
Medium	13	94.85	12.429	72	110
Total	56	89.04	14.120	60	110

To determine if the difference is statistically significant (i.e. are they similar with slightly different scores or statistically different) an Analysis of Variables (ANOVA) was calculated as shown on Table 4.8. The p value of 0.169 (listed as Sig. on Table 4.8) is greater than 0.05 preventing us from rejecting the hypothesis that the organizational size category groups are not the same.

Table 4.8 Organization Size Groups Scores ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	710.916	2	355.458	1.837	0.169
Within Groups	10255.013	53	193.491		
Total	10965.929	55			

To determine the minimum samples size required to have a p value of 0.05 with a power of 0.80 a power procedure was calculated. As depicted in Table 4.9 a minimum sample size of 53 for each group would be required to determine statistically significant means for the different size group

Table 4.9 Organization Size Groups Power Procedure

The SAS System

The POWER Procedure
Overall F Test for One-Way ANOVA

Fixed Scenario Elements	
Method	Exact
Group Means	90.78 94.85 86.35
Standard Deviation	13.91
Nominal Power	0.8
Alpha	0.05

Computed N per Group	
Actual Power	N per Group
0.803	53

4.3.5 How do Sectors Rank by Score?

This question is for determining if sectors differ in their cybersecurity scores (i.e. vulnerability). Table 4.10 ranks the sector A with the lowest mean score of 80.43 out of a possible 110 and sector E with the highest mean score of 104.83 for a difference of 24.4 points.

To determine if the difference is statistically significant (i.e. are they similar with slightly different scores or statistically different) an Analysis of Variables (ANOVA) was calculated as shown on Table 4.11. The p value of 0.159 (listed as Sig. on Table 4.11) is greater than 0.05 preventing us from rejecting the hypothesis that the organizational size category groups are not the same

To determine the minimum samples size required to have a p value of 0.05 with a power of 0.80 a power procedure was calculated. As depicted in Table 4.12 a minimum sample size of 6 for each group would be required to determine statistically significant means for the different size groups

Table 4.10 Sectors Groups Scores Statistical Descriptives

Anonymized Sector	N	Mean	Std. Deviation	Minimum	Maximum
A	7	80.43	14.129	63	101
K	2	80.50	3.536	78	83
H	5	82.40	14.241	67	103
D	5	85.80	13.065	75	106
J	3	86.00	23.896	60	107
I	3	87.00	16.523	70	103
C	9	87.11	14.819	63	109
B	5	91.80	15.595	72	105
G	5	92.60	10.922	79	107
F	6	94.50	9.354	78	104
E	6	104.83	5.307	97	110
Total	56	89.04	14.120	60	110

Table 4.11 Sector Groups Scores ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2788.492	10	278.849	1.534	0.159
Within Groups	8177.437	45	181.721		
Total	10965.929	55			

Table 4.12 Sector Groups Power Procedure

The SAS System

The POWER Procedure
Overall F Test for One-Way ANOVA

Fixed Scenario Elements	
Method	Exact
Group Means	80.43 91.8 87.11 98.8 104.83 94.5 92.6 82.4 87 86 80.5
Standard Deviation	13.48
Nominal Power	0.8
Alpha	0.05

Computed N per Group	
Actual Power	N per Group
0.818	6

4.3.6 Does Information Technology Outsourcing Affect Scores?

This question is for determining if outsourcing information technology support affects cybersecurity scores (i.e. vulnerability). Table 4.13 depicts that organizations that outsource information technology have a mean score of 86.04 and organizations that insource have a score of 91.83 for a difference of 5.79.

Table 4.13 Information Technology Outsourcing Statistic Descriptives

	N	Mean	Std. Deviation	Minimum	Maximum
Yes	27	86.04	13.093	60	107
No	29	91.83	14.687	63	110
Total	56	89.04	14.120	60	110

To determine if the difference is statistically significant (i.e. are they similar with slightly different scores or statistically different) an Analysis of Variables (ANOVA) was calculated as shown on Table 4.14. The p value of 0.126 (listed as Sig. on Table 4.14) is greater than 0.05 preventing us from rejecting the hypothesis that organizational size category groups are not the same

Table 4.14 Information Technology Outsourcing ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	468.828	1	468.828	2.412	0.126
Within Groups	10497.101	54	194.391		
Total	10965.929	55			

To determine the minimum samples size required to have a p value of 0.05 with a power of 0.80 a power procedure was calculated. As depicted in Table 4.15 a minimum sample size of 92 for each group would be required to determine statistically significant means for the different size groups

Table 4.15 Information Technology Outsourcing Power Procedure

The SAS System

The POWER Procedure
Overall F Test for One-Way ANOVA

Fixed Scenario Elements	
Method	Exact
Group Means	86.04 91.83
Standard Deviation	13.942
Nominal Power	0.8
Alpha	0.05

Computed N per Group	
Actual Power	N per Group
0.800	92

4.3.7 Does Cybersecurity Outsourcing Affect Scores?

This question is for determining if outsourcing cybersecurity support affects cybersecurity scores (i.e. vulnerability). Table 4.16 depicts that organizations that outsource cybersecurity have a mean score of 85.41 and organizations that insource have a score of 92.41 for a difference of 7.

Table 4.16 Cybersecurity Outsourcing Statistic Descriptives

	N	Mean	Std. Deviation	Minimum	Maximum
Yes	27	85.41	13.337	60	107
No	29	92.41	14.211	67	110
Total	56	89.04	14.120	60	110

To determine if the difference is statistically significant (i.e. are they similar with slightly different scores or statistically different) an Analysis of Variables (ANOVA) was calculated as shown on Table 4.17. The p value of 0.063 (listed as Sig. on Table 4.17) is greater than 0.05 preventing us from rejecting the hypothesis that organizational size category groups are not the same

Table 4.17 Cybersecurity Outsourcing ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	686.376	1	686.376	3.606	0.063
Within Groups	10279.553	54	190.362		
Total	10965.929	55			

To determine the minimum samples size required to have a p value of 0.05 with a power of 0.80 a power procedure was calculated. As depicted in Table 4.18 a minimum sample size of 62 for each group would be required to determine statistically significant means for the different size groups

Table 4.18 Cybersecurity Outsourcing Power Procedure

The SAS System

The POWER Procedure
Overall F Test for One-Way ANOVA

Fixed Scenario Elements	
Method	Exact
Group Means	85.41 92.41
Standard Deviation	13.797
Nominal Power	0.8
Alpha	0.05

Computed N per Group	
Actual Power	N per Group
0.800	62

4.4 Summary

This section began with the demographics of the fifty-six organizations that provided useable scorecard data. Based on data available from the scorecards the following questions were analyzed in order to address the research questions.

1. How do questions rank by scores?
2. Does ranking of questions ranked by size differ?
3. Does ranking of questions by sector differ?
4. How do organization sizes rank by scores?
5. How do sectors rank by scores?
6. Does Information Technology Outsourcing Affect Scores?
7. Does Cybersecurity Outsourcing Affect Scores?

By ranking the questions scores in ascending order, the lowest score questions identified areas for cybersecurity growth in the Pilot Group. Ranking the question scores by organization size categories and sectors revealed cybersecurity vulnerability across sizes and sectors are not identical.

Mean scores between size groups, and sectors groups, were found to differ but with p factors greater than 0.05 were therefore not statistically significant. Mean scores for organizations outsourcing vs insourcing information technology or cybersecurity were found to differ, but with p factors greater than 0.05 were therefore not statistically significant. Power procedures were calculated for all the mean score comparisons and minimum samples sizes were determined for obtaining p factors of 0.05 with a power of 0.80.

Analyzing the data available from the participating scorecards provided descriptive statistics and revealed samples sizes will need to be increased to obtain statistical significance in the results.

CHAPTER 5. DISCUSSION AND RECOMMEDATIONS

This dissertation began with a background of how cyber-attacks and breaches appear to keep increasing and the threats this poses to the critical infrastructure sectors that we depend on for our national economic security, public health, and safety. Several critical infrastructure sectors include industrial control systems that need to be protected from cyber-attacks since they control our physical world to include our electricity, water supply and transportation systems. Targeted cyber-attacks and data breaches are not exclusive to the private sector. Verizon reported the Public Administration sector was recorded with the greatest total cyber incidents and second most breaches compared to the other twenty private sectors (Verizon, 2018). Given the internet connectivity between governments and private organizations, cybersecurity needs to be a collaborative effort in order to mitigate and reduce cyber breaches.

The Governor of Indiana along with thirty-eight State governors signed an agreement to improve their State's cybersecurity. To do so Indiana's Governor Holcomb charged the Indian Executive Council on Cybersecurity to plan and execute several initiatives to include a Cybersecurity Scorecard. The Cybersecurity Scorecard is an initiative that will be used to measure the effectiveness of other Indiana cybersecurity initiatives.

This dissertation discussed how the Cybersecurity Scorecard was designed to not only benchmark and measure progress of initiatives but encourage organizations to assess, educate, and initiate cybersecurity improvements themselves. Since most organizations in the State of Indiana are small the Scorecard was designed to be useable by small organizations and non-technical experts.

To determine if the Cybersecurity Scorecard would be able to benchmark and measure the State of Indiana's cybersecurity volunteer organizations were asked to be part of a Pilot Group to use the Scorecard. The data collected from the scorecards was used to answer this dissertation's research questions.

5.1 Research Question 1

Is it possible to develop a cybersecurity scorecard based on identified vulnerabilities and threats, that provides effective actionable information for public and private organizations in the State of Indiana regardless of size or cyber expertise?

5.2 Answer to Research Question 1

For purposes of Research Question 1 "effective actionable information" is defined as identifying through the NIST cybersecurity framework desired outcomes and related informative references. If an organization lacks the funding, time, and/or expertise resources the actionable information provided by the scorecard will not be "effective". Given the qualified definition of "effective" the following data demonstrates the first research question is affirmative for the following reasons:

1. The Pilot Groups useable scorecard participation rate was 85%.
2. The participation of small organizations (the most cybersecurity vulnerable) was over 100%
3. The questions in the Scorecard are aligned with NIST-CSF Functions and Categories enabling an organization participating in the Scorecard to find for their questions with low scores informative references.

5.3 Research Question 2

How well will the cybersecurity scorecard quantitatively identify actionable information that may be unique to organizations in different critical infrastructure sectors and/or size categories?

