CISTAR CYBERSECURITY SCORECARD

by

Braiden M. Frantz

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer & Information Technology

West Lafayette, Indiana

December 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. J. Eric Dietz, Chair

Department of Computer and Information Technology

Dr. William Field

School of Agricultural and Biological Engineering

Dr. John Springer

Department of Computer and Information Technology

Approved by:

Dr. Eric Matson

Head of the Graduate Program

This thesis is dedicated to my wife and children

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

For the purpose of this study, the following research specific terms are used throughout the scope of this project.

- Accredited Cyber Training: Certifications in training courses that include the following: Certified Information Security Manager, CompTIA A+, CompTIA Security+, CompTIA Network+, Certified Information Systems Security Professional, CompTIA Advanced Security Practitioner+, or Certified Ethical Hacker
- Brute Force: Act of a cyber-criminal illegally entering numerous username and password combinations at random in hopes to guess correctly.
- Center for Innovative and Strategic Transformation of Alkane Resources (CISTAR): "Researchers from five premier U.S. research universities and industrial collaborators from more than a dozen companies focused on developing breakthrough solutions to more effective conversion of America's shale derived light hydrocarbon resources" (Center for Innovative and Strategic Transformation of Alkane Resources, 2017).
- Certification and Accreditation: "Certification involves the testing and evaluation of the technical and nontechnical security features of an IT system to determine its compliance with a set of specified security requirements. Accreditation is a process whereby a designated approval authority or other authorized management office authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk" (Grance, Hash, Peck, Smith & Korow-Diks, 2002).
- Credential Stuffing: Act of using compromised credentials, typically a username and password, across multiple domains in order to illegally gain access.
- Cyberspace: "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunication networks, computer systems, and embedded processors and controllers" (National Institute of Standards and Technology, 2011).
- Cybersecurity: "The ability to protect or defend the use of cyberspace from cyber-attacks" (National Institute of Standards and Technology, 2013)

- Cyber-criminal: "Also known as hackers who use computer systems to gain access to business trade secrets and personal information for malicious and exploitive purposes. Hackers are extremely difficult to identify on both an individual and group level due to their various security measures, such as proxies and anonymity networks, which distort and protect their identity" (Norwich University Online, 2017).
- Cyber-attack: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (Committee on National Security Systems Instruction, 2015).
- Defensive Cyberspace Operations: "Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems" (Committee on National Security Systems Instruction, 2015).
- Demilitarized Zone (DMZ): Within cyberspace, this is often present in the form of an additional firewall between a network and the public internet. Functions as an additional security layer provided to a local area network. Typically, the most vulnerable services to a potential compromise such as web and email servers reside within the DMZ, limiting the amount of damage incurred.
- Distributed Denial of Service (DDOS): "An attempt to make a machine or network resource unavailable for its intended use. It often consumes more computer resources than a device can handle or disrupts by disabling communication services. It is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems" (Metivier, 2018).
- Malware: "Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code" (Committee on National Security Systems Instruction, 2015).
- National Institute of Standards and Technology (NIST): "Part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories, providing

technology, measurement and standards for United States industry" (National Institute of Standards and Technology, 2019).

- NIST Best Practices: Recommended cybersecurity steps provided by the National Institute of Standards and Technology. These recommendations are offered free of charge in the form of publications and provide a baseline for all cybersecurity professionals to implement.
- Periodic Password Changes: Frequency of mandatory password changes for access to the organization's network. This is especially important for administrator accounts.
- Posture: Status of an organization's cybersecurity defenses and mechanisms/techniques in place. This may also encompass whether the company has trained cybersecurity professionals on staff.
- Purdue Process Safety and Assurance Center (P2SAC): The Purdue University Davidson School of Engineering organization that focuses upon educating chemical engineering students in areas of process safety, disaster preparation and the overall avoidance of injuries within research, manufacturing, pharmaceuticals, agriculture and consumer product development. Sponsors provide funding for educational safety, which include AMGEN, BP, Chevron, Dow, ExxonMobil, Honeywell, Lilly, Pfizer, Phillips 66, Shell and 3M. Risk management collaborations are in place with sponsors such as Fauske Associates and Kenexis.
- Supervisory Control and Data Acquisition (SCADA) System: "System of software and hardware elements that allows industrial organizations to control industrial processes locally or at remote locations, monitor/gather/process real-time data, record events into a log file or directly interact with devices such as sensors, valves, pumps, motors and more through human-machine interface software" (What is SCADA?, 2018).
- Threat Actor: Criminal acting within cyberspace to gain illegal access to a system or network.
- Threat Vector: Common procedures or attack techniques used by cyber-criminals to gain access to a computer or network with the intent of system exploitation.

LIST OF ABBREVIATIONS

CASP	CompTIA Advanced Security Practitioner
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CISTAR	Center for Innovative and Strategic Transformation of Alkane Resources
DDOS	Distributed Denial of Service
DMZ	Demilitarized Zone
LAN	Local Area Network
LOPA	Layer of Protection Analysis
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
P2SAC	Purdue Process Safety and Assurance Center
SCADA	Supervisory Control and Data Acquisition
SPSS	Statistical Package for the Social Sciences

ABSTRACT

Author: Frantz, Braiden, M. MS
Institution: Purdue University
Degree Received: December 2019
Title: CISTAR Cybersecurity Scorecard
Committee Chair: J. Eric Dietz

Highly intelligent and technically savvy people are employed to hack data systems throughout the world for prominence or monetary gain. Organizations must combat these criminals with people of equal or greater ability. There have been reports of heightened threats from cyber criminals focusing upon the energy sector, with recent attacks upon natural gas pipelines and payment centers. The Center for Innovative and Strategic Transformation of Alkane Resources (CISTAR) working collaboratively with the Purdue Process Safety and Assurance Center (P2SAC) reached out to the Computer and Information Technology Department to assist with analysis of the current cybersecurity posture of the companies involved with the CISTAR initiative. This cybersecurity research project identifies the overall defensive cyber posture of CISTAR companies and provides recommendations on how to bolster internal cyberspace defenses through the identification of gaps and shortfalls, which aided the compilation of suggestions for improvement. Key findings include the correlation of reduced cybersecurity readiness to companies founded less than 10 years ago, cybersecurity professionals employed by all CISTAR companies and all CISTAR companies implementing basic NIST cybersecurity procedures.

CHAPTER 1. INTRODUCTION

1.1 Introduction to the Problem

Throughout the country "over 500,000 miles of high-volume pipeline gather and transport natural gas, oil, and other hazardous liquids across the United States. In addition, nearly 900,000 miles of smaller distribution pipelines deliver natural gas to businesses and homes" (Parfomak, 2012, p. 1). Such a vast network of pipelines requires management systems to oversee operations, many of which are conducted remotely. Private companies also exist that manage payment or delivery of natural gas and petroleum, which tie into the larger industry networks. This creates a problem for companies concerning lateral movement by cyber criminals. When attempting to breach a system, in this case the natural gas or petroleum industry network, criminals often seek the path of least resistance. Smaller companies may not have the ability or resources to comply with the recommended cybersecurity provisions outlined by the federal government. This weakens not only the small business, but also any other business or organization that is networked to the company. The security concern could also spread to foreign companies that have established network trusts with compromised businesses or organizations located within the United States.

Cybersecurity risks to the petroleum and gas industries have been documented by the federal government since 2011. According to Parfomak (2012), the White House pushed a proposal, coupled with the Cybersecurity Act of 2012, that mandated cybersecurity regulations for critical infrastructure owned throughout the private sector. The original Cybersecurity Act would later be revised to include additional measures, all of which were voluntary, serving as an advisory role to the petroleum and gas industry.

1.1.1 Basic Petroleum and Natural Gas Pathway

In order to narrow the focus of the problem, this research will focus upon post-exploration and drilling operations. Off-shore drilling and well systems will not be included for research purposes due to the lack of presence throughout the petroleum and natural gas organizations involved in this study. Many of the companies associated with the Center for Innovative and Strategic Transformation of Alkane Resources (CISTAR) and Purdue Process and Safety Assurance Center (P2SAC) are involved with the production process and beyond. "The CISTAR team will develop innovative process designs for economic production of chemicals and transportation fuels from shale gas hydrocarbons." (Center for Innovative and Strategic Transformation of Alkane Resources, 2017). Additionally, the CISTAR vision includes a diverse network of processing plants, reinforcing the need for effective defensive cybersecurity. P2SAC is dedicated to the improvement of industrial safety in order to prevent disasters and save lives. This focus extends to the petroleum and natural gas industries, with process safety as an area of research for the companies that serve as sponsors. P2SAC is partnered with CISTAR under a National Science Foundation funded project to evaluate and improve cybersecurity for the organizations involved with the CISTAR initiative.

The petroleum and natural gas supply paths involve upstream, midstream and downstream operations (see *Figure 1.1*) prior to reaching the end user or customer. Midstream activities and the associated network systems are the focal point of this study, primarily the processing, storage and transfer of petroleum and natural gas. Additionally, company interface and trusts established with third party vendors can pose network risks, with historical examples of compromised vendor networks creating pipeline disruptions. These types of network trusts are becoming more popular, and while most are nested within the downstream industry, it is still

important to cover methods to prevent the spread of third-party network infections to companies within CISTAR and P2SAC.