5.4 Answer to Research Question 2

The cybersecurity scorecard design provided quantitative data that could be analyzed to identify actionable information. Analysis of the scorecard data revealed the following:

1. The most vulnerable cybersecurity areas. Ranking the questions by their mean scores in ascending order revealed the cybersecurity areas where organizations were least cybersecurity confident.
2. The most vulnerable cybersecurity areas based on organization size category. Ranking the questions by their mean score in ascending order for each size category revealed that organizations size categories differed as to where their organizations were least cybersecurity confident.
3. The most vulnerable cybersecurity areas based on sectors. Ranking the questions by their mean scores in ascending order for each sector revealed that sectors differed as to where their organizations were least cybersecurity confident
4. Cybersecurity based on organization size categories. Ranking the organization size categories by their mean scores in ascending order revealed that small organizations had the lowest cybersecurity confidence, large organizations had greater confidence and medium organizations had the greatest cybersecurity confidence.
5. Cybersecurity based on organization sectors. Ranking the sectors by their mean score in ascending order revealed that sector A had the lowest cybersecurity confidence, followed by the sectors K, H, D, J, I, C, B, G, F in order of increasing confidence with sector E having the greatest cybersecurity confidence
6. Cybersecurity based on information technology support outsourcing. Organizations that outsourced their information technology support were less cybersecurity confident.
7. [j1] Cybersecurity based on cybersecurity support outsourcing. Organizations that outsourced their cybersecurity support were less cybersecurity confident.

5.5 Significance of This Study

A search for "cybersecurity scorecards" on either Google's or Microsoft's Bing search engines revealed at a minimum over two hundred thousand results. The results revealed cybersecurity scorecards available from academic, private, as well as federal and state government organizations (Baldridge, 2017; National Cybersecurity and Communications Integration Center, 2017; National Institute of Standards and Technology,

2018a; State of Michigan, 2018). With the time available, various scorecards were reviewed and analyzed against the criteria provided by Indiana's Director of Cybersecurity Programs. The most important criteria was making the scorecard that small non-technical Indiana business and local governments could use given that over eighty percent of Indiana establishments have nineteen or less employees (U.S. Census, 2016). The scorecards reviewed found them thorough in technical detail and if not for a specific public and private sector very comprehensive. The more comprehensive scorecards (or self-assessment of evaluation instruments) tended to be larger documents which make them more challenging if not impossible for busy non-technical small organizations to use and benefit from.

Comprehensive cybersecurity evaluation tools can provide organizations effective actionable information but given the expertise and time those tools require makes them expensive to use. Whereas large organizations and many medium size organizations may have the expertise and time to utilize comprehensive cybersecurity evaluation tools, small organizations are resource disadvantaged. Indiana's focus on making a scorecard useable for over eighty percent of its public and private organizations (i.e. small) was made even more imperative given Verizon's report that during 2017 fifty eight percent of small organizations were victims of cyber breaches (Verizon, 2018).

The Indiana Cybersecurity Scorecard stands out from other cybersecurity self-assessment, evaluation, or scorecard tools based on the following:

1. Small organizations can use the scorecard as evidenced during the Pilot by their robust participation in completing the scorecard.
    a. Small organizations had the best participation rate. 84% (28 versus goal of 33) small organizations if you limit each sector to only three small organizations (the goal). If you count the total number of 34 small organizations that completed the scorecard the participation was 104% (34 versus goal of 33).
    b. 59% (13 versus goal of 22) medium organizations completed the scorecard.
    c. 82% (8 versus goal of 9) large organizations completed the scorecard.
2. The scorecard was designed to provide relevant actionable information to all participating organizations regardless of size and sector based on the following:

a. The scorecard is based on the NIST Cybersecurity Framework (NIST-CSF) which is based on best practices and references established industry and government standards. If large and medium organizations have already worked with the NIST-CSF, the scorecard question should be like question they have already answered. For medium and small organizations their answers to the scorecard questions may save them time when they begin to use the NIST-CSF.
b. The scorecard's relevance was increased by focusing on the Department of Defense's Cybersecurity Discipline Implementation Plan lines of effort based on recent and emerging cyber incident trends (Department of Defense, 2016b).
c. The scorecards questions can be used to identify the NIST Cybersecurity Framework's Core Categories which provide desirable outcomes and informative references. This enables scorecard users to use their low scoring questions to find relevant information for improving their cybersecurity.
d. The scorecard provides quantifiable information that can be used by organizations to measures their individual progress and by the State of Indiana to identify cybersecurity vulnerability trends specific to organization size categories and/or sectors.

The Cybersecurity Scorecard in this dissertation is now recorded as a deliverable in the Indiana Cybersecurity Strategic Plan (Governor Eric J. Holcomb, 2018). The data and analysis from this dissertation are being used to provide resources and deliverables to the members of the Pilot Group. During the middle of 2019 the Pilot Group will be asked to complete the Scorecard after its members have used the provided cybersecurity resources and deliverables. Predicated on comparison analysis of the 2018 and 2019 Scorecards, the Scorecard and possibly the cybersecurity improvement resources and deliverables will be modified, and the Scorecard is planned for production use by thousands of Indiana organizations to measure and improve the State of Indiana's cybersecurity.

5.6 Implications for Indiana Critical Infrastructure Cybersecurity

As noted in Chapter 4 two questions related to smart devices received the lowest and fifth lowest mean scores. The non-technical term "smart devices" was chosen to represent the internet of things devices (IoT) and industrial control systems (ICS). The low scores for smart devices indicated that the critical infrastructure organizations that submitted scorecards found their smart devices or IoT and ICS more vulnerable than at least seventeen other cybersecurity areas queried in the scorecard. This is significant for the following reasons:

1. As noted in Chapter 2 several critical infrastructure sectors depend on industrial control systems.
2. For the first half of 2018 Kaspersky reported that the percentage of ICS computers attacked increased from 37.5% to 41.21% compared to the last half of 2107 (Kaspersky Lab, 2018).
3. Symantec reported that ICS related vulnerabilities increased 39% and attacks against Internet of Things devices (IoT) increased 600% during 2017 (Symantec Corporation, 2018).

Quantifiably identifying a major cybersecurity vulnerability area that simultaneously is currently subject to escalating cyber threats and attacks is necessary but not enough to accelerate cybersecurity improvements in Indiana. As noted in Chapter 2 the challenges to improving cybersecurity include:

1. Identifying all the relevant resource considerations
2. Conducting a cost-benefits analysis to determine the best cybersecurity investments
3. and Quickly identifying and resolving any additional issues that may hamper cybersecurity improvements

To improve Indiana's cybersecurity for smart devices or any of its identified vulnerable areas will require a "process of devising a system, component, or process to meet desired needs. it is a decision-making process (often iterative), in which the basic sciences, mathematics, and the engineering sciences are applied to convert resources optimally to meet these stated needs" (ABET (Accreditation Board for Engineering and Technology), 2017) In other words, an engineering problem solving model (Cowan et

al., 1982; Sharp, 1991) will be required to improve cybersecurity and may be summarized as

1. Recognizing a need
2. Defining the problem, the objectives and the constraints
3. Collecting information and data
4. Generating alternative solutions
5. Evaluating the consequences of different solutions
6. Deciding and specifying

The scorecard designed in this dissertation can support an engineering problem solving model since it will allow benchmarking and measuring progress as iterative engineering solutions are implemented.

When the scorecard is used in production to collect data from thousands of Indiana private and public organizations there may be enough sample data to apply regression analysis to identify relationships between training, plans, and processes with the cybersecurity areas that score the lowest for sectors and organization size categories. In combination with emerging cyber threats and attacks data the scorecard may support moving from reactive to proactive cybersecurity by applying grounded theory. Grounded theory is a focus on generating theories or hypothesis (e.g. for accelerating cybersecurity) from the data versus using the data to prove or disprove a theory specified beforehand. "A grounded theory is one that is inductively derived from the study of the phenomena it represents" (Corbin & Anselm, 1990)

In summary, the critical infrastructure cybersecurity implication of this study includes:

1. For Indiana's public and private organizations to get ahead of critical infrastructure cyber attackers it requires initiatives and a means of tracking progress in the planning and execution those initiatives. The Pilot demonstrated the scorecard is a tool that most participating organizations could use. There are many cybersecurity scorecards to choose from, but the best ones are those that get used and make it easier to identify actionable information for quickly improving cybersecurity.

2. Accelerating the increase in Indiana's cybersecurity will require using the scorecard data with an engineering problem solving approach.
3. As more scorecard data is collected regression analysis and grounded theory may help move Indiana's cybersecurity from reactive to proactive.

5.7 Recommendations for Future Studies

During the process of conducting this study several insights were gained on tasks that could have been done better and future research to increase the State's cybersecurity. The following is a list of those tasks and future research.

1. Compare scorecard results with third party evaluations. If we assume that small non-technical organizations are truthful and competent in scorecard responses, study how well do the scorecards compare with evaluations conducted by experienced cybersecurity experts. Assuming evaluations conducted by experts reflect reality, if the scorecards and evaluations findings are similar it means the scorecard's objective to enable organizations to self-assess was met. If the scorecard's and evaluation's findings are dissimilar it could mean several things to include the scorecard's design does not reflect reality, the organization's self-assessment was unconsciously inaccurately, or the evaluation and scorecard measured the same areas differently. Given that organizational resources may be invested predicated on what the scorecard reveals, getting it right is important.
2. Survey Pilot participants on their opinion of the scorecard's usefulness. The results from the survey may help identify how the scorecard's design and processes can make it easier and more effective for users.
3. Research how federal and state statutes, regulations, and policies for each critical infrastructure sector relate to the mean score for Indiana's sectors. The answers to this research may help government craft more effective policies for sectors that have lower scores.[j2]
4. Investigate how scorecards completed by executives compare with the scorecards completed by their information technology and cybersecurity personnel. The results from this investigation may identify if differences in perceptions should affect organization or government cybersecurity policies and resources.

5. Research emerging cybersecurity threats and attacks to update (i.e. re-calibrate) the scorecard once Pilot study is complete. Cybersecurity threats are constantly changing. During 2019 new cybersecurity threats may emerge that didn't exist when the scorecard was initially designed during the first half of 2018. The scorecard should be updated in coordination with the Indiana – Information Sharing and Analysis Center, Indiana's Intelligence Fusion Center, and Department of Homeland Security.
6. Research training requirements identified by the questions with lowest scores. The second, third, and fourth questions with lowest scores in Table 4.4 (which ranks the questions by their mean scores) have training dependencies. Specifically, they refer to a cyber emergency response plan, periodic cybersecurity awareness training, and a process in place to address a cyberthreat. All three activities require knowledge in tasks that non-information technology and cybersecurity personnel may seldom use. Given that cybersecurity training retention diminishes over time, periodic just in time training (JITT) can be used to ensure an effective response to a cyber emergency or threat (Craig, 2018). After the appropriate just in time training approaches have been identified and applied the scorecard can be used to calibrate training needs based on sectors and organization sizes.

5.8 Summary

The first version of Indiana's Cybersecurity Scorecard in this dissertation supports the following,

1. Increasing cybersecurity awareness. Enabling scorecard users to become more self-aware based on threats, can help private and public organizations focus their cybersecurity improvements and prepare for potential cyber incidents. The scorecard can help organizations focus their limited resources on the best cybersecurity investments and encourage a shift from reactive to proactive cybersecurity.
2. Organizations benchmarking their status to help measure future progress. The scorecard may be used for improving accountability within an organization.

3. Identifying cybersecurity differences between sectors and sizes of organizations in case systemic issues need to be addressed by industry or the government. This in turn enables organizations individually and with external support if required make progress towards accelerating improvements in the State's cybersecurity

It is important to note that a completed scorecard is a snapshot in time and the threats, attacks or an organization's cybersecurity can begin changing as soon as the scorecard is completed. Consequently, an organization should periodically update their scorecard so that it reflects reality and their cybersecurity is suitable for the current and emerging threats. As Indiana's organizations increase their cybersecurity competence, the Scorecard's questions, data collection, and analysis processes have been designed with flexibility to support changes and remain relevant and useful.

APPENDIX A. INDIANA CYBERSECURITY SCORECARD

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Welcome to the State of Indiana's Cybersecurity Scorecard Pilot in partnership with Purdue University!

This Scorecard should take you approximately 10-15 minutes to complete and your inputs will be kept confidential and be reported in aggregate only.

If you would like to mail your Scorecard response instead of submitting it online, complete the following and send it to:

Indiana Executive Council on Cybersecurity
Attn: Chetrice Mosley, Cybersecurity Program Director
100 N. Senate Avenue
N551
Indianapolis, Indiana 46204

After completing the Scorecard, we recommend making a copy to share with your team and management as well as for measuring future progress.

For your reference there is a Glossary of Terms at the end of this Scorecard with definitions for technical terms highlighted in blue lettering. If you have any questions on this Scorecard please give us a call at (765) 494-9728.

Name of Organization

_____

Your E-mail Address

_____

How many employees are there in your organization (full and part time)?

_____

How many employees have information technology related duties?

_____

How many employees have cybersecurity related duties?

_____

Does your organization outsource your information technology needs?

- ○ Yes
- ○ No

Does your organization outsource your cybersecurity needs?

- ○ Yes
- ○ No

Question 1

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.	○	○	○	○	○	○

Question 2

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	○	○	○	○	○	○

Question 3

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	○	○	○	○	○	○

Question 4

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our business/organization model influences the way we approach cybersecurity.	○	○	○	○	○	○

Question 5

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	○	○	○	○	○	○

Question 6

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	○	○	○	○	○	○

Question 7

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	○	○	○	○	○	○

Question 8

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have **system checks** in place to make sure that our data is not compromised or changed.	○	○	○	○	○	○

Question 9

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	○	○	○	○	○	○

Question 10

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	○	○	○	○	○	○

Question 11

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our cybersecurity technology (such as **antivirus**, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	○	○	○	○	○	○

Question 12

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a **cyberthreat**.	○	○	○	○	○	○

Question 13

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a cyber emergency response plan in place to address a **cyberattack** on our organization.	○	○	○	○	○	○

Question 14

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. **ransomware**), we know how our organization would recover our data and/or operational systems.	○	○	○	○	○	○

Question 15

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
After a **cyberthreat** or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	○	○	○	○	○	○

Question 16

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our executive leadership receives periodic status, physical, and cybersecurity updates.	○	○	○	○	○	○

Question 17

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	○	○	○	○	○	○

Question 18

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We provide our employees cybersecurity awareness and/or training.	○	○	○	○	○	○

Question 19

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We protect our business and customer information so that only the employees that need to see it, can.	○	○	○	○	○	○

Question 20

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We would know if our cybersecurity technology detected a **cyberthreat**.	○	○	○	○	○	○

Question 21

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	○	○	○	○	○	○

Question 22

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	○	○	○	○	○	○

To find your score, please add the numbers associated with the responses for questions 1 through 22. For example, selecting "Almost Every Time (4)" has a numberical value of 4.

Your score is _____

Refer to the chart below to determine where you fall on the scale.

Grade	Exemplary	Accomplished	Developing	Beginning	Undeveloped
Minimum with color code	88	66	44	22	0
Range	110-88	87-66	65-44	43-22	21-0
Spread	22	21	21	21	21

Thank you for your participation! You will be contacted in the coming weeks by someone on the Council about the next steps in the Cybersecurity Scorecard Pilot program. If you have any additional questions or feedback, please feel free to contact me.

Chetrice L. Mosley
Cybersecurity Program Director
Indiana Office of Technology
Indiana Department of Homeland Security
Office: (317) 234-5023
Email: MosleyCLM@iot.in.gov

Glossary of Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security
Antivirus- i.e. McAfee, Norton, or Windows Defender
Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing
Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information
Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.

APPENDIX B. SCORECARD ALIGNMENT WITH NIST-CSF CATEGORIES

NIST-CSF Focus Areas Categories	NIST-CSF	Scorecard Questions
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	1	2, 3, 17
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	2	4
Governance (ID.GV): The policies, procedures, andprocesses to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	3	5
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	4	6
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	5	9, 19
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	6	18
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	7	8
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	8	7, 10

	Pilot Indiana Cybersecurity Scorecard (final version)
	Name of Organization
	Your E-mail Address
	How many employees are there in your organization (full and part time)?
	How many employees have technology-related duties?
	How many employees have cybersecurity-related duties?
	Does your organization outsource your technology needs?
Scorecard Questions	Does your organization outsource your cybersecurity needs?
NIST-CSF	1	
1	2	My organization values cybersecurity.
1	3	We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.).
2	4	We have evaluated the operational need of my data and systems to our organization's function (if we are a grocery store we need to set pricing, scan barcodes, weigh produce, etc.)
3	5	Our business/organization model influences the way we approach cybersecurity.
4	6	When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.
8	7	We are familiar with the cybersecurity threat or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.
7	8	We apply physical (doors and locks) controls in the same way I apply computer (ID and password) controls.
5	9	We have system checks in place to make sure that my data is not compromised or changed.
		Our data is available to employees or clients when needed. (if our government or commercial site was unavailable to customers or employees, we would know what to do).

NIST-CSF Focus Areas Categories	***NIST-CSF***	***Scorecard Questions***
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	9 & 10	11
All unused outward (to public internet) devices are disconnected	11	21
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	12	22
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	13	20
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	14	14
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	15	12
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	16	13
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	17	15

NIST-CSF	***Scorecard Questions***	***Pilot Indiana Cybersecurity Scorecard (final version)***
8	10	As with the general policies in our business (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.
9, 10	11	Our cybersecurity technology (such as antivirus, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.
15	12	We have a process in place to address a cyber threat.
16	13	We have a cyber emergency response plan in place to address a cyberattack on our organization.
14	14	If we were impacted by a cyber emergency (e.g. ransomware), we know how our business would recover our data and/or operational systems.
17	15	After a cyber threat or emergency, our organization will make changes to people, process, technology, etc. to improve our security.
	16	Our executive leadership receives periodic status, physical, and cybersecurity updates.
1	17	We keep an inventory of our data (customers, payroll, and/or financial data) and devices that provide access to our data.
6	18	We provide our employees cybersecurity awareness and/or training.
5	19	We protect our business and customers information so that only the employees that need to see it, can.
13	20	We would know if our cybersecurity technology detected a cyberthreat.
11	21	Our 'smart' devices (such as a security cameras, thermostat, HVAC, alarm systems, etc.) are not connected to a publically available internet connection.
12	22	Our 'smart' devices (such as a security cameras, thermostat, HVAC, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software

APPENDIX C. SCORECARD QUALTRICS CONFIGURATION

Standard: Introduction of scorecard (2 Questions)
Block: Demographics (7 Questions)
Standard: Scorecard (16 Questions)
Standard: Block 3 (9 Questions)

EmbeddedData
Score = ${gr://SC_3VQ7UCEdzj2CHxH/Score}

Branch: New Branch
If
If Score Is Greater Than or Equal to 88

EmbeddedData
ScoreResponse = You are ranked as Exemplary

Branch: New Branch
If
If Score Is Greater Than or Equal to 66
And Score Is Less Than or Equal to 87

EmbeddedData
ScoreResponse = You are ranked as Accomplished

Branch: New Branch
If
If Score Is Greater Than or Equal to 44
And Score Is Less Than or Equal to 65

EmbeddedData
ScoreResponse = You are ranked as Developing

Branch: New Branch
If
If Score Is Greater Than or Equal to 22
And Score Is Less Than or Equal to 43

EmbeddedData
ScoreResponse = You are ranked as Beginning

If
If Score Is Greater Than or Equal to 0
And Score Is Less Than or Equal to 21

EmbeddedData
ScoreResponse = You are ranked as Undeveloped

Standard: Block 4 (1 Question)

Page Break

Start of Block: Introduction of scorecard

Q1.1 Welcome to the State of Indiana's Cybersecurity Scorecard Pilot in partnership with Purdue University! This Scorecard should take you approximately 10-15 minutes to complete and your inputs will be kept confidential and be reported in aggregate only. After completing the Scorecard, we recommend downloading a copy of the Scorecard for yourself with your entries to share with your team and management as well measure future progress. The Scorecard allows you to review and update any entries before final submission and if you are interrupted you can return to the link on your email invite and resume working on the Scorecard. Complete the Scorecard prior to June 22, 2018. If you have any questions or problems with this Scorecard, please give us a call at (765) 494-9728.

Q1.2 Audience: office manager, operations manager, information technology manager, business manager, and the like.

End of Block: Introduction of scorecard

Start of Block: Demographics

Q2.1 Name of Organization

_____

Q2.2 Your E-mail Address

_____

Q2.3 How many employees are there in your organization (full and part time)?

_____

Q2.4

How many employees have information technology related duties?

_____

Q2.5 How many employees have cybersecurity related duties?

_____

Q2.6

Does your organization outsource your information technology needs?

- ○ Yes (1)
- ○ No (2)

Q2.7 Does your organization outsource your cybersecurity needs?

- ○ Yes (1)
- ○ No (3)

Page Break

End of Block: Demographics

Start of Block: Scorecard

Q3.1 Question 1

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
Our organization values cybersecurity. (1)	○	○	○	○	○	○

Q3.2 Question 2

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.) (1)	○	○	○	○	○	○

Q3.3 Question 3

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.) (1)	○	○	○	○	○	○

Q3.4 Question 4

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
Our business/organization model influences the way we approach cybersecurity. (1)	○	○	○	○	○	○

Q3.5 Question 5

	I Don’t Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision. (1)	○	○	○	○	○	○

Q3.6 Question 6

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees. (1)	○	○	○	○	○	○

Q3.7 Question 7

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls. (1)	○	○	○	○	○	○

Q3.8 Question 8

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We have **system checks** in place to make sure that our data is not compromised or changed. (1)	○	○	○	○	○	○

Q3.9 Question 9

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do). (1)	○	○	○	○	○	○

Q3.10 Question 10

	I Don’t Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity. (1)	○	○	○	○	○	○

Q3.11 Question 11

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
Our cybersecurity technology (such as **antivirus**, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data. (1)	○	○	○	○	○	○

Q3.12 Question 12

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We have a process in place to address a **cyberthreat**. (1)	○	○	○	○	○	○

Q3.13 Question 13

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
We have a cyber emergency response plan in place to address a **cyberattack** on our organization. (1)	○	○	○	○	○	○

Q3.14 Question 14

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
If we were impacted by a cyber emergency (e.g. **ransomware**), we know how our organization would recover our data and/or operational systems. (1)	○	○	○	○	○	○

Q3.15 Question 15

	I Don't Know (0) (1)	Strongly Disagree (1) (2)	Disagree (2) (3)	Neither Agree or Disagree (3) (4)	Agree (4) (5)	Strongly Agree (5) (6)
After a **cyberthreat** or emergency, our organization will make changes to people, process, technology, etc. to improve our security. (1)	○	○	○	○	○	○

DEF

Technical Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security

Antivirus- i.e. McAfee, Norton, or Windows Defender

Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing

Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information

Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.