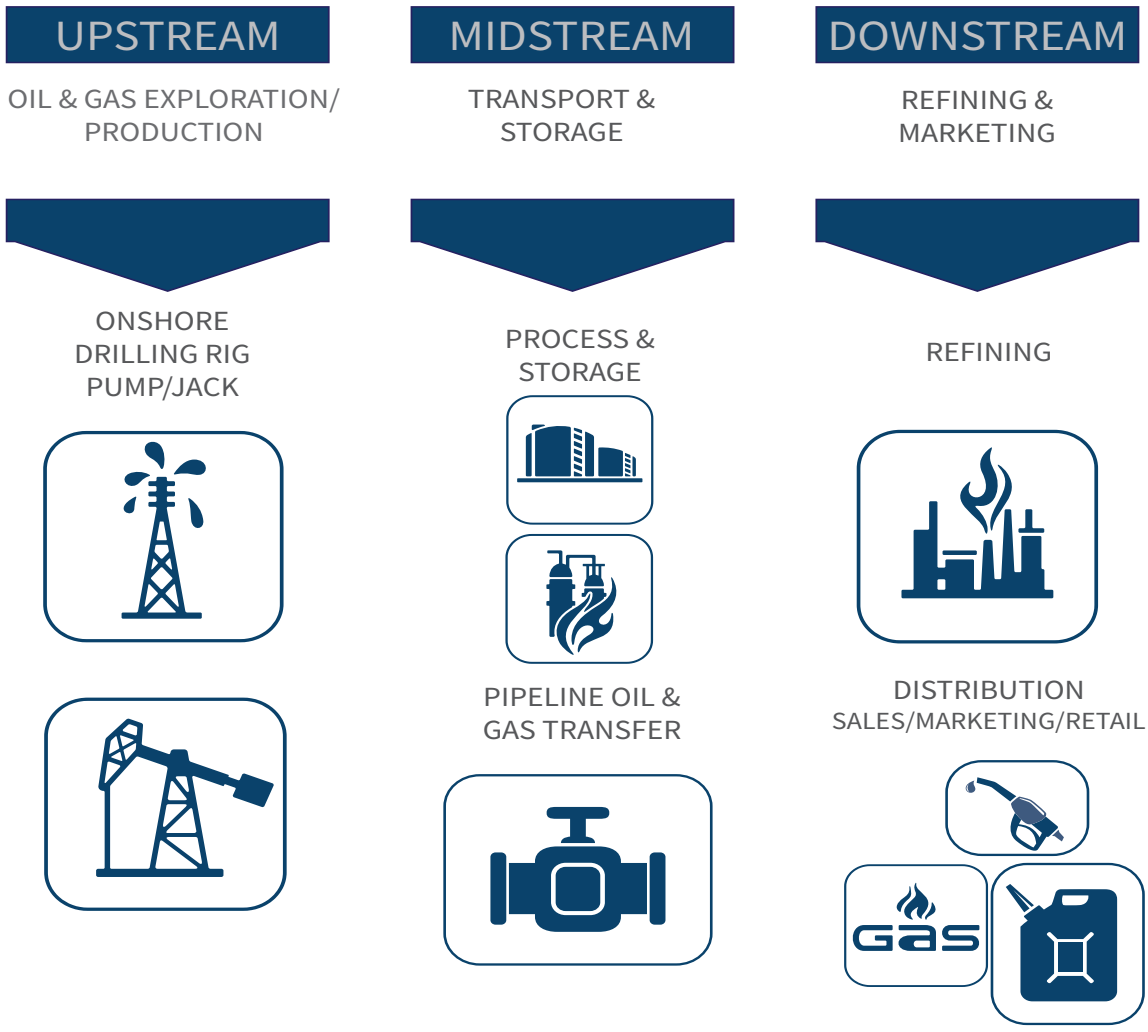


Figure 1.1 - Petroleum and Natural Gas Supply Path

1.2 Statement of the Problem

The problem addressed by this study is the vulnerable cybersecurity structure within petroleum and natural gas companies associated with the CISTAR and P2SAC. There have been reports of heightened threats from cyber criminals focusing upon the energy sector, with recent attacks upon natural gas pipelines and payment centers. CISTAR and P2SAC reached out to the Computer and Information Technology Department to assist with analysis of the current cybersecurity posture of companies involved with CISTAR.

1.3 Significance

Throughout recent years, cyber criminals have shifted focus to the United States energy sector. Energy is considered critical infrastructure, with petroleum and natural gas organizations falling into this category. Many of these organizations are within the private sector and operate autonomously from one another. As of 2017, the United States had "944 oil rigs total, all of which are potential targets for cyber-attacks" (Alpi, 2017). In addition to these on and offshore oil rigs, the United States averages close to 1,000,000 active oil and gas wells, many of which are located in rural or isolated areas with no security. These wells feed processing facilities prior to movement into regional plants. From there, natural gas is transported via pipelines with petroleum making its way to refineries. All of these facilities and/or sites provide cyber-criminals with endless options to orchestrate an effective cyber-attack.

Credible threats exist and recent attacks directed at natural gas companies have heightened awareness of the cyber threat. "In April 2018, new cyberattacks reportedly caused the shutdown of the customer communications systems at four of the nation's largest natural gas

pipeline companies…in January 2019, congressional testimony by the Director of National Intelligence singled out gas pipelines as critical infrastructure vulnerable to cyberattacks which could cause disruption for days to weeks." (U. S. Congress, 2019). Petroleum and natural gas companies can no longer stand idle in regard to cybersecurity and must implement defensive cybersecurity measures in order to thwart potential attackers.

1.4 Research Questions

The following research questions were developed for application toward this research project:

1. Does the age of an organization factor into cyber-attack response time?
2. What extent do CISTAR and P2SAC organizations dedicate resources, both human and monetary, to cybersecurity defenses?
3. Do CISTAR and P2SAC organizations have basic NIST recommended cybersecurity processes in place?

1.5 Purpose

The purpose of this proposed study is to answer all of the research questions and develop the following deliverables:

1. Qualtrics survey containing 27 cybersecurity centric questions for dissemination to CISTAR and P2SAC organizations.
2. Recommendations of cybersecurity improvement areas for distribution to CISTAR and P2SAC leadership.

1.6 Scope

The scope of this research will focus upon the application of cybersecurity practices throughout the petroleum and natural gas companies associated with CISTAR and P2SAC. This research will focus upon cybersecurity shortfalls and gaps within these companies and provide recommendations for improvement.

The research population will consist of cybersecurity professionals employed within the companies associated with CISTAR and P2SAC. The population will not be vast due to the limited number of petroleum and natural gas companies under CISTAR. The sample will consist of employees familiar with the function and structure of a respective company's cybersecurity department. Sampling in this manner will ensure fair data collection regardless of company size.

1.7 Assumptions

For this research to be conducted within the scope previously outlined, it is important to note a few key assumptions must be accepted. These assumptions will be considered true and factual for the remainder of this research project.

Assumptions for this research project are as follows:

1. Qualtrics survey respondents will be familiar with cybersecurity practices of their respective company or organization.
2. Qualtrics survey respondents will provide truthful answers.
3. All Qualtrics survey respondents will be associated with either the petroleum or natural gas industry.

1.8 Limitations

The intent of this research is to analyze and capture cybersecurity weaknesses within the petroleum and natural gas companies associated with CISTAR and P2SAC despite specific limitations. Data collection is reliant upon volunteer participation from CISTAR company employees. The total number of participants was limited by the number of companies within CISTAR, and employees with organizational cybersecurity knowledge, which did not provide an abundance of data for analysis. Also, every CISTAR company may not have an accredited cybersecurity professional employed to implement recommendations from this study.

1.9 Delimitations

This research is limited to cybersecurity within the petroleum and natural gas industries only. Other energy sectors are not being assessed, even though cyber-crime often overlaps throughout various industries. This project is also limited to the companies participating with the CISTAR and P2SAC initiatives and does not encompass petroleum and natural gas companies throughout this country and the world.

CHAPTER 2. REVIEW OF LITERATURE

2.1 Methodologies

The problem with cybersecurity defense is that there is no definitive way to defend against a potential attack. Cyber-criminals are continuously developing new attack vectors to harm all infrastructure with a network connection. These criminals typically choose the path of least resistance when targeting areas for exploitation. Simple steps to defend a network may be the difference between fending off a potential cyber-attack or falling victim. There is a misconception that all cybersecurity defense mechanisms are complicated and difficult to comprehend. This is not the case and many of the defenses available are free to implement, with the only items required being attention to detail and time.

Periodic password changes can boost defenses by cutting off illegal access. If a username/password is compromised, it could go undetected for an infinite amount of time. However, if periodic password changes are enforced by an organization, it could cut off a hacker with illegal access. This type of defense costs nothing to implement, and though tedious, improves network defenses. Administrator accounts with elevated permissions are especially important considering all of the network change privileges tied to these accounts. Normal users throughout a network cannot make significant changes, but a compromised administrator account could be detrimental to the entire network.

Software can also become compromised from time to time, requiring a patch from the developer in order to restore security. Adjusting network settings to automatically push software patches is another free and easy way to defend a network. If criminals gain illegal access through

a software flaw, then lateral movement throughout the rest of the network is possible. Criminals just need an opening to exploit a network, and sometimes it can be unrelated to the actual target.

2.2 Boolean Logic

Literature review focused upon the use of the Engineering Village database throughout the entirety of the project. Engineering Village pools together information from 12 other databases for ease of research, providing access to journals, specific trade publications, government reports and current scholarly articles. However, the initial search strategy proved to be difficult, especially when conducting petroleum or natural gas cybersecurity searches within Engineering Village. Results were dated and not plentiful when using specific cyber search terms. Within Engineering Village, Boolean Logic was changed to include all “or” searches, resulting in numerous sources from recent years, which is important when combating a constantly evolving criminal network. Notable keywords used for searches within all databases are listed in *Figure 2.1*.

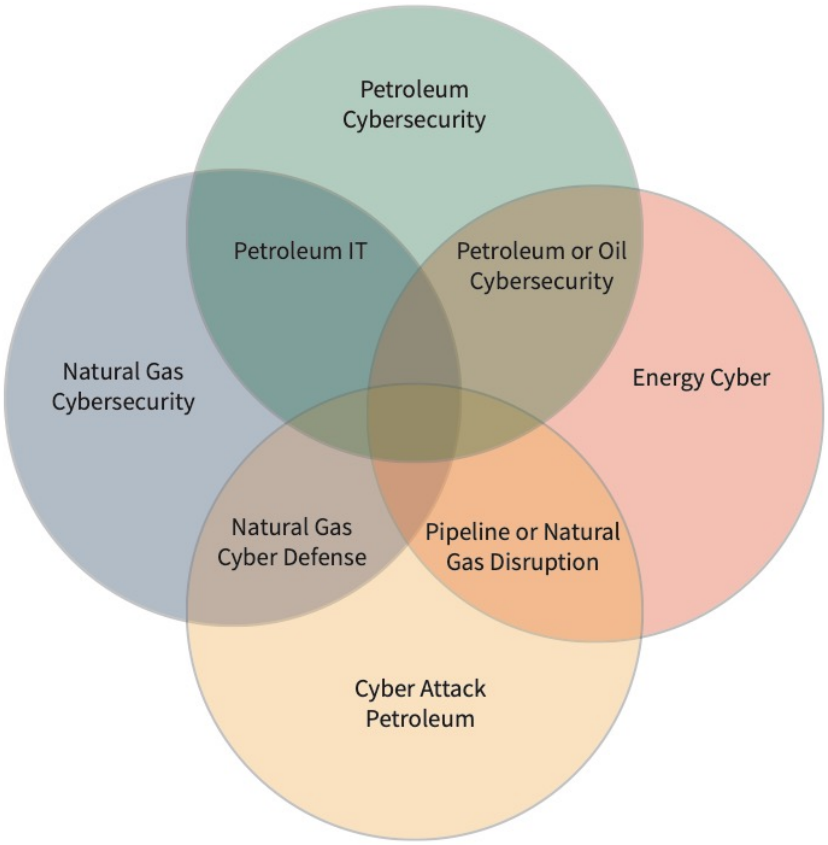


Figure 2.1 - Boolean Logic Venn Diagram

An amended search within Engineering Village was performed for petroleum cybersecurity, or petroleum cyber security, or oil cyber security. This logic change yielded over 1,000 results, many of which were completed in 2018-2019. Due to the continuous changes within cyber, the recent sources help provide an accurate picture of current cyber-criminal activity that will be the focus of defensive cybersecurity actions.

Searches were also conducted for natural gas cybersecurity or natural gas defense. The incorporation of "defense" produced thousands of results, which were then sorted by year. Again, there were several recent sources, but only a few were considered applicable sources. The

term" defense" resulted in protective measures beyond the scope of cyber, but cyber-related results were also discovered using these terms.

The most fruitful search involved cyber-attack petroleum, or petroleum disruption, or natural gas disruption. This logic produced over 10,000 results that were sifted through by year and keyword. Disruptions by either physical or online means are what companies associated with CISTAR and P2SAC are ultimately trying to prevent and insight into how previous disruptions took place assists with development and implementation of strong cyber defenses.

Finally, a search for energy cyber was run without any other logic. No other logic was added to improve results since the cyber relativity was already present after the initial search. Since petroleum and natural gas are often rolled into "energy" as a whole, looking at cyber threats to other energy sectors could offer insight into additional threats or organizational cybersecurity gaps.

IEEE Xplore and ProQuest were other databases used extensively for the review of literature. Similar Boolean Logic was used while searching each database, which provided multiple sources related to the research project. Overall, the ProQuest sources proved to be less dated than those produced by Engineering Village or IEEE Xplore.

2.3 SCADA Systems

As cybersecurity issues continue to become more complex, it has become a necessity for businesses and organizations of all sizes or specialties. Identification of threat vectors and subsequent defense mechanisms are integral steps to successful defensive cybersecurity measures. The ability to effectively identify threats enables an organization to improve its cyber

defenses. An effective example of this approach was developed by Lamp, Rubio-Medrano, Zhao, & Ahn (2019) and appropriately named Exploitation Solutions (*ExSol*) which:

> Works by comparing the potential for exploitation, i.e. threats and attack vectors, versus the implemented solutions, i.e. security features and requirements, in order to understand how much risk the system may contain, allowing for a better understanding of the system state, current threats, attack vectors and vulnerabilities. (p. 1)

While the system created by Lamp et al. may not fit all situations, it serves as a foundational approach that can be tailored to multiple scenarios. Similar systems that compare exploitations to solutions for cyber threat vectors should be in place and utilized by an organization's cybersecurity department.

Supervisory control and data acquisition (SCADA) systems are very popular throughout the petroleum and natural gas industries. Distributed pipelines and facilities, some that are in remote locations, require monitoring systems in order to control operations. To control the distributed well system and regulate the flow of petroleum or natural gas, SCADA and pipeline monitoring systems are in place. These systems are complex and require network connectivity in order to function properly. SCADA systems are vulnerable to cyber-attacks due to network connectivity, and if they are compromised, represent a high risk to organizations. Typical SCADA systems contain supervisory, control and physical layers. All of these layers have network connectivity and could be subject to threats, "broadly classified into four main categories: insiders, hackers, criminal groups and nation-states" (Do, Fillatre, Nikiforov, & Willett, 2017, p. 30). It is important to be mindful of the various threat categories and realize that some of the most effective and dangerous threats may originate from within an organization.

Insiders are familiar with the organizational construct and could possibly be more effective during an attack.

The number of components connected to the network in a typical petroleum or natural gas structure could potentially be overlooked. During an evaluation of a midstream oil terminal, Das & Morris (2018) determined that "the physical system model incorporates 217 sensors and actuators". These sensors and actuators were part of the terminal, which included tank farms, tanker trucks, shipping terminal and 150km of pipeline. The design of the tested terminal will vary at other locations but captured a typical setup for the average petroleum company. Petroleum and gas companies are becoming more reliant upon the internet as they phase out legacy systems and migrate to internal networks to accommodate large scale operations. It is important to focus upon all key points that rely upon network connectivity and be cognizant of the various threats posed to the network. Once a criminal gains access to any portion of the network, they have the ability to move laterally and impact all facets of the entire network.

SCADA systems also protect pipelines from weather disruptions, specifically hurricanes, that impact the petroleum industry. A compromise of the SCADA or network monitoring system could create a service disruption and cost companies exorbitant amounts of money to recover. The federal government is aware of the danger facing these companies and has produced the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity. "Using this framework and other consensus standards can equip upstream operators with the process and tools they need to prevent cyberattacks" (Natural Gas Systems, 2017, p. 14). NIST guidelines are free and updated on a regular basis, so the bulk of research is handled by the federal government. Companies and lesser governmental agencies can build their cybersecurity defenses around NIST practices to protect themselves from an

attack. However, these organizations must have trained cybersecurity personnel that can comprehend and implement the NIST guidelines. Without the appropriate personnel, natural gas and petroleum companies will remain at a higher risk to a cybersecurity breach.

2.4 Foreign Attacks

Foreign businesses are not immune to cybersecurity attacks and have been targeted by cyber-criminals for decades. An attack in 2012 known as Shamoon was carried out against the Saudi Arabian company Saudi Aramco, one of the world's largest producers of petroleum, using malware to wipe data stored on "approximately 30,000 computers. The attack was likely perpetrated by someone with inside access to the company's network and delivered using a small USB drive." (Clayton and Segal, 2013, p. 2). Insider threats can be extremely dangerous and are very difficult to prevent since they are introduced to the network by an employee familiar with company operations. While the attack eliminated the data on tens of thousands of computers within the Saudi Aramco network, costing the company an exorbitant amount of money for replacements, there were no pipeline or production disruptions.

Companies located abroad with United States' partnerships pose an indirect cybersecurity risk. ExxonMobil and Qatar Petroleum jointly operate RasGas within Qatar and were subject to the same Shamoon malware in 2012 that temporarily disabled the company computer systems. At the time, Qatar was the world's largest producer of liquefied natural gas, which likely drew the attention of the responsible threat actors. The Shamoon malware "hit the giant Qatari natural-gas firm and disabled its website and email servers (Clayton and Segal, 2013, p. 5). It is unknown if the Qatari or American company was the intended target, but the alliance formed between the two made it possible for a cybersecurity breach that impacted both sides.

2.5 Natural Gas Importance

The United States "has become the largest producer of natural gas in the world… and the natural gas supply chain is extensive and spans from the production well-head to consumer burner tip" (Natural Gas Systems, 2017, p. 4). Access to domestic energy has kept costs low, increased demand and propelled natural gas to the forefront of a clean fuel initiative. While the aforementioned attributes of natural gas seem positive, there is reason for concern among those familiar with cybersecurity risks. The physical structure of natural gas pipelines and distributed well systems are excellent combatants against disruptions. Many of the pipelines are underground, which is an excellent defense that limits physical access and flow is controlled via the use of compressors. As noted in Judson's (2013) report:

> The natural gas network has few single points of failure that can lead to a system- wide propagating failure. There are a large number of wells, storage is relatively widespread, the transmission system can continue to operate at high pressure even with the failure of half of the compressors, and the distribution network can run unattended and without power. (p. 6)

2.6 Current Threats

Cybersecurity threats are constantly evolving, which makes it difficult to compile an all-encompassing list of cyber threats. When a patch is introduced for vulnerable software, cyber criminals begin working to circumvent the patch. An example is the Trisis/Triton malware variant that first appeared in 2017, targeting a Saudi Arabian petroleum plant. According to Kovacs (2019), Triton "targeted Schneider Electric's Triconex safety instrumented systems (SIS)

through a zero-day vulnerability. The attack was discovered after a SIS triggered a shutdown of some industrial systems". This cyber threat was introduced to the Saudi Arabian company by the cyber-criminal Xenotime, a threat actor that has been tracked by numerous agencies involved with cybersecurity and credited with the Trisis/Triton malware. The malware displayed "incidents of attempted authentication with credential 'stuffing' or using stolen usernames and passwords to try and force entry into target accounts" (Kovacs, 2019). Additionally, there have been reports of a credible threat to the United States energy sector using similar techniques involving SIS from varying manufacturers. Hacking techniques used by this malware are relatively easy to defend against, with defense mechanisms involving strong passwords, regular password change requirements and auditing of compromised usernames.

Many users tend to utilize the same username and password across numerous domains. This becomes a problem when a database or website becomes compromised by hackers. The compromised username and password are then entered into numerous websites until the cyber-criminals successfully gain access to another system. Requiring users or employees to regularly change their passwords would aid in keeping a username and password unique to one database or website. Users are less likely to habitually change their username and password across all domains they visit, thus negating the ability of a cyber-criminal to use the compromised credentials to illegally gain access elsewhere. Other defense techniques include long, complex passwords that are difficult to guess. Finally, enabling some version of automatic account locking following numerous unsuccessful password entries limits the number of times a hacker can attempt to breach an account.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

The problem addressed by this study is the vulnerable cybersecurity structure within petroleum and natural gas companies associated with CISTAR and P2SAC. The purpose of the methodology used for this research project will produce project deliverables that result from the combination of researching current cybersecurity protocols and the application of data collection. The data collected for analysis will be representative of cybersecurity measures in place throughout CISTAR and P2SAC organizations. Once analysis was complete, see *Figure 3.1* for timeline, results were compared to current industry standards to generate the deliverables. Deliverables will be distributed to all organizations throughout CISTAR and P2SAC to assist the respective cybersecurity departments in combating cyber-criminal activity aimed at the petroleum and natural gas industries.