Page Break

End of Block: Scorecard

Start of Block: Block 3

Q4.1 Question 16

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
Our executive leadership receives periodic status, physical, and cybersecurity updates. (1)	○	○	○	○	○	○

Q4.2 Question 17

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data. (1)	○	○	○	○	○	○

Q4.3 Question 18

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
We provide our employees cybersecurity awareness and/or training. (1)	○	○	○	○	○	○

Q4.4 Question 19

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
We protect our business and customer information so that only the employees that need to see it, can. (1)	○	○	○	○	○	○

Q4.5 Question 20

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
We would know if our cybersecurity technology detected a **cyberthreat**. (1)	○	○	○	○	○	○

Q4.6 Question 21

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection. (1)	○	○	○	○	○	○

Q4.7 Question 22

	I Don't Know (0) (1)	Never (1) (2)	Almost Never (2) (3)	Occasionally /Sometimes (3) (4)	Almost Every Time (4) (5)	Every Time (5) (6)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software (1)	○	○	○	○	○	○

Q39

Technical Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security

Antivirus- i.e. McAfee, Norton, or Windows Defender

Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing

Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information

Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.

Page Break

Q36 Your score is: ${gr://SC_3VQ7UCEdzj2CHxH/Score}

To review your entries, click on the left arrow. Otherwise, please continue.

End of Block: Block 3

Start of Block: Block 4

Q5.1

${e://Field/ScoreResponse}

Please click on the right arrow to complete the Scorecard.
You can then download a PDF of your results for your records.
Thank you for your participation!

${date://CurrentDate/FL} ${date://CurrentTime/MT} MDT

End of Block: Block 4

APPENDIX D. QUALTRICS EXPORT AND EXCEL DATA CODING

1. Procedure for exporting Scorecard data from Qualtrics
    (1) Open the State of Indiana Cybersecurity Scorecard survey from the list provide from selecting the "Project" menu option in Qualtrics
    (2) Select the "Data & Analysis" menu option
    (3) Select the "Export & Import" menu option
    (4) Select "Export" then "CSV" (Comma Separated Values) download option
    (5) Download data and ease finding the downloaded data with easy to identify file name and folder.
    (6) Open file in Excel and save as an Excel Workbook (*.xlsx) file.
2. The following are the procedures for preparing *.xlsx file for import into SPSS. Two files will be required. The first file will be useful for descriptive statistics using the scores from the Scorecard "as is". The second file will be necessary for ANOVA and regression analysis and will require the values for choices to be increased by "1" so that all zeros are replaced by a "1" This will enable inputs from all participants to be used for linear ANOVA and regression analysis which requires non-zero values.
    (1) Delete rows 2 and 3 (Duplicate Column/Variable Names)
    (2) Referencing the column titled "Finished" retain all the rows that are shown as "TRUE" and hide all the rows that are shown as "FALSE" (i.e. "FALSE" indicates incomplete Scorecard).
    (3) Insert seven columns to the left of column A
        (a) Label the 1st column on the left "Size". This will be used for ANOVA
        (b) Label the 2nd column "Large", the 3rd column "Medium", and the 4th column "Small". These columns will be used for regression analysis.
        (c) Label the 5th column "Sector"
        (d) Label the 6th column "%IT"
        (e) Label the 7th column "%Cyber"
    (4) Data sort the entire worksheet by the column labeled "ExternalReference". This will order the contacts by Sector.

(5) In column labeled “Sector” Code sector and organization with for anonymization
   (a) Business with 10
   (b) Communications with 3
   (c) Defense Industry with 2
   (d) Elections with 4
   (e) Energy with 5
   (f) Finance with 6
   (g) Government Services with 7
   (h) Healthcare with 11
   (i) K-12 Education with 1
      (j) Local Government with 9
      (k) Water and Wastewater with 8
   (6) Under the “Size” column
      (a) Enter “1” for large organizations (designated as 1)
      (b) Enter “2” for medium organizations (designated as 2 or 3)
      (c) Enter “3” for small organizations (designated as 4,5,6,7,..)
   (7) Under “Large”, “Medium”, and “Small” columns enter a 1s as follows:
      (a) If the “Size” column has a value of 1 enter a 1 in the “Large” column
      (b) If the “Size” column has a value of 2 enter a 1 in the “Medium” column
      (c) If the “Size” column has a value of 3 enter a 1 in the “Small” column
   (8) For the “%IT” column for each row divide the column titled Q2.4 by Q2.3 (i.e. number of IT employees by the number of total employees)
   (9) For the “%Cyber” column for each row divide the column titled Q2.5 by Q2.3 (i.e. number of Cybersecurity employees by the number of total employees)
(10) Please note that ResponseID will be used for the anonymization ID of participating organizations
(11) Review employee data for organization (Q2.3), information technology related duties (Q2.4), and cybersecurity duties (Q2.5), change to integers as required by coding and recording changes.

(a) Eliminate “+” or “~”

(b) Eliminate “greater than”, “approx.”, or “Over”

(c) Etc.

(12) Check to see if there is more than one entry from any given organization and if so randomly hide any extra entries (i.e. row) so that only one remains per organization.

(13) Hide the following columns (so that sensitive data is not imported into SPSS)

(a) Start Date

(b) EndDate

(c) Status

(d) IPAddress

(e) Progress

(f) LocationLatitude

(g) ScoreResponse

(h) Duration (in seconds)

(i) Finished

(j) RecordedDate

(k) RecipientLastName

(l) RecipientFirstName

(m) RecipientEmail

(n) ExternalReference

(o) LocationLatitude

(p) LocationLongitude

(q) DistributionChannel

(r) UserLanguage

(s) Q2.1 (Name of Organization)

(t) Q2.2 (Your Email Address)

(u) SC0

(v) ScoreResponse

(w) Q2.1 – Topics

(x) ScoreResponse – Topics

(14) Search and Replace “Yes” with “1” and “No” with “2”

(15) Save the above work as two additional different files, one will be used for descriptive statistics (DS) and the second for ANOVA and regression anal. (AR)

(16) Open the descriptive statistics file (DS) and “Search and Replace” as follows:

(a) I Donâ€™t Know (0) with 0

(b) Strongly Agree (5) with 5

(c) Agree (4) with 4

(d) Neither Agree or Disagree (3) with 3

(e) Disagree (2) with 2

(f) Strongly Disagree (1) with 1

(g) Every Time (5) with 5

(h) Almost Every Time (4) with 4

(i) Occasionally / Sometimes (3) with 3

(j) Almost Never (2) with 2

(k) Never (1) with 1

(l) Save the file.

(17) Open the ANOVA and regression analysis file (AR) and “Search and Replace” as follows:

(a) I Donâ€™t Know (0) with 1

(b) Strongly Agree (5) with 6

(c) Agree (4) with 5

(d) Neither Agree or Disagree (3) with 4

(e) Disagree (2) with 3

(f) Strongly Disagree (1) with 2

(g) Every Time (5) with 6

(h) Almost Every Time (4) with 5

(i) Occasionally / Sometimes (3) with 4

(j) Almost Never (2) with 3

(k) Never (1) with 2

(l) Save the file

3. The two files are now ready for import into SPSS for analysis

APPENDIX E. SPSS PREPARATION STEPS FOR STATISTICAL ANALYSIS

1. Import (DS) XLSX file into SPSS
2. In "Variable View" check to ensure that all Variable "Types" are "Numeric" except the "ResponseID" which "String" should be.
3. Label the following Variables as indicated
    a. IT = IT Percent of Total Employees
    b. Cyber = Cybersecurity Percent of Total Employees
    c. ResponseID = ID Number
    d. Q2.3 = How many employees are there in your organization (full and part time)?
    e. Q2.4 = How many employees have information technology related duties?
    f. Q2.5 = How many employees have cyber security related duties?
    g. Q2.6 = Does your organization outsource your information technology needs?
    h. Q2.7 = Does your organization outsource your cybersecurity needs?
    i. Q3.1 = 1. Our Organization values cybersecurity
    j. Q3.2 = 2. (ID.AM) We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)
    k. Q3.3 = 3. (ID.AM) We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)
    l. Q3.4 = 4. (ID.BE) Our business/organization model influences the way we approach cybersecurity.
    m. Q.3.5 = 5. (ID.GV) When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.
    n. Q3.6 = 6. (ID.RA) We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.
    o. Q3.7 = 7. (PR.IP) We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.

p. Q3.8 = 8. (PR.DS) We have system checks in place to make sure that our data is not compromised or changed.
q. Q3.9 = 9. (PR.AC) Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).
r. Q3.10 = 10. (PR.IP) As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.
s. Q3.11 = 11. (PR.PT) Our cybersecurity technology (such as antivirus, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.
t. Q3.12 = 12. (RS.MI) We have a process in place to address a cyberthreat.
u. Q3.13 = 13. (RC.RP) We have a cyber emergency response plan in place to address a cyberattack on our organization.
v. Q3.14 = 14. (RC.RP) If we were impacted by a cyber emergency (e.g. ransomware), we know how our organization would recover our data and/or operational systems.
w. Q3.15 = 15. (RC.CO) After a cyberthreat or emergency, our organization will make changes to people, process, technology, etc. to improve our security.
x. Q4.1 = 16. Our executive leadership receives periodic status, physical, and cybersecurity updates.
y. Q4.2 = 17. (ID.AM) We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.
z. Q4.3 = 18. (PR.AT) We provide our employees cybersecurity awareness and/or training.
aa. Q4.4 = 19. (PR.AC) We protect our business and customer information so that only the employees that need to see it, can.
bb. Q4.5 = 20. (DE.DP) We would know if our cybersecurity technology detected a cyberthreat.

cc. Q4.6 = 21. (PR.AC & PR.PT) Our ‘smart’ devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.

dd. Q4.7 = 22. (DE.CM) Our ‘smart’ devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software.