3.2 Research Approach

This research project utilized an online Qualtrics survey to gather data for analysis combined with interviews of professionals associated with CISTAR, P2SAC and Kenexis consulting firm. The survey was disseminated to a distribution list from the CISTAR and P2SAC companies, with hard copy surveys passed out during the 2018 P2SAC conference that also contain a link to the online Qualtrics survey. Paper copy surveys were manually entered into Qualtrics to capture the data and store it at a central location. Additional survey distribution went

to non-CISTAR/P2SAC companies to develop situational awareness on cybersecurity issues within other natural gas and petroleum companies.

Initial data analysis was provided through Qualtrics. Negative trends identified through response analysis were compiled and compared to the current NIST standards. After comparison to NIST standards, the researcher organized a list of cybersecurity recommendations for implementation by CISTAR or P2SAC petroleum and natural gas companies. These recommendations were ranked in order of monetary cost to the company to assist with a phased implementation plan.

3.3 Population and Sample

The research population consists of cybersecurity professionals employed within the companies associated with CISTAR and P2SAC. Due to the varying company sizes, total population size was estimated based upon total number of employees within all cybersecurity departments. A question covering company size is nested within the Qualtrics survey in order to aid population estimate. The population was not vast due to the limited number of petroleum and natural gas companies under the CISTAR and P2SAC initiative.

Company size was determined during data analysis and review of Qualtrics responses. Sampling in this manner will ensure fair data collection and level analyses to produce recommendations applicable to all CISTAR or P2SAC organizations, regardless of the size of respective cybersecurity branches.

3.4 Variables

Variables for this research project did not fall within the realm of traditionally defined dependent or independent variables. The independent variables associated with this study are the presence of a cybersecurity branch and company age. These variables cannot be manipulated within the study since it is reflective of CISTAR companies' current design and history. Dependent variables include varying cybersecurity measures used throughout CISTAR companies, accredited cybersecurity training, and the size of cybersecurity branches.

3.5 Time Action Plan

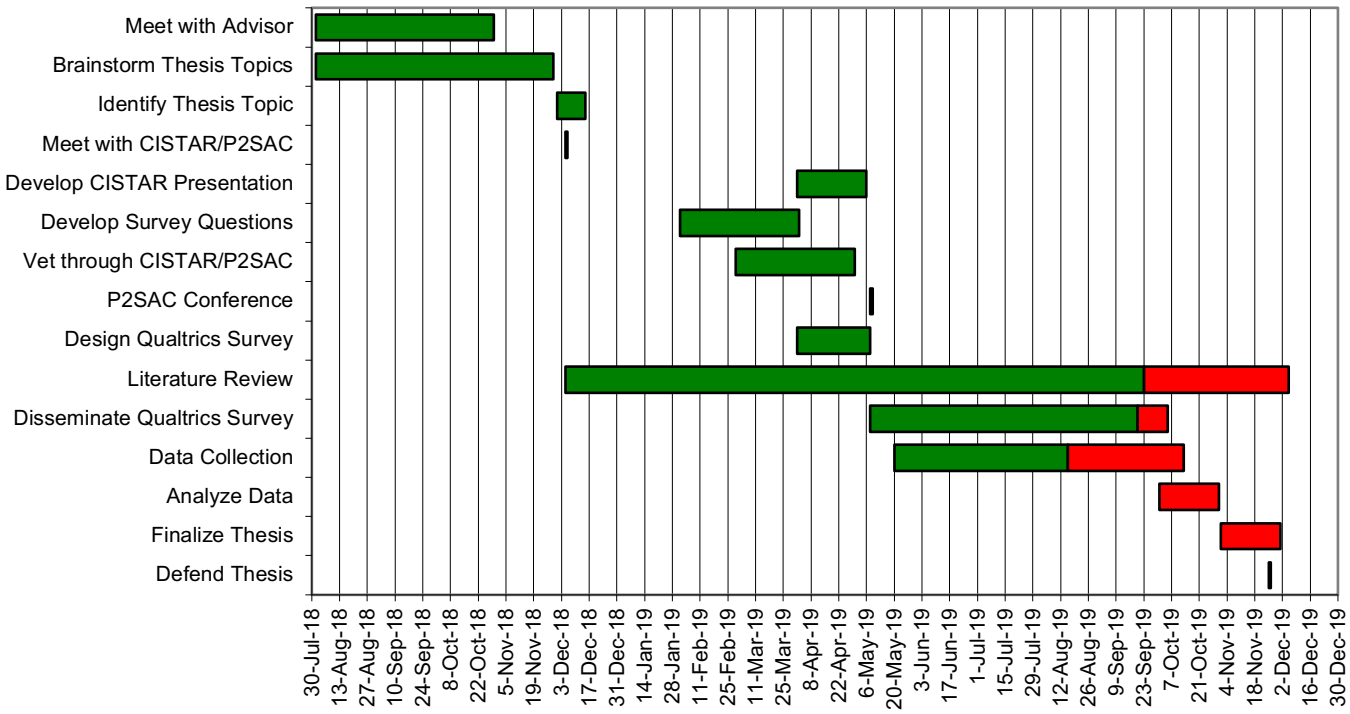


Figure 3.1 - Gantt Chart

3.6 Data Analysis

The quantitative data collected was stored within Qualtrics until collection was complete. Initial analysis involved a Pearson's Chi-Square Test to examine the relationship between the variables "cybersecurity response time" and "age" and the dependent variables (measures, training and size). A one-way ANOVA was applied to examine the number of accredited cybersecurity professionals on staff for each organization.

3.7 Validity and Reliability

The Qualtrics survey was built upon the NIST cybersecurity framework. Basic demographic questions were used in order to establish the industry background of the survey respondents, followed by the remaining questions all based upon NIST standards. Additionally, nearly 75% of the survey questions, excluding demographics, align to the State of Indiana Cybersecurity Scorecard (Lerums, 2018), which was reviewed by the Indiana Director of Cybersecurity Programs.

Logic, application of analyses and overall relevance of the study were consistently reviewed and refined by the researcher's committee members, Purdue statistics department consultant, Associate Director of P2SAC and Director of CISTAR. Reliability of data was supported by Qualtrics, which codes and converts data for use within Statistical Package for the Social Sciences (SPSS). Recoding of survey data within SPSS was kept to a minimum, with all recoding logic confirmed by the Purdue University Department of Statistics.

3.8 Conclusion

Application of the methodology outlined for this research project will produce results that answer all of the research questions. The data collected from this study shall determine the current cybersecurity posture of CISTAR and P2SAC organizations in order to serve as a foundation to build a sound defensive cybersecurity plan. Recommendations for improving cybersecurity will stem from the results of the Qualtrics survey that identify any gaps or weaknesses. Once these vulnerabilities are identified, sound cybersecurity practices will be recommended to CISTAR and P2SAC organizations for implementation and become the initial planning product of a layered cybersecurity defensive plan.

CHAPTER 4. ANALYSIS AND RESULTS

4.1 Overview

The analyses and results contained in this section were collected from 15 usable Qualtrics cybersecurity scorecards. The scorecard was comprised of four numerical scaled questions and 23 nominal scale questions. Responses were then captured within SPSS and recoded to produce data focused upon this research project.

The initial section of the survey contained demographic questions to establish background information on each respondent. Company type, age, size and number of cybersecurity professionals employed were all taken into account as factors that supported the relevant data collected throughout the scorecard. Detailed analysis of the data collected via the scorecard was used to answer the research questions:

1. Does the age of an organization factor into cyber-attack response time?
2. What extent do CISTAR and P2SAC organizations dedicate resources, both human and monetary, to cybersecurity defenses?
3. Do CISTAR and P2SAC organizations have basic NIST recommended cybersecurity processes in place?

Analyses were run within SPSS to provide statistical results from the comparison of survey responses to offer details and correlations on the research questions.

4.2 Qualtrics Survey

The Qualtrics survey used 27 questions, see *Figure 4.1*, for data collection. All survey questions were broken down into three sections: demographics, cybersecurity and physical security. Respondents were all assumed to be sourced from respective organizational cybersecurity branches.

CISTAR Cybersecurity Scorecard

1. Name of organization.
2. When was your organization founded?
3. What most closely resembles your job title?
4. Approximately how many personnel work within your organization (full-time, part-time, contractors)?
5. Approximately how many personnel within the organization have accredited cybersecurity training?
6. What type of facility do you support?
7. What cybersecurity system design practices are in place at your organization?
8. How frequently does your organization audit update current cybersecurity protection measures?
9. Does management allocate a portion of the annual budget for cybersecurity defense?
10. What priority does your organization place upon cybersecurity?
11. How quickly does management respond to cybersecurity breaches?
12. Does your organization track known cybersecurity breaches?
13. How many known cybersecurity breaches occur in a typical year?
14. Do you use multi-factor authentication?
15. What type of multi-factor authentication do you use?
16. Is your facility system network (accessible by computer) monitored to prevent unauthorized access?
17. For well-sites, are procedures in place to prevent unintended or unauthorized changes, damage, or destruction to the system network?
18. Is your well-site designed to permit remote control?
19. Does your well network system contain legacy systems incapable of being updated to meet changing cybersecurity requirements?
20. Are the legacy systems necessary for operations?
21. Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. connected to a publicly available internet systems?
22. Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. periodically monitored for vulnerabilities?
23. Is physical security monitored to prevent unauthorized access to the organization?
24. What type of physical security monitoring system(s) are in place?
25. Are there external barriers/security measures to prevent unauthorized access?
26. Describe the physical conditions of barriers.
27. Does protocol include locking all structures upon exit?

Figure 4.1 - CISTAR Cybersecurity Scorecard Questions

4.3 Demographics

There were 15 participants that took part in this survey. The age of the organizations ranged from 4 to 45 years, with the mean age, $M = 15$, and the standard deviation of 14.41. Overall organizational age was used over the age of respective cybersecurity departments due to the lack of documented origin dates for each cybersecurity branch. The study included cybersecurity professionals from petroleum, natural gas and federal government entities.

Table 4.1 Organization Age and Cyber Response Time

	N	Mean	Std. Deviation	Std. Error Mean
Age	15	14.47	14.41	3.72
Response Time	15	1.47	.83	.22

4.4 Analyses

A Pearson's Chi-Square Test was run to compare cyber-attack response time to the age of an organization, see Table 4.2, which showed marginal differences existed between the expected and observed outcomes within the crosstabulation table, except for response times within 24 hours. 75% of organizations that were four years old took up to 24 hours to initiate a response following a cyber-attack. No other organization, regardless of age, took longer than a few hours, with 100% of organizations 10 years and older responding under an hour. Cramer's $V = .66$, $p = .68$, suggesting a significant, very strong association exists between cyber-attack response time and organizational age.

Table 4.2 Chi-Square Cyber-Attack Response Time and Organization Age Crosstabulation

			Age									
			4	7	9	10	11	12	37	43	45	Total
Response Time	Less than one hour	Count	1	1	3	1	1	1	1	1	1	11
		Expected Count	2.9	.7	2.9	.7	.7	.7	.7	.7	.7	11
	Within few hours	Count	0	0	1	0	0	0	0	0	0	1
		Expected Count	.3	.1	.3	.1	.1	.1	.1	.1	.1	1
	Within 24 hours	Count	3	0	0	0	0	0	0	0	0	3
		Expected Count	.8	.2	.8	.2	.2	.2	.2	.2	.2	3
Total		Count	4	1	4	1	1	1	1	1	1	15
		Expected Count	4	1	4	1	1	1	1	1	1	15

A one-way ANOVA was run to determine if a relationship exists between organizational cybersecurity priority and the total number of employees with accredited cyber training or cybersecurity budget.

There was not a statistically significant difference between groups as demonstrated by the one-way ANOVA ($F(1,13) = .47$, $p = .51$) and ($F(1,13) = .32$, $p = .58$). No significant difference was shown between cybersecurity priority and personnel with accredited cyber training ($p = .51$) or between cybersecurity priority and cybersecurity budget ($p = .58$).

Table 4.3 One-way ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Personnel w/ Accredited Cyber Training	Between Groups	.26	1	.26	.47	.51
	Within Groups	7.08	13	.54		
	Total	7.33	14			
Cybersecurity Budget	Between Groups	.04	1	.04	.32	.58
	Within Groups	1.7	13	.13		
	Total	1.73	14			

4.5 Research Question 1

Does the age of an organization factor into cyber-attack response time?

4.5.1 Answer to Research Question 1

The research data indicates that older organizations respond to cyber-attacks faster than organizations established within the past 10 years. All respondents from organizations 10 years of age and older responded to a cyber-attack in less than an hour, while 44% of organizations less than 10 years of age experienced a delayed response. The relatively new companies that participated in this study accounted for all of the respondents that did not address a known cyber-attack in less than an hour. The data suggests that organizations established less than 10 years ago do not emphasize cybersecurity as much as older companies (established over 10 years ago). Cybersecurity must become a priority for all organizations and a delay of just a few hours to quarantine a known cyber breach could prove extremely costly. Cyber criminals are capable of

exfiltrating large amounts of data in a short period of time, so response times must be kept to a minimum in order to protect an organization's respective network.

4.6 Research Question 2

What extent do CISTAR and P2SAC organizations dedicate resources, both human and monetary, to cybersecurity defenses?

4.6.1 Answer to Research Question 2

The one-way ANOVA did not show that either the number of employees with accredited cyber training or the cybersecurity budget were linked to organizational priority. However, 80% of the organizations included in this study employ four or more cybersecurity professionals with accredited cyber training. The remaining 20% of organizations employed one to four cybersecurity professionals, with all of the companies in this category employing less than 450 individuals. The smaller number of individuals utilizing the network likely requires fewer full-time cybersecurity professionals to defend the network, not ignorance toward cybersecurity.

Among the respondents that completed the Qualtrics survey, 87% stated that their organization allocated a portion of the annual budget for cybersecurity. The remaining 13% were not familiar with the annual budget and did not provide a response. The overwhelming majority of organizations already allocate funds each year toward cybersecurity, which is necessary for adequate defense against cyber-attacks. This study would benefit from further research to examine the size and allocation of funds for each organization's cybersecurity budget. This

would help determine if the budget is adequate for the size of the company and evaluate the effectiveness of the cybersecurity measures in place.

4.7 Research Question 3

Do CISTAR and P2SAC organizations have basic NIST recommended cybersecurity processes in place?

4.7.1 Answer to Research Question 3

Strictly reviewing NIST recommendations to improve cybersecurity posture, question #3 within the scorecard addressed current cybersecurity defensive measures in place. Question #14 was also used for this research question since it addressed the use of multi-factor authentication, which is another advanced method of authenticating users and covered by NIST Special Publication 800-63B. Data analysis showed that all organizations within this study utilize varying degrees of recommended industry defense methods. Scorecard data analysis produced the following:

1. 93% of organizations have a layered cybersecurity defense
2. 93% of organizations use multi-factor authentication
3. 100% of organizations utilize a firewall
4. 80% of organizations utilize a DMZ
5. 73% of organizations utilize virtual machines

Basic NIST cybersecurity processes are in place, with the overwhelming majority of organizations using a layered cyber defense strategy. This implies that foundational

cybersecurity fundamentals are in place within the organizations that participated in this study. Additional research would be necessary in order to examine the details of each company's cybersecurity program to assess whether these processes are not only in place, but properly executed and monitored by the cybersecurity branch.

CHAPTER 5. SUMMARY AND RECOMMENDATIONS

5.1 Overview

Collection of data was conducted via mixed methods: Qualtrics survey, phone interviews and meetings with cybersecurity professionals. The focus of the cybersecurity recommendations within this section are directed toward remote, unmanned facilities located within the petroleum and natural gas infrastructure. These facilities are often controlled off-site, and cyber-criminals could potentially introduce pipeline disruptions or system failure during a network breach. Response times would be slowed due to the proximity of the facility and increase response time or the conduct of cyber forensics.

Many of the organizations contained within the results of the Qualtrics survey indicate varying degrees of defensive cybersecurity measures are in place. However, defense in depth is the key to thwarting off a cyber-attack and transforming a network into a hard target. Hackers are more apt to move on from a network if they encounter multiple layers of cybersecurity. Additionally, many cyber-attacks occur due to ignorance or the lack of implementing protocols already adopted by an organization.

The following recommendations are foundational items provided by NIST as best practices. The recommendations are not all inclusive and cybersecurity professionals associated with CISTAR and P2SAC should familiarize themselves with NIST publications. An appendix has been provided to assist organizations with locating popular NIST publications, specifically the ones referenced within this study. There are multiple methods to improve cybersecurity that are free to accomplish and simply need enforcement by an organization's cybersecurity team. Other defensive measures require either an upfront cost, maintenance cost, or both, but typically

offer more advanced cybersecurity. Organizations with cybersecurity budgets can outsource cyber-related items to consulting firms or companies specializing in cloud-based services. This route reduces the physical footprint required to house servers and hardware.

5.2 Password Requirements

Establishment of password length and mandating regular password changes are two cost efficient methods to bolster network defenses. CISTAR and P2SAC organizations should develop policy that outlines both of these password related items, tasking the cybersecurity department with password enforcement. NIST recommendations for passwords set by humans is a minimum of eight characters (National Institute of Standards and Technology, 2017). However, given the power of modern computing, other well-known cybersecurity professionals recommend the use of passphrases, wherever possible. Passphrases are deemed to be more secure and difficult to crack by cyber criminals, offering a higher level of protection.

If the use of a passphrase is untenable, ensure that procedures are put in place to best defend a password from compromise. Granting password entries up to 10 times prior to locking out an account offers protection against password cracking, but also enables the owner of the credentials an opportunity to correctly enter a password. During an interview with Jim McGlone from Kenexis Consulting Corporation on October 3, 2019, he suggested implementing passwords that “use rules that allow for several words and numbers to be used without disallowing every repeat, using simple schemas”. The simplification of schemas produces a combination of number and letter sequences that a user can easily remember, rather than passwords that exceed 10 characters of random letters, numbers and symbols. Employees typically prefer to choose their own passwords for the sake of memory, but computer-generated

passwords are also welcomed, and usually offer better protection against password theft due to the random use of characters. Taking that into account, passwords should be compared to dictionary words, disallowing words found within the dictionary. These types of words are used by password crackers to compromise passwords and should not be contained within credentials.

5.2.1 Password Best Practices

NIST no longer recommends changing passwords periodically, now recommending "no password expiration period" (National Institute of Standards and Technology, 2019). Password change requirements were forcing users to create very similar passwords, with the only change often being the addition of an extra character. Others would write down passwords or save them online, which defeats the purpose of changing it to gain increased protection. Modern password advice also includes elimination of password hints. Users are prone to entering very obvious password hints, which can be guessed by hackers. Typically, there is no limit to password entry when using a hint, so cyber criminals can enter an unlimited number of passwords to crack the password. Finally, very similar to hints, are knowledge-based questions. Many websites utilize knowledge-based questions for password recovery, which typically include your date of birth of nickname. These types of questions are often nested somewhere else online, especially with the high use of social media throughout society. Criminals can use information extracted from other websites in order to guess a password, and this process is made much easier when there is a direct question in place to aid password recovery.

5.2.2 Credential Audits

Another safe practice regarding username and password credentials involves the removal of access once an employee no longer works for an organization. Procedures should be in place to suspend or remove system access for employees upon completion of their employment term. Network or system access suspension should become part of out-processing to ensure it is not overlooked. Suspending access for ex-employees will prevent a form of insider attack where the former employee accesses the network using their credentials to harm the organization. Insider attacks pose a serious risk to organizations due to network familiarity by the attacker and can go undetected for significant periods of time. Finally, auditing for stale credentials should occur regularly to ensure access is limited to those that require it. As previously suggested, a compromised account may go unnoticed for an indefinite period of time unless a password change takes place. This cuts off unauthorized access and the same methods apply to stale credentials. If a former employee had their credentials compromised, then moves on from the organization, a potential cyber-criminal could retain unauthorized access to a network or system. Severing network access to former employees or conducting regular audits of credentials makes certain that only those that require network access receive it.

5.3 Patch Cycles

Businesses and organizations must have a system in place to identify and implement software patches. Microsoft releases software patches and updates every Tuesday of the week, so a similar policy is imperative to stay abreast of current software vulnerabilities. Patches released by large software companies have been tested prior to release, however, that does not mean that

all patches are prepared for immediate introduction to a network. “It is always recommended that organizations duplicate the operations environment with absolute functional fidelity, but issues associated with component cost and test space may limit the ability of the organization to have a fully functional test unit” (Department of Homeland Security, 2008). If a test environment is unavailable, the patch should not be loaded onto all machines simultaneously. Identify one machine to use for patch testing and monitor performance following the update. This will minimize network degradation and possible disruptions due to unforeseen patch interface. According to NIST (2013), this process is referred to as a “phased approach” and is best to deploy patches to “standardized desktop systems and single-platform server farms of similarly configured servers”.