4. For Variable Name “Size” assign the following the Labels: “Large” for “1”, “Medium” for “2”, and “Small” for “3”.
5. For Variable Name “Sector” assign the following Labels: “A” for “1”, “B” for “2”, “C” for “3”, “D” for “4”, “E” for “5”, “F” for “6”, “G” for “7”, “H” for “8”, “I” for “9”, “J” for “10”, “K” for “11”.
6. For Variable Names Q2.6 & Q2.7 assign the following Labels: “Yes” for “1”, and “No” for “2”.
7. Select the following “Measure” indicated for the Variable Names as indicated
    a. Select Nominal for Variable Names: Large, Medium, Small, Sector, ResponseID.
    b. Select Scale for Variable Names: IT, Cyber, Q2.3, Q2.4, Q2.5, and Score
    c. Select Ordinal for all remaining Variable Names Size, Q2.6, Q2.7, and Q3.1 through Q4.7.
8. Save the above as a (DS) SPSS SAV file
9. Import (AR) XLSX file into SPSS and apply steps 2 through 7 above and save the file as a (AR) SPSS SAV file.
10. When steps 1 through 9 above are complete the SPSS Variable View for both the (DS) and (AR) files should appear as shown in Figure E.1.

File Edit View Data Transform Analyze Direct Marketing Graphs Utilities Extensions Window Help

	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Size	Numeric	2	0		{1, Large...	None	5	Right	Ordinal	Input
2	Large	Numeric	2	0		None	None	6	Right	Nominal	Input
3	Medium	Numeric	2	0		None	None	7	Right	Nominal	Input
4	Small	Numeric	2	0		None	None	7	Right	Nominal	Input
5	Sector	Numeric	3	0		{1, A}...	None	10	Right	Nominal	Input
6	IT	Numeric	5	4	IT Percent of Total Employees	None	None	5	Right	Scale	Input
7	Cyber	Numeric	5	4	Cybersecurity Percent of Total...	None	None	6	Right	Scale	Input
8	ResponseId	String	17	0	ID Number	None	None	17	Left	Nominal	Input
9	Q2.3	Numeric	6	0	How many employees are the...	None	None	12	Right	Scale	Input
10	Q2.4	Numeric	5	0	How many employees have inf...	None	None	12	Right	Scale	Input
11	Q2.5	Numeric	4	0	How many employees have c...	None	None	12	Right	Scale	Input
12	Q2.6	Numeric	2	0	Does your organization outso...	{1, Yes}...	None	12	Right	Ordinal	Input
13	Q2.7	Numeric	2	0	Does your organization outso...	{1, Yes}...	None	12	Right	Ordinal	Input
14	Q3.1_1	Numeric	1	0	1. Our Organization values cy...	None	None	12	Right	Ordinal	Input
15	Q3.2_1	Numeric	1	0	2. (ID.AM) We know the type ...	None	None	12	Right	Ordinal	Input
16	Q3.3_1	Numeric	1	0	3. (ID.AM) We have evaluated ...	None	None	12	Right	Ordinal	Input
17	Q3.4_1	Numeric	1	0	4. (ID.BE) Our business/organ...	None	None	12	Right	Ordinal	Input
18	Q3.5_1	Numeric	1	0	5. (ID.GV) When we make a d...	None	None	12	Right	Ordinal	Input
19	Q3.6_1	Numeric	1	0	6. (ID.RA) We are familiar with...	None	None	12	Right	Ordinal	Input
20	Q3.7_1	Numeric	1	0	7. (PR.IP) We apply physical ...	None	None	12	Right	Ordinal	Input
21	Q3.8_1	Numeric	1	0	8. (PR.DS) We have system c...	None	None	12	Right	Ordinal	Input
22	Q3.9_1	Numeric	1	0	9. (PR.AC) Our data is availab...	None	None	12	Right	Ordinal	Input
23	Q3.10_1	Numeric	1	0	10. (PR.IP) As with the gener...	None	None	12	Right	Ordinal	Input
24	Q3.11_1	Numeric	1	0	11. (PR.PT) Our cybersecurity...	None	None	12	Right	Ordinal	Input
25	Q3.12_1	Numeric	1	0	12. (RS.MI) We have a proces...	None	None	12	Right	Ordinal	Input
26	Q3.13_1	Numeric	1	0	13. (RC.RP) We have a cyber ...	None	None	12	Right	Ordinal	Input
27	Q3.14_1	Numeric	1	0	14. (RC.RP) If we were impact...	None	None	12	Right	Ordinal	Input
28	Q3.15_1	Numeric	1	0	15. (RC.CO) After a cyberthre...	None	None	12	Right	Ordinal	Input
29	Q4.1_1	Numeric	1	0	16. Our executive leadership r...	None	None	12	Right	Ordinal	Input
30	Q4.2_1	Numeric	1	0	17. (ID.AM) We keep an inven...	None	None	12	Right	Ordinal	Input
31	Q4.3_1	Numeric	1	0	18. (PR.AT) We provide our e...	None	None	12	Right	Ordinal	Input
32	Q4.4_1	Numeric	1	0	19. (PR.AC) We protect our b...	None	None	12	Right	Ordinal	Input
33	Q4.5_1	Numeric	1	0	20. (DE.DP) We would know if...	None	None	12	Right	Ordinal	Input
34	Q4.6_1	Numeric	1	0	21. (PR.AC & PR.PT) Our 's...	None	None	12	Right	Ordinal	Input
35	Q4.7_1	Numeric	1	0	22. (DE.CM) Our 'smart' devic...	None	None	12	Right	Ordinal	Input
36	Score	Numeric	3	0		None	None	12	Right	Scale	Input

Figure E.1 SPSS Variable View

APPENDIX F. SAS STEPS FOR POWER PROCEDURE ANALYSIS

The following are the steps required to use ANOVA results from SPSS to conduct a Power Procedure on SAS to determine the sample sizes for a minimum power of 0.80. Figure F.1 depicts the descriptive statistics for the scores based on organizational size categories and for each size category. Figure F.2 depicts the Analysis of Variables for the scores versus size descriptive statistics in Figure F.1.

	N	Mean	Std. Deviation	Minimum	Maximum
Small	34	86.35	13.946	60	109
Large	9	90.78	15.746	67	110
Medium	13	94.85	12.429	72	110
Total	56	89.04	14.120	60	110

Figure F.1 Descriptives for Scores Versus Size

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	710.916	2	355.458	1.837	0.169
Within Groups	10255.013	53	193.491		
Total	10965.929	55			

Figure F.2 ANOVA of Scores Versus Size Descriptive Statistics

To conduct a Power Procedure in SAS acquire from Figure 4.1 the "Mean" for each group and from Figure 4.2 the "Mean Square / Within Groups" as listed below:

1. Means Large = 90.78
2. Means Medium = 94.85
3. Means Small = 86.35
4. Mean Square / Within Groups = 193.491

Calculate the square root of the Mean Square / Within Groups (√193.491 = 13.91) and along with the group Means enter them as 13.91 and 90.78|94.85|86.35 into the SAS power procedure code as shown in Figure F.3.

```
proc power;
    onewayanova test=overall
        groupmeans = 90.78|94.85|86.35     /*These are the sample means
from your pilot study*/
        stddev = 13.91 /* This is root MSE*/
        npergroup = . /* ntotal = npergroup*3, where 3 is the number of
groups*/
        power = .8;
    plot x=power min=0 max=1;
run;
```

Figure F.3 SAS Power Procedure Code

Figure F.4 depicts the SAS power procedure run output and how it calculates that for a power of 0.803 the N for each group will need to be at least 53.

The SAS System

The POWER Procedure
Overall F Test for One-Way ANOVA

Fixed Scenario Elements	
Method	Exact
Group Means	90.78 94.85 86.35
Standard Deviation	13.91
Nominal Power	0.8
Alpha	0.05

Computed N per Group	
Actual Power	N per Group
0.803	53

Figure F.4 SAS Power Procedure Run Output

APPENDIX G PILOT GROUP SCORECARD DATA

ResponseId	Q2.3	Q2.4	Q2.5	Style	Sector	Q2.6	Q2.7	Q3.1_1	Q3.2_1	Q3.3_1	Q3.4_1	Q3.5_1	Q3.6_1	Q3.7_1	Q3.8_1	Q3.9_1	Q3.10_1	Q3.11_1	Q3.12_1	Q3.13_1	Q3.14_1	Q3.15_1	Q4.1_1	Q4.2_1	Q4.3_1	Q4.4_1	Q4.5_1	Q4.6_1	Q4.7_1	Score
R_12oicXtzxIkFlP2	3000	50	4	1	A	2	2	4	4	3	4	4	4	2	3	2	4	1	1	4	4	3	3	3	4	4	0	2	67
R_1DVfVb4VMRru42n	1050	20	3	2	A	2	2	4	4	5	4	5	3	4	4	3	5	4	4	4	5	4	4	2	4	4	5	3	87
R_1go7sCIJvQGzKIB	1000	21	3	1	D	2	2	4	4	0	3	4	4	4	3	5	5	5	4	4	5	5	4	0	5	5	4	5	0	82
R_1HSZhVfgdFMmIy5	1800	15	1	2	D	1	1	5	5	3	3	4	3	2	4	4	2	4	3	2	4	3	4	3	3	4	3	5	3	75
R_1iak0JYpymdPngA	50,000	30,000	250	3	C	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	109
R_1ibqI6E4O8sBKUx	500	9	3	2	K	2	1	5	4	4	2	4	5	5	3	4	4	5	2	2	3	5	3	3	5	5	3	5	2	83
R_1ieMbZcGSowthK1	1000	15	1	3	D	1	1	3	3	2	3	2	4	3	5	4	3	5	4	4	5	3	3	2	2	3	4	5	3	75
R_1JWRDQ8PWqwp9Ag	215	215	5	3	I	1	1	5	4	3	4	5	5	5	5	4	5	4	4	5	5	3	3	3	4	5	4	0	2	88
R_1pldCQejmt17D7A	200	200	1	2	J	1	1	5	5	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	107
R_1q3yv0w1Mh97bwa	160	1	0	1	H	1	2	4	4	4	4	4	4	4	4	4	4	2	2	0	5	4	5	0	5	0	0	0	0	67
R_1YuiNsNmRTmb33P	30	2	2	3	H	1	1	5	5	5	5	4	2	4	5	4	4	4	4	5	5	2	5	3	5	5	0	0	0	86
R_23agqH0DKyaAsDF	75	2	2	3	G	2	2	5	5	5	4	5	5	4	4	4	3	4	3	3	3	3	3	3	5	3	0	0	0	79
R_25Gy4TDnsK8E90Z	17	12	12	3	H	2	2	4	4	3	3	4	4	5	4	4	4	4	4	4	4	3	3	4	5	4	3	4	4	85
R_27w0KIQ5zhGgkSI	20	15	0	3	H	1	1	3	4	3	3	4	4	4	4	4	2	3	2	2	4	3	3	4	3	3	2	5	3	71
R_28CjHkwyX4eL4Kt	24	5	1	3	C	2	2	4	5	4	4	3	4	4	2	4	4	3	3	2	4	4	1	3	1	4	2	1	2	68
R_28YVQIAryYBUnJD	550	20	7	2	F	2	2	5	5	5	2	5	5	5	5	5	4	5	5	5	5	4	5	5	5	5	4	5	4	103
R_2bH1tH2X6yARMqx	450	15	5	2	E	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	110
R_2ePswJn0ZGmu36t	70	35	3	3	B	2	2	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	3	5	4	5	5	5	104
R_2qdrWBCIufp8bHg	770	96	6	1	G	1	1	5	5	4	4	4	5	5	5	5	5	4	5	4	5	5	4	5	5	5	4	5	1	99
R_2rMzUsMM9N1cA9o	1149	16	1	3	A	2	1	5	5	3	4	2	5	2	2	4	4	4	4	2	5	5	5	5	3	5	3	1	3	81
R_2SAel3oCKfV5h8N5	125	34	11	3	C	2	2	4	5	5	4	4	5	5	5	5	4	5	4	4	5	4	4	4	4	4	4	3	4	94
R_2scBbwYtEHuLUlq	8	2	1	3	C	1	2	5	5	4	4	5	4	4	4	4	3	4	3	3	3	4	4	4	3	4	4	5	3	86
R_2VaPYu5klLWv4BZ	5,000	140	6	3	E	1	1	5	5	4	5	4	4	4	4	5	5	5	5	5	4	4	5	5	5	5	5	4	4	102
R_2XcFCSzI6whYdpU	800	12	5	2	A	2	2	4	5	5	4	5	4	5	5	4	4	4	4	4	5	3	5	5	3	5	3	3	4	93
R_2xXoahSNqWi1kmq	1000	500	4	3	A	2	2	5	5	4	5	4	5	5	5	4	5	5	5	5	4	5	4	4	5	5	4	5	3	101
R_2y3LpDFIfLiKvAw	21	8	2	3	C	1	1	5	5	4	5	4	4	4	4	4	4	3	3	4	4	4	5	3	4	3	3	3	3	87
R_2Yol5PEt1H4j1Gs	425	6	6	3	I	2	2	4	4	3	4	4	4	4	4	2	3	4	0	0	4	2	4	2	4	4	5	5	5	70