Prior to any patch being put onto a network, there should be a determination of the severity or risk associated with the respective program requiring the software patch. For instance, if a virus is present on networks used by other petroleum or natural gas companies and specifically targets the energy sector, then a patch to prevent this virus would become urgent. Many patches are made available prior to any compromises taking place, however, that is not always the case. If a breach has already taken place by exploiting a vulnerability within a program, then it is likely that the hacker or threat group will continue probing other networks for the same gap. This would be a time to recommend an off-cycle patch to push the patch(es) as soon as possible. The timeline for an off-cycle update will be compressed due to the urgency of the threat, and *Figure 5.1* depicts the recommended actions by the Department of Homeland Security (2008):

1. Where possible, create a backup/archive and verify its integrity by deploying it on a standby system.
2. Create a checklist/procedure for patch activities and deploy the patch on the standby system.
3. Test the patched standby system for operational functionality and compatibility with other resident applications.
4. Swap the patched standby system into production and keep the previous unpatched production system as a standby for emergency patch regression.
5. Closely monitor the patched production system for any issues not identified during testing.
6. Patch the standby system (old production) after confidence is established with the production unit.
7. Update software configuration management plan and related records.

Figure 5.1 - Off-cycle Patch Checklist

5.4 Antivirus Software

Antivirus software serves as an obvious defensive measure to prevent malware, spyware and viruses. There are numerous reputable antivirus companies available to provide software tailored to specific organizational needs. NIST recommends utilization of antivirus software as a popular choice for threat mitigation and *Figure 5.2* outlines the recommended antivirus capabilities by the National Institute of Standards and Technology (July 2013):

1. Scanning critical host components such as startup files and boot records.
2. Watching real-time activities on hosts to check for suspicious activity; a common example is scanning all email attachments for known malware as emails are sent and received. Antivirus software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.
3. Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software. Antivirus software should monitor activity involving the applications most likely to be used to infect hosts or spread malware to other hosts.
4. Scanning files for known malware. Antivirus software on hosts should be configured to scan all hard drives regularly to identify any file system infections and, optionally, depending on organization security needs, to scan removable media inserted into the host before allowing its use. Users should also be able to launch a scan manually as needed, which is known as on- demand scanning.
5. Identifying common types of malware as well as attacker tools.
6. Disinfecting files, which refers to removing malware from within a file, and quarantining files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored; however, many infected files cannot be disinfected. Accordingly, antivirus software should be configured to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected.

Figure 5.2 - Recommended Antivirus Capabilities

5.5 Two-factor Authentication

The implementation of two-factor authentication provides an excellent means of advancing defensive cybersecurity and if not already in place, examined by CISTAR and P2SAC stakeholders. The basis of the added protection involves adding a second layer of verification for identity authentication. The fundamentals of two-factor authentication involve the following:

something you know (knowledge), something you have (possession) and something you are (inherence).

Typically, this type of authentication is not 100% cost-free and requires an investment in order to create a second means of authentication. Username and password credentials do not cost anything and generally serve as the initial means for accessing a network or system. The second layer of defense can be accomplished through possession or biometrics. Typically, possession items include a smart card, security token or smart phone with an application such as Steam, LastPass or Duos. Google and Microsoft also offer their own application-based verification methods and selection comes down to organizational preference.

Finally, biometrics can be used as the second layer of authentication. This is by far the most expensive verification option due to equipment costs. Facial recognition, retina scans, or fingerprint scanning are popular means to validate identity using biometrics, all of which are unique to each individual user. While the monetary investment for biometric screening is quite high, the cost can be justified by providing identity confirmation that is incredibly difficult to replicate or compromise.

5.6 Demilitarized Zone

A demilitarized zone (DMZ) within cyberspace is much different in construct than that of the military, but the underlying concept is similar. The focus of a military-centric DMZ is the removal of military personnel. This removal of troops makes the area safer and less prone to armed conflict. A cyberspace DMZ focuses upon removal or prevention of access by malicious cyber-attackers that could potentially infiltrate an organization's network to introduce dangerous

crippling viruses or malware. The DMZ is put in place to prevent an attack, whether the context is military operations or cyberspace.

A DMZ offers excellent protection to a local area network (LAN). If cyber-criminals are successful in compromising a server located within the DMZ, they are restricted from accessing the remainder of the network. A firewall is in place between the server located within the DMZ and other servers upon the LAN, which would block malicious attempts by attackers to access. This limits connectivity to safeguard the network but does not limit connectivity between hosts within the DMZ and the internet. Web and email servers require internet connectivity to function but pose the biggest threat to the majority of LANs.

A DMZ is often an additional firewall for external facing servers. A firewall will be established between servers within the DMZ and external network connections. A second firewall is setup between the DMZ and the remaining LAN servers. The second firewall forces potential cyber-criminals to work harder to breach a network and provides additional time for identification by a network intrusion or monitoring device. The added workload placed upon hypothetical attackers is an excellent defensive technique and usually prompts them to move on to a less defended network. Finally, a subnet behind a DMZ offers further protection against cyber-criminals. “Subnetting the DMZ by clustering assets of similar functionality enhances the resiliency and reduces the attack surface” (ICS Cybersecurity, 2019). The concept of a subnet breaks the organizational network into smaller sections, which creates a type of defense in depth. This complements the comprehensive layer of protection analysis (LOPA) that analyzes and assesses risk. Cyber threats are no different and must be incorporated into LOPA moving forward as well as developing layered defenses to prevent cybersecurity attacks.

DMZs are becoming less popular within the cybersecurity industry. They were once the go-to method to secure LANs, but as cloud-based services have evolved, DMZs have dipped in popularity. A DMZ is internally hosted, where cloud-based services are not, minimizing server space requirements and maintenance. Options available on the cloud come at a financial cost but do offer firewall protection through the cloud provider and reduce network configuration requirements.

5.7 Mandatory Training

Requirements should be put in place that outline training courses for cybersecurity personnel. Employees within the cybersecurity branch should have experience or training directly related to cyberspace. Foundational knowledge on cyberspace operations is a necessity to understand the functionality and structure of a network. This knowledge can then be applied to building or growing defensive mechanisms to prevent or defeat a cyber-attack.

An undergraduate degree within cybersecurity is an excellent starting point to screen potential employees. Most universities cover similar information under a cybersecurity curriculum and finding a cybersecurity major at a four-year university is still a rarity. An increasing number of four-year institutions are offering cybersecurity as a major field of study, which is a sign of the importance placed upon cyber by major companies. However, a four-year degree within cybersecurity is not mandatory to fully understand cyberspace and fill a cybersecurity position.

Implementation of cyber course completion requirements ensures that personnel have adequate knowledge to oversee the maintenance and defense of a network. Cyberspace is constantly evolving, both in terms of threats and vulnerabilities. Hackers systematically refine

their techniques to find a weakness within software or network defenses. Once an exploit is discovered, use of that threat vector spreads quickly among cyber criminals. It is imperative that cybersecurity professionals are properly trained and possess the skillset to quickly implement protective measures against emerging threats. Courses such at CompTIA A+, Network+ and Security+ provide basic information technology fundamentals that serve as foundational knowledge for the understanding of a network. According to Madden (2019) "CompTIA certifications are some of the industry's most sought-after certifications because the Department of Defense requires several for nearly any IT related position".

Certifications are awarded for successfully passing an examination for each of the respective CompTIA courses and serve as feeders into more advanced certification courses like CompTIA Advanced Security Practitioner Plus (CASP+), Penetration Testing Plus (PenTest+) and Certified Ethical Hacker. CASP+ and PenTest+ are follow-on courses that could be levied upon employees that are overseeing either management positions within the cybersecurity team or tasked with serving on a vulnerability assessment team that attempts to penetrate an organization's network, providing details on how it was accomplished to improve defenses.

Advanced training courses such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) are excellent management certifications. Developing job descriptions and advertisements that either require these certifications or outline a mandatory timeline for completion, such as within one year of hire, also improve a cybersecurity team. Both CISSP and CISM require investments of time and money from the individual pursuing the certification, and budgeting to cover the cost of sending employees to a one-week training course helps take the financial burden of achieving certifications off of employees. CISSP and CISM courses are offered throughout the year at

various locations and like all accredited certifications, require renewal every 2-3 years. Renewal typically involves passing a certification test, which exposes students to changes and updates that may have been imposed since they last certified their training.

5.8 Red Team Use

Red team testing is a high-level process of network penetration testing. Red teams are not hackers, but rather members either employed within a company or outsourced to another trusted cybersecurity company. An individual participating on a red team takes on the appearance of a hacker attempting to infiltrate your network, then provides feedback on specific areas to detect, prevent and reduce network vulnerabilities. By taking on the appearance of a hacker, a red team will simulate real-world cyber-attacks using current threats in an attempt to infiltrate a network. Phishing emails are a common practice used by a red team which demonstrates a “click rate” of employees. Employees are one of the most vulnerable pieces of a network and lack of education regarding phishing emails often causes them to click on hyperlinks, leading to fake websites requesting sensitive information. Results from a red team can shape training requirements for employees and identify network vulnerabilities.

APPENDIX A. CISTAR CYBERSECURITY SCORECARD

Petroleum Cybersecurity Scorecard

Start of Block: Demographics

Q1 Name of organization

_____

Q2 When was your organization founded?

_____

Q3 What most closely resembles your job title?

- ○ Cybersecurity / Cyber Operations Personnel
- ○ Chief Security Officer
- ○ Information Technology Personnel
- ○ Operations Technology Personnel
- ○ Risk Management Personnel
- ○ Other _____

Q4 Approximately how many personnel work within your organization (full-time, part-time, contractors)?

_____

Q5 Approximately how many personnel within the organization have accredited cybersecurity training?

- ○ None
- ○ 1-2
- ○ 3-4
- ○ More than 4

Q6 What type of facility do you support?

- ○ Centralized (Refinery)
- ○ Regional (Central processing facility, storage facility)
- ○ Distributed (Well site)
- ○ All of the above
- ○ Other _____

End of Block: Demographics

Start of Block: Emergency Plan and Response (Cybersecurity)

Q7 What cybersecurity system design practices are in place at your organization?

- [ ] Firewall
- [ ] DMZ (Demilitarized Zone)
- [ ] Virtual Machines
- [ ] None
- [ ] Other _____

Q8 How frequently does your organization audit update current cybersecurity protection measures?