ResponseId	Q2.3	Q2.4	Q2.5	Size	Sector	Q2.6	Q2.7	Q3.1_1	Q3.2_1	Q3.3_1	Q3.4_1	Q3.5_1	Q3.6_1	Q3.7_1	Q3.8_1	Q3.9_1	Q3.10_1	Q3.11_1	Q3.12_1	Q3.13_1	Q3.14_1	Q3.15_1	Q4.1_1	Q4.2_1	Q4.3_1	Q4.4_1	Q4.5_1	Q4.6_1	Q4.7_1	Score
R_2YriLpxE3NFS7Vz	600	4	4	3	D	1	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	3	5	5	4	5	106
R_301v7TYCDwwVTaR	22	2	0	3	F	1	1	5	5	5	3	3	4	4	4	3	4	5	3	3	3	4	4	5	2	2	4	1	2	78
R_31M1GWURUPTVBW9	153	1	1	2	H	1	1	5	5	5	5	5	4	5	5	5	5	5	5	5	5	3	3	5	5	5	5	3	5	103
R_3D2cQc2MOayGDxp	1300	20	1	3	A	2	1	3	4	2	3	4	4	2	2	4	2	2	2	2	4	4	2	3	2	4	3	4	1	63
R_3EhSzYsPcZbeIDj	900	250	15	1	E	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	110
R_3EKIaZevAS6YUh5	28	2	2	3	F	1	1	5	5	5	4	4	4	4	5	4	4	4	4	4	3	4	5	4	3	5	5	5	5	95
R_3fBpdrkklICVfdJ	400	400	18	2	G	2	2	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	3	107
R_3hbR3iLg7jCaec2	6000	1000	50	1	F	1	1	4	3	3	4	4	5	5	4	4	5	5	5	4	5	4	5	3	5	5	4	4	4	94
R_3HHW3oCLxQBhcoC	40	2	2	3	J	1	1	4	3	3	5	4	4	4	1	2	4	4	1	1	1	4	3	2	3	4	3	0	0	60
R_3hrNIOw7L0UiTq4	400	400	20		F	2	2	5	5	3	4	4	5	3	4	4	5	5	5	4	4	4	5	4	5	5	5	3	3	94
R_3htO7yLCsAsuYh6	183	4	1	3	F	2	2	4	5	5	5	4	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	104
R_3hzugMrY6yjzzDe	6	1	1	3	B	1	1	5	5	4	5	4	4	4	2	2	3	4	2	2	4	4	3	3	3	4	3	5	3	78
R_3j6Sp4uETMMtJH7	200,000	50,000	1000	1	C	2	2	5	5	5	4	4	5	4	4	5	5	5	5	5	4	5	5	5	5	4	5	4	4	102
R_3JIWaiOmEX8C2DY	17	6	2	3	C	2	2	5	5	4	4	3	4	4	4	4	2	4	3	2	4	4	4	4	3	4	3	5	3	82
R_3jVFZIBTiN05OZL	75	2	2	3	G	1	1	5	5	5	5	4	5	5	4	4	3	5	4	4	4	5	3	3	4	4	3	5	3	92
R_3L1qgl7zCpIrRSM	1000	20	1	3	A	2	2	4	4	3	2	2	4	4	3	4	3	4	3	2	3	4	3	4	2	4	3	3	3	71
R_3POjmlSHFuzJNad	60,000			1	B	2	2	5	5	5	5	5	5	5	5	0	5	5	5	5	5	5	5	5	5	5	5	5	5	105
R_3s4WYX5NWsKpak2	165	6	9	2	F	2	2	5	5	5	4	2	5	5	4	5	3	4	4	4	2	5	4	5	5	5	4	5	3	93
R_6KDpH3ragNFc19v	16	1	1	3	K	1	1	4	5	4	3	4	3	4	3	4	3	5	3	3	4	5	3	3	3	3	4	5	0	78
R_8cdHOfNY0lOiVih	1200	65	6	2	E	2	2	4	5	4	4	4	5	4	5	5	5	5	4	4	5	5	4	3	5	4	5	3	5	97
R_8q2ihOH1aZ1MNjj	80	12	14	3	E	2	2	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	108
R_A7gAjiaNwSx8JO1	21	3	1	3	C	1	1	5	5	5	5	4	4	5	4	4	3	5	3	2	3	5	5	4	5	5	4	5	3	93
R_cYXud5qcww7RJAJ	110	80	12	3	B	1	1	4	5	4	4	5	5	5	5	4	4	5	5	5	5	5	3	5	4	5	5	4	4	100
R_DFSZpnHwc8fiyTD	18,500	800	120	3	E	2	2	5	4	4	4	4	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	102
R_DS2LmvQGIecBs4x	250	40	3	3	G	1	1	5	4	4	3	3	4	4	4	4	4	4	4	3	4	5	3	5	5	5	4	5	0	86
R_OMZt8QkSPxTOTkJ	42	42	3.00	3	C	1	1	4	3	2	2	2	4	4	2	3	2	3	2	2	4	4	2	1	2	4	4	5	2	63
R_sdIZnc7raIYpNIf	300	250	250	3	D	1	1	4	4	4	2	3	4	5	5	4	4	5	5	5	5	4	4	4	4	5	4	3	4	91
R_VVke1pl8zwwXhOp	475	3	3	2	I	2	2	5	5	5	5	4	5	5	5	5	2	5	5	5	5	5	4	5	4	5	4	5	5	103
R_xIMwPTwkSpPUSnD	350	150	5	2	B	1	1	2	3	2	2	2	3	4	4	4	4	4	2	2	5	5	3	4	3	4	4	3	3	72
R_Z91RXekL9d79V4Z	55,000	9000	50	1	J	1	2	4	5	5	4	4	5	4	5	5	5	4	4	5	4	4	4	3	4	4	4	3	2	91

LIST OF REFERENCES

ABET (Accreditation Board for Engineering and Technology). (2017). *Criteria for accrediting engineering programs: Effective for reviews during the 2018-2019 accreditation cycle*. Retrieved from http://www.abet.org

Accenture and Ponemon Institute. (2017). *2017 Cost of Cyber Crime Study - Insights on the Security Investments That Make a Difference*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Baldridge. (2017). *Baldridge Cybersecurity Excellence Builder*. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/04/03/baldrige-cybersecurity-excellence-builder-v1.0.pdf

Bartman, T., & Carson, K. (2015). *Securing critical industrial systems with SEL solutions*. Puttman, Washington. Retrieved from https://cdn.selinc.com//assets/Literature/Publications/White Papers/0013_SecuringCritical_TB_20150406.pdf?v=20150812-075045

Carcano, A. (2018). Russian Cyber Attacks on Critical Infrastructure: The "New Normal." Retrieved November 18, 2018, from https://www.nozominetworks.com/2018/07/24/blog/russian-cyber-attacks-on-critical-infrastructure-the-new-normal/

Clinton, B. Presidential Decision Directive 63 (1998). Retrieved from http://fas.org/irp/offdocs/pdd/pdd-63.htm

Corbin, J., & Anselm, S. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*.

Cowan, J., Bartlett, J., Haldane, D., Harris, S. A., Walley, F., Cathcart, R., … Twort, A. (1982). Design Education Based on an Expressed Statement of the Design Process. *Proceedings of the Institution of Civil Engineers*, *72*(4), 659–673. https://doi.org/10.1680/iicep.1982.1606

Craig, C. (2018). *Can We Afford to Train Respondes the Traditional Way, Manuscript submitted for publication*. Purdue University, West Lafayette, Indiana.

Defense Acquistion University. (2016). DOTmLPF-P analysis. Retrieved from https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2#

Department of Defense. (2016a). DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard. Retrieved from https://dodcio.defense.gov/Portals/0/Documents/Cyber/CNDSP Plain Language Overview - DISTRO.pdf?ver=2017-01-31-125734-897

Department of Defense. DoD Cybersecurity Discipline Implementation Plan (2016). Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

Department of Homeland Security and Multi-State Information Sharing and Analysis Center. (2018). Nationwide Cyber Security Review. Retrieved August 31, 2018, from https://www.cisecurity.org/ms-isac/services/ncsr/

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

DHS ICS-CERT. (2015). *NCCIC / ICS-CERT Year in Review 2015*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

DHS ICS-CERT. (2016). Cyer security evaluation tool fact sheet. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

General Electric. (2012). Cyber security for industrial controls, 1–8. Retrieved from https://www.gemeasurement.com/sites/gemc.dev/files/cyber_security_for_industrial_controls_english.pdf

Governor Eric J. Holcomb. (2018). *Indiana Cybersecurity Strategic Plan*. Indianapolis, Indiana. Retrieved from https://www.in.gov/cybersecurity/files/Cybersecurity-Report-FINAL-no-Appendices1.pdf

Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*, *3*, 73–86.