- ○ Never
- ○ Yearly
- ○ Monthly
- ○ Weekly

Q9 Does management allocate a portion of the annual budget for cybersecurity defense?

- ○ Yes
- ○ I don't know
- ○ No

Q10 What priority does your organization place upon cybersecurity?

- ○ High
- ○ Moderate
- ○ Low

Q11 How quickly does management respond to cybersecurity breaches?

- ○ Immediately
- ○ Within a few hours
- ○ Within 24 hours
- ○ More than 24 hours
- ○ I don't know

Q12 Does your organization track known cybersecurity breaches?

- ○ Yes
- ○ Maybe
- ○ No

Q13 How many known cybersecurity breaches occur in a typical year?

_____

Q14 Do you use multi-factor authentication? (Ex. password, token, biometrics)

- ○ Yes
- ○ I don't know
- ○ No

Q15 What type of multi-factor authentication do you use?

- ○ Something you know (Ex. password, code word, PIN)
- ○ Something you have (Ex. keys, smart card, token)
- ○ Something you are (Ex. fingerprints, facial recognition, retina scan)

Q16 Is your facility system network (accessible by computer) monitored to prevent unauthorized access?

- ○ Yes
- ○ Maybe
- ○ No

Q17 For well-sites, are procedures in place to prevent unintended or unauthorized changes, damage or destruction to the system network?

- ○ Definitely yes
- ○ Probably yes
- ○ Might or might not
- ○ Probably not
- ○ Definitely not

Q18 Is your well-site designed to permit remote control?

- ○ Yes
- ○ Maybe
- ○ No

Q19 Does your well network system contain legacy systems incapable of being updated to meet changing cybersecurity requirements? (Windows XP, outdated Mac OS, unsupported software, etc)

- ○ Yes
- ○ I don't know
- ○ No

Q20 Are the legacy systems necessary for operations? (Windows XP, outdated Mac OS, unsupported software, etc)

- ○ Yes
- ○ Maybe
- ○ No

Q21 Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. connected to a publicly available internet system?

- ○ Yes
- ○ I don't know
- ○ No

Q22 Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. periodically monitored for vulnerabilities?

- ○ Definitely yes
- ○ Probably yes
- ○ Might or might not
- ○ Probably not
- ○ Definitely not

End of Block: Emergency Plan and Response (Cybersecurity)

Start of Block: Physical Security

Q23 Is physical security monitored to prevent unauthorized access to the organization?

- ○ Yes
- ○ Maybe
- ○ No

Q24 What type of physical security monitoring system(s) are in place? Select all that apply

- ☐ Cameras
- ☐ Security guard
- ☐ Access control point
- ☐ Alarm
- ☐ Other _____

Q25 Are there external barriers/security measures to prevent unauthorized access?

- ○ Yes
- ○ I don't know
- ○ No

Q26 Describe the physical condition of barriers.

- ○ Good
- ○ Bad
- ○ Other _____

Q27 Does protocol include locking all structures upon exit?

- ○ Definitely yes
- ○ Probably yes
- ○ Unknown
- ○ Probably not
- ○ Definitely not

End of Block: Physical Security

Start of Block: Thank you

Q28 Thank you for taking this survey. Your results will contribute to the overall study. Clicking forward will give you the option to print the results for your records.

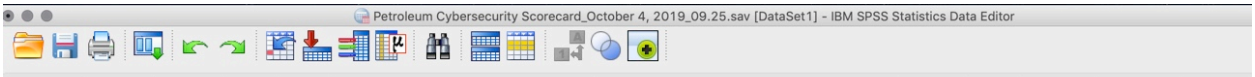
End of Block: Thank you

APPENDIX B. SCORECARD ALIGNMENT WITH NIST FRAMEWORK

CISTAR Cybersecurity Scorecard Question	NIST Framework Aspect	NIST Framework Concern
Demographic Questions 1-6 1. Name of organization 2. When was your organization founded? 3. What most closely resembles your job title? 4. Approximately how many personnel work within your organization? 5. Approximately how many personnel within the organization have accredited cybersecurity training? 6. What type of facility do you support?		
7. What cybersecurity system design practices are in place at your organization?	Trustworthiness Trustworthiness	Privacy Security
8. How frequently does your organization audit update current cybersecurity protection measures?	Trustworthiness Trustworthiness Trustworthiness Trustworthiness	Business Policy Resilience Security
9. Does management allocate a portion of the annual budget for cybersecurity defense?	Business Functional	Cost Sensing
10. What priority does your organization place upon cybersecurity?	Business Lifecycle	Utility Maintainability
11. How quickly does management resond to cybersecurity breaches?	Functional Lifecycle Timing	Performance Maintainability Logical Time
12. Does your organization track known cybersecurity breaches?	Data	Operations On Data
13. How many known cybersecurity breaches occur in a typical year?	Business Functional	Cost Monitorability
14. Do you use multi-factor authentication?	Data Human	Identity Usability
15. What type of multi-factor authentication do you use?	Data Human	Identity Usability
16. Is your facility system network (accessible by computer) monitored to prevent unauthorized access?	Functional Functional	Monitorability Sensing

17. For well-sites, are procedures in place to prevent unintended or unauthorized changes, damage or destruction to the system network?	Functional Trustworthiness	Controllability Security
18. Is your well-site designed to permit remote control?	Boundaries Functional	Networkability Communication
19. Does your well network system contain legacy systems incapable of being updated to meet changing cybersecurity requirements?	Functional Lifecycle	Performance Operability
20. Are the legacy systems necessary for operations?	Functional Lifecycle	Performance Operability
21. Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. connected to publicly available internet system?	Business Functional Functional	Regulatory Monitorability Sensing
22. Are smart devices such as security cameras, thermostats, HVAC, alarm systems, etc. periodically monitored for vulnerabilities?	Functional Trustworthiness	Monitorability Security
23. Is physical security monitored to prevent unauthorized access to the organization?	Functional Functional	Physical Physical Context
24. What type of physical security monitoring system(s) are in place?	Functional Functional	Monitorability Physical
25. Are there external barriers/security measures to prevent unauthorized access?	Boundaries	Responsibility
26. Describe the physical condition of barriers.	Business Functional	Environment Physical
27. Does protocol include locking all structures upon exit?	Functional Human Human	Contollability Human Factors Usability

APPENDIX C. SCORECARD SPSS DATA



	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Q1	String	2000	0	Organization	None	None	15	Left	Nominal	Input
2	Q2	String	2000	0	Organization Founded	None	None	15	Left	Nominal	Input
3	Q3	Numeric	40	0	Job Title	{1, Cybersecurity / Cyber Operations Personnel}...	None	5	Right	Scale	Input
4	Q3_6_TEXT	String	2000	0	Job Title (Other)	None	None	15	Left	Nominal	Input
5	Q4	String	2000	0	Total Personnel	None	None	15	Left	Nominal	Input
6	Q5	Numeric	40	0	Personnel w/ Accredited Cyber	{1, None}...	None	5	Right	Scale	Input
7	Q6	Numeric	40	0	Facility Type	{1, Centralized (Refinery)}...	None	5	Right	Scale	Input
8	Q6_5_TEXT	String	2000	0	Facility Type (Other)	None	None	15	Left	Nominal	Input
9	Q7_1	Numeric	40	0	Cybersecurity in Place (Firewall)	{1, Firewall}...	None	5	Right	Scale	Input
10	Q7_2	Numeric	40	0	Cybersecurity in Place (DMZ)	{1, DMZ (Demilitarized Zone)}...	None	5	Right	Scale	Input
11	Q7_3	Numeric	40	0	Cybersecurity in Place (Virtual Machines)	{1, Virtual Machines}...	None	5	Right	Scale	Input
12	Q7_4	Numeric	40	0	Cybersecurity in Place (None)	{1, None}...	None	5	Right	Scale	Input
13	Q7_5	Numeric	40	0	Cybersecurity in Place (Other)	{1, Other}...	None	5	Right	Scale	Input
14	Q7_5_TEXT	String	2000	0	Cybersecurity in Place (Free Text)	None	None	15	Left	Nominal	Input
15	Q8	Numeric	40	0	Org Update Cybersecurity Measures	{1, Never}...	None	5	Right	Scale	Input
16	Q9	Numeric	40	0	Cybersecurity Budget?	{1, Yes}...	None	5	Right	Scale	Input
17	Q10	Numeric	40	0	Cybersecurity Priority	{1, High}...	None	5	Right	Scale	Input
18	Q11	Numeric	40	0	Cyber Breach Response Time	{1, Immediately}...	None	5	Right	Scale	Input
19	Q12	Numeric	40	0	Org Track Cyber Breaches	{1, Yes}...	None	5	Right	Scale	Input
20	Q13	String	2000	0	Cyber Breaches per Year	None	None	15	Left	Nominal	Input
21	Q14	Numeric	40	0	Multi-factor Authentication?	{1, Yes}...	None	5	Right	Scale	Input
22	Q15_1	Numeric	40	0	Multi-factor (Something you know)	{1, Something you know (Ex. password, code word, PIN)}...	None	5	Right	Scale	Input
23	Q15_2	Numeric	40	0	Multi-factor (Something you have)	{1, Something you have (Ex. keys, smart card, token)}...	None	5	Right	Scale	Input
24	Q15_3	Numeric	40	0	Multi-factor (Something you are)	{1, Something you are (Ex. fingerprints, facial recognition, ret...	None	5	Right	Scale	Input
25	Q16	Numeric	40	0	Facility network monitored for unauthorized access?	{1, Yes}...	None	5	Right	Scale	Input
26	Q17	Numeric	40	0	Well-site network monitored for unauthorized access?	{1, Definitely yes}...	None	5	Right	Scale	Input
27	Q18	Numeric	40	0	Well-site remote access?	{1, Yes}...	None	5	Right	Scale	Input
28	Q19	Numeric	40	0	Network contain legacy systems?	{1, Yes}...	None	5	Right	Scale	Input
29	Q20	Numeric	40	0	Legacy systems necessary for ops?	{1, Yes}...	None	5	Right	Scale	Input
30	Q21	Numeric	40	0	Smart devices on network?	{1, Yes}...	None	5	Right	Scale	Input
31	Q22	Numeric	40	0	Smart devices monitored for breaches?	{1, Definitely yes}...	None	5	Right	Scale	Input
32	Q23	Numeric	40	0	Physical security monitored?	{1, Yes}...	None	5	Right	Scale	Input
33	Q24_1	Numeric	40	0	Physical security (camera)	{1, Cameras}...	None	5	Right	Scale	Input
34	Q24_2	Numeric	40	0	Physical security (security guard)	{1, Security guard}...	None	5	Right	Scale	Input
35	Q24_3	Numeric	40	0	Physical security (access control point)	{1, Access control point}...	None	5	Right	Scale	Input
36	Q24_4	Numeric	40	0	Physical security (alarm)	{1, Alarm}...	None	5	Right	Scale	Input
37	Q24_5	Numeric	40	0	Physical security (Other)	{1, Other}...	None	5	Right	Scale	Input
38	Q24_5_TEXT	String	2000	0	Physical security (Other text)	None	None	15	Left	Nominal	Input
39	Q25	Numeric	40	0	External barriers in place?	{1, Yes}...	None	5	Right	Scale	Input
40	Q26	Numeric	40	0	Barrier condition	{1, Good}...	None	5	Right	Scale	Input
41	Q26_3_TEXT	String	2000	0	Barrier condition (Other)	None	None	15	Left	Nominal	Input
42	Q27	Numeric	40	0	Protocol include locking at exit?	{1, Definitely yes}...	None	5	Right	Scale	Input
43	Q24_5_TEX...	String	255	0	Q24_5_TEXT - Sentiment	None	None	15	Left	Nominal	Input
44	Q24_5_TEX...	Numeric	40	2	Q24_5_TEXT - Sentiment Score	None	None	5	Right	Scale	Input
45	Q24_5_TEX...	Numeric	40	2	Q24_5_TEXT - Sentiment Polarity	None	None	5	Right	Scale	Input
46	Q24_5_TEX...	String	255	0	Q24_5_TEXT - Topics	None	None	15	Left	Nominal	Input
47	Q24_5_TEX...	String	255	0	Q24_5_TEXT - Parent Topics	None	None	15	Left	Nominal	Input
48	Organizatio...	Numeric	8	2	Age	None	None	18	Right	Scale	Input