Holcomb, E. J. Executive Order 17-11: Continuing The Indiana Executive Council on Cybersecurity (2017). Retrieved from https://www.in.gov/gov/files/EO_17-11.pdf

Indiana Executive Council on Cybersecurity. (2017). *Indiana Executive Council on Cybersecurity Council Charter*. Retrieved from https://www.in.gov/cybersecurity/files/Exectuive Council on Cybersecurity Charter_Voted_September 27 2017.pdf

Indiana Finance Authority. (2016). *Evaluation of Indiana ' s Water Utilities An analysis of the State ' s aging infrastructure*. Indianapolis, Indiana.

Indiana Utility Regulatory Commission. (2017). Retrieved April 30, 2017, from http://www.in.gov/iurc/

Kambic, J., Smith, T., & Yang, B. (2013). An introduction to SCADA / ICS systems and the security surrounding them. In *ITERA*.

Kaspersky Lab. (2018). *Threat Landscape for Industrial Automation Systems, H1 2018*. Retrieved from https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/

Keeper Security. (2017). *2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)*. Retrieved from https://csrps.com/Media/Default/2017 Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

Loeb, M. P., & Gordon, L. A. (2006). *Managing Cyber-Security Resources: A Cost-Benefit Analysis*. New York, New York: McGraw Hill.

Loukas, G. (2015). A History of Cyber-Physical Security Incidents. *Cyber-Physical Attacks*, 21–57. https://doi.org/10.1016/B978-0-12-801290-1.00002-3

Mahan, R., Fluckiger, J., & Clements, S. (2011). Secure data transfer guidance for industrial control and SCADA systems, (September). Retrieved from http://www.pnnl.gov/main/publications/external/technical_reports/pnnl-20776.pdf

National Cybersecurity and Communications Integration Center. (2017). *Cyber Security Evaluation Tool*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC ICS_FactSheet_CSET_S508C.pdf

National Governors Association. (2017a). A Compact to Improve State Cybersecurity. Retrieved August 1, 2018, from https://ci.nga.org/files/live/sites/ci/files/1617/docs/1707CybersecurityCompact.pdf

National Governors Association. (2017b). NGA Governer's Guide to Cybersecurity. Retrieved from http://mediaw.nga.org/media/resources/cybersecurity/index.html

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity v1.0*. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2018a). 180521 NIST Cybersecurity Framework Assessment & Auditing Resources. Retrieved from https://www.nist.gov/cyberframework/assessment-auditing-resources

National Institute of Standards and Technology. (2018b). *Framework for Improving Critical Infrastructure Cybersecurity v1.1*. https://doi.org/10.1109/JPROC.2011.2165269

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of S*, 1–41. https://doi.org/10.1109/JPROC.2011.2165269

Pence, M. R. Executive Order 16-01: Establishing The Indiana Executive Council on Cybersecurity (2016). Retrieved from https://www.in.gov/governorhistory/mikepence/files/Governor_Pence_EO_Cybersecurity_4-20-2016.pdf

Ponemon Institute LLC. (2018). *2018 Cost of Data Breach Study, Global Overview*. Retrieved from https://www.ibm.com/security/data-breach

PwC. (2014). *Why you should adopt the NIST cybersecurity framework*. Retrieved from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Rockwell Automation. (2013). *Flexible solutions for your supervisory control and data*. Retrieved from http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp031_-en-e.pdf

Schneider Electric. (2015). *Modicon controllers platform cyber security reference manual*. Retrieved from http://download.schneider-electric.com/files?p_File_Id=1069830531&p_File_Name=EIO0000001999.01.pdf

Sharp, J. J. (1991). Methodologies for problem solving: An engineering approach. *Vocational Aspect of Education*, *42*(114), 147–157. https://doi.org/10.1080/03115519108619446

State of Michigan. (2018). *CySAFE IT Security Assessment Tool v2.0*. Retrieved from https://www.michigan.gov/documents/cybersecurity/cysafe_flyer_SOM3_468548_7.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) security. *NIST Special Publication 800-82 Rev2*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-82r2

Symantec Corporation. (2018). *Internet Security Threat Report* (Vol. 23). Retrieved from https://www.symantec.com/security-center/threat-report

The Center for Infrastructure Assurance and Security. (n.d.). Community Cyber Security Maturity Model. Retrieved August 31, 2018, from http://cias.utsa.edu/the-ccsmm.html

The Council of Economic Advisers. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy, (February), 62. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

The White House. The National Strategy to Secure Cyberspace, GOV US Executive Branch § (2003). Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

The White House. (2013a). Executive Order 13636: Improving critical infrastructure cybersecurity. *Federal Register*, *78*(33), 1–8. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

The White House. Presidential Policy Directive - Critical Infrastructure Security and Resilience (2013). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

U.S. Census. (2016). US Census County Business Patterns by Employment Size Class. Retrieved from https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=BP_2016_00A3&prodType=table

U.S. Computer Emergency Readiness Team. (2018). US-CERT Alert TA18-074A Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved November 18, 2018, from https://www.us-cert.gov/ncas/alerts/TA18-074A

Verizon. (2018). *2018 Data Breach Investigations Report*. Retrieved from https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Zetter, K. (2016a). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zetter, K. (2016b). Lessons learned from the power outage in Ukraine and how electric grid of the future will reduce cybersecurity risk. Retrieved from http://cip.gmu.edu/2016/05/24/lessons-learned-power-outage-ukraine-electric-grid-future-will-reduce-cybersecurity-risk/

VITA

James E. Lerums

Experience

- Colonel, U.S. Army
  - Chief, Information Superiority Knowledge Management and Chief Financial Officer, Operations Directorate, Headquarters, U.S. European Command, Stuttgart, Germany, U.S Army, April 2008 – June 2013
  - Chief, Operations Assessments, Strategic Operations, Multi-National Force-Iraq, Baghdad, Iraq, U.S. Army, December 2006 – November 2007
  - Director, Knowledge Management Operations, Multi-National Corps-Iraq, Baghdad, Iraq, U.S. Army, November 2005 – December 2006
  - Deputy Chief of Staff, Logistics, 5th Signal Command, Manheim, Germany, U.S. Army, September 2004 – September 2005
  - Chief, Deployment and Distribution Management Center, 21st Theater Support Command, Kaiserslautern, Germany, U.S. Army, October 2003 – September 2005
  - Director of Field Services, 21st Theater Support Command, Kaiserslautern, Germany, U.S. Army, December 2002 – October 2003
  - Department Head / Battalion Commander, 4th/84th Training Battalion, 3rd Brigade, 84th Division (Individual Training), Anderson, Indiana, U.S. Army, January 2000 – December 2001
- Financial Advisor, Indianapolis, Indiana, Morgan Stanley Dean Witter, December 1996 – January 2014
- Sales and Marketing Manager, Indianapolis, Indiana, Hurco Companies, Incorporated, November 1995 – June 1996
- Manager System Integrator Program / Manager, District Program Development, Automation Products Group, Allen-Bradley Company, Highland Heights, Ohio, October 1990 – May 1995
- Area Manager, Communications Division Products (*for factory automation*), Indianapolis, Indiana, Allen-Bradley Company, January 1987 – September 1990
- Sales Engineer / Manager Electronic Sales – Electronics Group, Indianapolis, Indiana, Allen-Bradley Company, February 1983 – December 1986
- Product Manager - Quality Assurance Software Products, Rochester, New York, Hansford Data Systems, September 1981 – January 1983
- Entrepreneur Principal – Metal Products Manufacturer, Canandaigua, New York, Valerco, November 1980 – September 1981
- Engineer / National Sales Representative, Macedon, New York, Mobil Chemical Company, Packaging Division, January 1978 – November 1980
- Battalion Signal Officer, 326 Engineer Battalion, 101st Airborne Division (Air Assault), Fort Campbell, Kentucky, U.S. Army, January 1977 – December 1978
- Platoon Leader, 501st Signal Battalion, 101st Airborne Division (Air Assault), Fort Campbell, Kentucky, U.S. Army, March 1975 – December 1976

Education

- Purdue University — West Lafayette, IN
  Ph.D. Interdisciplinary Information Security, — December 2018
  Specialization: Operational Aspects of Cyber Security
  Principal Advisor: J. Eric Dietz
  Dissertation: Measuring the State of Indiana's Cybersecurity

- Purdue University — West Lafayette, IN
  M.S. Interdisciplinary Information Security, — August 2016
  Thesis: Accelerating Cybersecurity Improvements for Critical Infrastructure Industrial Control Systems

- Purdue University — West Lafayette, IN
  Graduate Certificate in Information Security Policy, — May 2016

- Defense Acquisition University,
  Fundamental of Systems Acquisition Management, — March 2008

- Army Logistics Management College
  Multi-Functional Logistics Operations, — December 2002

- US Army Command and General Staff College
  Command and General Staff Officer Course — December 1996

- Pennsylvania State University — State College, PA
  B.S. Electrical Engineering, — August 1974

General Interest

Information Security, Cyber Forensics, Cyber Security Operations, Social Economic and Legal Aspects of Information Security, "Right-Sizing" Cyber Security Solutions and Implementations, Cyber Warfare, Cyber Risk, Cyber Exercises, Physical Security Exercises

H**onors, Fellowships, and Awards**

- Purdue Polytechnic Seed Grant Program ($17,400) (2016)
- Published Paper - The Ethics of Hacking Back*,* was selected for highlighting in *IEEE's Xplore Innovation Spotlight* (2016)
- Legion of Merit
- Bronze Star (with 1 Oak Leaf Cluster)
- Defense Meritorious Service Medal
- Meritorious Service Medal (with 2 Oak Leaf Clusters)
- Joint Service Commendation Medal (with 1 Oak Leaf Cluster)
- Army Commendation Medal (with 1 Oak Leaf Cluster)
- Army Achievement Medal
- Army Reserve Components Achievement Medal (with 5 Bronze Oak Leaf Clusters)

Professional Memberships

- Armed Forces Communications and Electronic Association (AFCEA)
- Association of the United State Army (AUSA)
- Center for Education and Research in Information Assurance and Security Student Association
- High Technology Crime Investigation Association (HTCIA)
- Information Systems Security Association (ISSA)
- InfraGard
- Institute of Electrical and Electronic Engineers (IEEE)

Refereed Journal Publications

- Lerums, J., Economics of Critical Infrastructure Industrial Control Systems' Cyber Security (In process)
- Lerums, J., Reichart, K. & Dietz, J.E., Developing a Public/Private Cybersecurity Scorecard for the State of Indiana (In process)
- Lerums, J., Poe, La'Reshia, & Dietz, J.E., Simulation Modeling Cyber Threats, Risks, and Prevention Costs (In process)
- Holzer, C., & Lerums, J., The Ethics of Hacking Back. In *IEEE Xplore* 2016

Technical Papers

- Ringenberg, T., Lerums, J., Rayz, J. (2018). Detecting Decoy Chat Differences with Fantasy Versus Contact Offenders
- Dietz, J. E., Lerums J., Magee, T., (2017). Bankers Life Fieldhouse Large-Scale Event Table Top Exercise After Action Report
- Dietz, J. E., Lerums J., Magee, T., (2017). Bankers Life Fieldhouse Large-Scale Event Table Top Exercise Situation Manual
- Hartman, E., Hilgers, R., Lerums, J., Poe, L. (2017) AnyLogic Modeling Cyber Threats, Risks, and Prevention Costs (2nd Edition)
- Lerums, J., (2017). Economics of Critical Infrastructure Industrial Control Systems' Cyber Security
- Gilbert, A., Iyer, S., Lerums, J., (2016). AnyLogic Modeling Cyber Threats, Risks, and Prevention Costs (1st Edition)
- Lerums, J. (2016). Checking, Increasing, and Confirming a Smart Home's IoT Security
- Lerums, J. (2015). Developing an Exercise Model for Validating Cyber Security Operations
- Lerums, J. (2015). 2007 Estonia Cyber Attack – Analysis of National Responses During and Subsequent to Attack
- Garramone, M., Lerums, J. (2015). Managing Contributions Following a Local Disaster
- Chong, R., Flory, C., Lerums, J., Long, D., Prof. Dark, M., Prof. Foreman, C. (2014). FIDO Password Replacement: Spoofing a Samsung Galaxy S5 and PayPal Account Using a Latent Fake Fingerprint
- Lerums, J., Liles, S., (2014). Authentication Security – Passwords vs FIDO

Conference or Symposium Proceedings

- Lerums, J. (2018) Economics of Critical Infrastructure Industrial Control Systems' Cyber Security. In the *6th IAJC International Conference.* Orlando, Florida
- Lerums, J., Reichart, K. & Dietz, J.E. (2018) Developing a Public/Private Cybersecurity Scorecard for the State of Indiana. In the *IEEE Homeland Security and Technology Conference*. Boston, Massachusetts
- Lerums, J., Poe, L., & Dietz, J.E. (2018) Simulation Modeling Cyber Threats, Risks, and Prevention Costs. In the *IEEE International Conference on Electro/Information Technology*. Rochester, Michigan
- Holzer, C. & Lerums, J. (2016). The Ethics of Hacking Back. In the *IEEE Homeland Security and Technology Conference.* Boston, Massachusetts
- Lerums, J. (2016). Checking, Increasing, and Confirming a Smart Home's IoT Security. In the *Information and Telecommunications Education and Research Association Conference*. Louisville, Kentucky

Chapters in Books

- Dietz J.E., Iyer, S., Glass, P., Gruesbeck, K.L., Lerums, J., Schultz, N., Smith, A, (2017). Use of Simulation Modeling to Reduce Consequences of an Active Shooter. In Dietz, J.E., and Black, D.E. Editors, Riechart, K. Assistant Editor, *Large Event Security*, New York, NY, USA: CRC Press: Taylor & Francis (in progress)

Research Experience

- **Graduate Research Assistant**, Polytechnic Computer Information and Technology, Purdue University, W. Lafayette, IN September 2016 – Present
    - Developed foundation model to examine cyber security risks, benefits, and costs
    - Met with ITaP (Information Technology at Purdue) and Statistics Department to fine tune modeling
    - Using AnyLogic software modeling simulated several iterations of a given type of cyberattack to measure effectiveness of a defense in depth cyber solution
    - Researching cyber scorecard methodology for accelerating cyber security improvements
- **Thesis Research**, Polytechnic Computer Information and Technology
  Purdue University, W. Lafayette, IN January 2016 – August 2016
    - Participated as a Scribe and Senior Evaluator during the State of Indiana's Crit-Ex 16.1&2 Exercises
    - Collaborated with both U.S. and Indiana Departments of Homeland Security
    - Researched US NIST and ICS-CERT Critical Infrastructure standards and assessments tools for critical infrastructure control systems
    - Researched business databases to analyze the size and revenues of Indiana Water Utilities as well vendor solutions for the cyber security state of recent industrial control systems.

  - Identified constraints to accelerating cyber security improvements to water utilities' critical infrastructure control systems
- **Knowledge Management and Congressional Research (**Chief, Operations Assessment), , Multi-National Force- Iraq, U.S. Army, December 2006 - October 2007
  - Researched knowledge management requirements based on forward looking theater strategy and operations, identified critical data collection and analysis processes, and published the first document assigning data proponents and their responsibilities which increased integrity of databases and reporting.
  - Recognized for time sensitive, complex and critical research and reports for Congressional testimony.
  - Researched veracity and differences in various types of significant activity and media reports and determined various strengths and weaknesses between reports.
- **Knowledge Management Research** (Director, Knowledge Management Operations), Multi-National Corps – Iraq, U.S. Army,
  January - November 2006
  - Researched the data schemas for the various reporting systems to synchronize data from various sources, eliminate redundancy, and enable predictive statistical analysis.
  - Based on operations and changing threat situations researched various reporting systems and designed technical and human factors testing environments to determine best system solution for collecting significant activities reports for predictive database analysis.
  - Based on research outcome secured $2M in funding to implement and sustain country wide reporting and database system.
  - Secured and executed over $30K of funding to research a reporting data schema proof of concept OLAP cube (a multidimensional data base that is optimized for data warehousing and Online Analytical Processing (OLAP) applications).

Academic Leadership Involvement

- 2018 Law and Society Intern Program
  Purdue Homeland Security Institute
  Mentor – Spring 2018 Semester
- 2017 Law and Society Intern Program
  Purdue Homeland Security Institute
  Mentor – Spring 2017 Semester
- CERIAS Student Association
  Purdue University
  Officer, August 2016 – Present
- CERIAS and CIT Graduate Students
  Purdue University
  Mentor – Spring 2016 – Present
- 2016 Atlantic Council Cyber 9/12 Competition

Team Coach, January 2016 – March 2016

- 2016 State of Indiana Crit-Ex 16.2 Functional Water Utility Disruption Facilitated Cyber Exercise
  Senior Evaluator - May 2016
- 2015 Atlantic Council Cyber 9/12 Competition
  Purdue University
  Senior Mentor, January 2015 – March 2015

Academic Services

- *Board Member of the Interdisciplinary Graduate Programs Student Advisory Board,* Purdue University November 2016 – Present

Other Major Engagement Activity

- *Chief, Information Superiority Knowledge Management and Chief Financial Officer*, Operations Directorate, Headquarters U.S. European Command, U.S. Army 2008-2013
  - Engaged U.S. government departments and agencies, other nations, and non-governmental organizations locally and internationally to research and implement knowledge management solutions which increased the speed, accuracy, and synchronization of collaboration, planning, and reporting to senior leadership.
  - Acquired over $11.5M of additional funding and successfully upgraded operations center.
  - As Directorate's Chief Financial Officer secured and executed a $12M (70%) increase in FY 2012 annual funding during the federal reduction in spending and manpower.
- *Chief, Operation Assessment*, Strategic Operations, Multi-National Force – Iraq, U.S. Army, 2007
  - Led several database and reporting conferences attended by key subject matter experts from across Iraq to reduce duplication of effort, synchronize correct data and mitigate "confusion potential" for critical data requirements.
  - Recognized for implementing a reporting and database system between the Coalition Forces and Government of Iraq.
- *Deputy, Chief of Staff Logistics*, 5th Signal Command, U.S. Army, 2004-2005
  - Conducted post-award administration on over 20 contracts valued at over $200M (which included over 290 contractors)
  - Led multiple organizations through a complex bid-solicitation process for a new operations maintenance and supply contract totaling over $180M
- *Chief, Deployment and Distribution Management*, 21st Theater Support Command, U.S. Army 2004-2005
  - Engaged multiple organizations across at least three continents to ensure efficient and effective shipment and distribution of personnel and billions of dollars in equipment and supplies.

Teaching Experience

- Guest Lecturer, South East Michigan IEEE Chapter
  - Presented paper: Developing a Public/Private Cybersecurity Scorecard for the State of Indiana, November 2018
- Guest Lecturer, Purdue University
  - CS 591 Information Security and Cyber Crime Seminar, Fall 2018
  - CNIT 581 Homeland Security Seminar, Spring 2017
  - CNIT 511 Foundations in Homeland Security Studies, Fall 2017
- Teaching Assistant, Homeland Security Seminar, Spring 2017
  - Tasked and oversaw four multi-disciplinary graduate and undergraduate teams on four diverse research projects that included large event and cyber security.
  - Independently taught a class on smoothly planning and execution of research projects
  - Organized several class in-process-reviews to ensure diverse research projects stayed on schedule
  - Interfaced with client (Banker's Life Fieldhouse) and worked scheduling and logistics to ensure that researchers collected and reported on required data
- Director, Knowledge Management Operations, Multi-National Corps – Iraq, U.S. Army, 2006
  Directed the country wide training for newly fielded Command Post of The Future (CPOF), Significant Activity (SIGACT), and Improvised Explosive Device (IED) reporting systems in Iraq.
- Director, Field Services, 21st Theater Support Command, U.S. Army, 2002
  Directed curriculum development and instruction by senior personnel for training new organizational structure and operations with courses taught in three separate tiers for junior, mid-level, and senior personnel.
- Department Head (Battalion Commander), 4th/84th Signal Training Battalion, U.S. Army, 2000-2001
  - Department Head for communications / computer school with a faculty and staff of fifty who conducted hands on training in five states for over 220 students annually (with capacity for over 400)
  - Reaccredited the school's six computer and communications training programs
- Principal Instructor (Assistant Chief of Staff, Security Plans and Operations), 21st Theater Support Command, U.S. Army, 1997-1999
  - Organized and led course development for staff logistics training of over 750 personnel in fifteen separate organizations to experience and exercise real world operations for a specified area.
  - Planned and executed the training calendar to ensure organizations met multiple required training standards.
  - Increased mission-directed individual competencies by negotiating operations-tempo training overseas with overseas partner organizations.

- Principal Instructor (Manager System Integrator / Manager Distributor Program Development) Allen-Bradley Company, 1993-1995
    - Developed curriculum, selected instructors, managed administration, logistics and promotions for the Distributor Technical University Conference (annual attendance increased by 300%).
    - Managed industrial programmable logic controls training for System Integrators and Distributors

Certificates and Training

- AnyLogic Simulations Software Training – August 2017
- FEMA IS-15.b Special Events Contingency Planning for Public Safety Agencies – July 2017
- FEMA IS-100.b Introduction to Incident Command System – July 2017
- FEMA IS-120.a An Introduction to Exercises – July 2017
- FEMA IS-130 Exercise Evaluation and Improvement Planning – July 2017
- FEMA IS-200.b ICS for Single Resources and Initial Action Incident – July 2017
- FEMA IS-230.d Fundamentals of Emergency Management – August 2017
- FEMA IS-235.c Emergency Planning – June 2017
- FEMA IS-700.a National Incident Management System Introduction – September 2015
- FEMA IS-800.b National Response Framework Introduction – July 2017