APPENDIX D. CYBERSECURITY QUICK REFERENCE GUIDE

CYBERSECURITY QUICK REFERENCE GUIDE

Cybersecurity Area	Reference
Biometric Specifications	NIST Special Publication 800-76-2
Cryptographic Key Generation	NIST Special Publication 800-133, Rev. 1
Cyber-Physical Framework	NIST Special Publication 1500-201
Cyber Risk Management	NIST Special Publication 800-39
Digital Identity Guidelines	NIST Special Publication 800-63B
Information Security Handbook	NIST Special Publication 800-100
Interconnected IT Systems	NIST Special Publication 800-47
Malware Prevention	NIST Special Publication 800-83, Rev. 1
Patch Management	NIST Special Publication 80-40, Rev. 3
Public Cloud Computing	NIST Special Publication 800-144
Public Web Server Security	NIST Special Publication 800-44, Ver. 2
Security and Privacy Controls	NIST Special Publication 800 - 53
Software Patch Management	DHS National Cyber Security Division

APPENDIX E. PURDUE INSTITUTIONAL REVIEW BOARD APPROVAL

PURDUE UNIVERSITY

HUMAN RESEARCH PROTECTION PROGRAM
INSTITUTIONAL REVIEW BOARDS

To: J. Eric Dietz

From: Purdue University Human Research Protections Program (HRPP)

Title: CISTAR Cybersecurity Scorecard

Date: 04-30-2019

Re: PROPEL Determination-Not Human Subjects Research

Through the answers you provided in response to questions in the Purdue Research Online Portal Exemption Logic (PROPEL), Purdue's HRPP has determined that the research does not qualify as Human Subjects Research under federal human subjects research regulations (e.g., 45 CFR 46).

The answers provided in PROPEL indicate that you will NOT:

- Collect data for the purpose of research intended to create generalizable knowledge. Reasons that are not considered research include purposes such as internal programmatic evaluation, quality improvement, or business analysis.
- Involve Human Subjects by collecting data from a living individual through intervention or interaction with the individual and/or identifiable private information.

What are your responsibilities now, as you move forward?

- If you have further questions about this determination, you must contact the Purdue IRB.
- You and the members of your research team acknowledge that this study is subject to review at any time by Purdue's HRPP staff, Institutional Review Board, and/or Research Quality Assurance unit. At any time, this project may be subject to monitoring by these Purdue entities to confirm the applicability of this determination. The Purdue IRB has final authority in determining if an activity is Human Subjects Research requiring IRB review.
- This determination is the Purdue HRPP assessment of regulations related only to human subjects research protections. This determination does not constitute approval from any other Purdue campus department or outside agency. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local, state, and federal laws that may apply.
- Finally, if any changes occur with respect to this project, recognize that such changes could change the need for review by HRPP/IRB. Should you change the intent of the activity to involve publication, presentation, or any different application of this work, it is likely that IRB review will be required. Therefore, it is important that you again complete PROPEL to ensure that the IRB review requirements remain the same.

Should you have any questions about your rights and responsibilities regarding conducting research with people, on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu. We are here to help!

LIST OF REFERENCES

Alpi, D. M. (2017). *Cyber vulnerabilities within critical infrastructure: The flaws of industrial control systems in the oil and gas industry* (Order No. 10682879). Available from ProQuest Dissertations & Theses Global. (1972645948). Retrieved from https://search.proquest.com/docview/1972645948?accountid=13360

Center for Innovative and Strategic Transformation of Alkane Resources. (2017, January 01). Retrieved from http://erc-assoc.org/content/center-innovative-and-strategic-transformation-alkane-resources

Clayton, B., & Segal, A. (2013, June). Addressing Cyber Threats to Oil and Gas Suppliers. Retrieved from https://www.cfr.org/report/addressing-cyber-threats-oil-and-gas-suppliers

Committee on National Security Systems Instruction (CNSSI) No. 4009, Committee on National Security Systems Glossary, April 2015

Das, R., & Morris, T. (2018). Modeling a Midstream Oil Terminal for Cyber Security Risk Evaluation. *Critical Infrastructure Protection XII IFIP Advances in Information and Communication Technology,* pp. 149-175. doi:10.1007/978-3-030-04537-1_9

Department of Homeland Security National Cyber Security Division. *Recommended Practice for Patch Management of Control Systems.* (2008, December). Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf.

Do, V. L., Fillatre, L., Nikiforov, I., and Willett, P., "Security of SCADA systems against cyber–physical attacks," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 5, pp. 28-45, May 2017. doi: 10.1109/MAES.2017.160047

Grance, T., Hash, J., Peck, S., Smith, J., & Korow-Diks, K. (2002). *Security Guide for Interconnecting Information Technology Systems* (47th ed., Vol. 800) (United States, National Institute of Standards and Technology, U.S. Department of Commerce). Gaithersburg, MD: National Institute of Standards and Technology.

ICS Cybersecurity: Implementing a PCN DMZ. (n.d.). Retrieved October 21, 2019 from https://www.aesolns.com/aecyber/pcn-dmz/

Judson, N. (2013). *Interdependence of the Electricity Generation System and the Natural Gas System and Implications for Energy Security* (Tech. No. 1173). Lexington, MA: Lincoln Laboratory, Massachusetts Institute of Technology.

Kovacs, E. (2019, June 14). Hackers Behind 'Triton' Malware Target Electric Utilities in US, APAC. Retrieved from https://www.securityweek.com/hackers-behind-triton-malware-target-electric-utilities-us-apac

Lamp, J., Rubio-Medrano, C. E., Zhao, Z., and Ahn, G., "ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems," *2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Montreal, QC, Canada, 2019, pp. 1-6.

Lerums, J. E. (2018). *Measuring the State of Indiana's Cybersecurity* (dissertation).

Madden, J. (2019, July 26). What are the Best Cybersecurity Certifications?. Retrieved from https://www.comptia.org/blog/what-are-the-best-cybersecurity-certifications.

Mentzer, R. A., & Ribeiro, F. (2018, December 3). CISTAR Cybersecurity Scorecard [Personal interview].

Metivier, B. (2018, March 12). Threat Hunting: Common Attack Vectors and Delivery Channels. Retrieved from https://www.sagedatasecurity.com/blog/threat-hunting-common-attack-vectors-and-delivery-channels

National Institute of Standards and Technology. Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* (July 2013). http://dx.doi.org/10.6028/NIST.SP.800-40r3

National Institute of Standards and Technology. Special Publication 800-39, *Managing Information Security Risk: Organization, Mission and Information System View*. (2011)

National Institute of Standards and Technology. Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. (2013)

National Institute of Standards and Technology. Special Publication 800-63B, *Digital Identity Guidelines*, (June 2017). https://doi.org/10.6028/NIST.SP.800-63b

National Institute of Standards and Technology. Special Publication 800-63-3, *Digital Identity Guidelines, Revision 3*, (June 2019). https://doi.org/10.6028/NIST.SP.800-63-3

National Institute of Standards and Technology. Special Publication 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, (July 2013). http://dx.doi.org/10.6028/NIST.SP.800-83r1

National Institute of Standards and Technology. Special Publication 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview*. (June 2017). doi.org/10.6028/NIST.SP.1500-201

National Institute of Standards and Technology. (2019, July 11). Retrieved from https://www.nist.gov/

Natural Gas Systems: Reliable & Resilient. (2017, July). Retrieved from https://www.aga.org/sites/default/files/ngc_reliable_resilient_nat_gas_white_paper.pdf

Norwich University Online. (2017, February). Who Are Cyber Criminals? Retrieved from https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals

U. S. Congress, Congressional Research Service. (2011). *Keeping America's Pipelines Safe and Secure: Key Issues for Congress* (P. W. Parfomak, Author) [Cong. Rept. R41536 from 112th Cong., 1st sess.]. Washington, D.C.: Congressional Research Service.

U. S. Congress, Congressional Research Service. (2012). *Pipeline Cybersecurity: Federal Policy* (P. W. Parfomak, Author) [Cong. Rept. R42660 from 112th Cong., 2nd sess.]. Washington, D.C.: Congressional Research Service.

U. S. Congress, Congressional Research Service. (2019). *Pipeline Security: Homeland Security Issues in the 116th Congress* (P. W. Parfomak, Author) [Cong. Rept. IN11060 from 116th Cong.]. Washington, D.C.: Congressional Research Service.

What is SCADA? (2018, September). Retrieved from https://inductiveautomation.com/resources/article/what-is-scada