2019

A Study of Perceptions on Incident Response Exercises, Information Sharing, Situational Awareness, and Incident Response Planning in Power Grid Utilities

Joseph Garmon
University of Central Florida

A STUDY OF PERCEPTIONS ON INCIDENT RESPONSE EXERCISES, INFORMATION SHARING, SITUATIONAL AWARENESS, AND INCIDENT RESPONSE PLANNING IN POWER GRID UTILITIES

by
JOSEPH P. GARMON
B.S. Purdue University, 1989
M.B.A. University of South Florida, 1996
M.S. University of Central Florida, 2015

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Industrial Engineering and Management Systems
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Fall Term
2019

Major Professor: Waldemar Karwowski

ABSTRACT

The power grid is facing increasing risks from a cybersecurity attack. Attacks that shut off electricity in Ukraine have already occurred, and successful compromises of the power grid that did not shut off electricity to customers have been privately disclosed in North America. The objective of this study is to identify how perceptions of various factors emphasized in the electric sector affect incident response planning. Methods used include a survey of 229 power grid personnel and the use of partial least squares structural equation modeling to identify causal relationships. This study reveals the relationships between perceptions by personnel responsible for cybersecurity, regarding incident response exercises, information sharing, and situational awareness, and incident response planning. The results confirm that the efforts by the industry on these topics have advanced planning for a potential attack.

To Kathy and our families

ACKNOWLEDGMENTS

I would like to express my appreciation to my research advisor, Dr. Waldemar Karwowski, my committee chair, and the person who pushed me in different directions to ensure that I considered all aspects and opportunities in this research and provided motivation to complete the process. I would also like to thank my committee members, Dr. Ahmad Elshennawy, Dr. Peter Hancock, and Dr. Thomas Wan. Without Dr. Wan, I would not have nearly as strong an understanding of structural equation modeling.

My research is closely related to my full-time work. Jay Bartlett, Curtis Taylor, and the team at my current employer, Wabash Valley Power Alliance, provided support allowing me to finish this project. I would also like to thank Tom Turke and the team at my former employer, Seminole Electric Cooperative, for their support.

The work done in this paper built on the work of the NERC Critical Infrastructure Protection Committee. I have benefited greatly from their work and am proud of having contributed to the work performed by this team. My role as a past Operating Security Chair was the motivation to perform this research.

Finally, I could not have completed this without Kathy and our families. They kept me going through the process.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Background

As demonstrated by recent attacks, the electric sector faces an increasing risk of disruption of services to end customers. As electricity is a core critical infrastructure for modern society, this risk goes beyond just the businesses and threatens the general public. The industry has set requirements to manage an incident successfully and to prepare for attacks against the bulk electric system (NERC, 2019c). Not only does the industry recognize the importance of this preparation, but North American governments recognize this need. Further, books such *as Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* (Koppel, 2015) raised awareness across the general public.

Addressing the threat of a massive cybersecurity incident in the power grid is complex. As of 2015, there are about 16,000 transmission substations, 7,098 high voltage transmission lines, and 1,057 gigawatts of generation serving 334 million customers in the interconnected power systems that make up the North American power grid. This grid includes the mainland U.S., portions of Canada, and portions of Baja California in Mexico (NERC, 2016c). These totals do not include local distribution power lines and substations.

No cybersecurity attacks since 2014 have resulted in a loss of power supply (loss of load) to any customer in the North American power grid (NERC, 2016f, 2019d). However, cyberattacks that resulted in loss of load occurred on two occasions in Ukraine in 2015 and 2016 (Assante, Conway, Lee, & E-ISAC, 2016; Assante, Conway, Lee, & E-ISAC, 2017). Further,

there are reports that the Russian hacking group, variously identified as Dragonfly or Energetic Bear, has obtained access within the power grid to the point they could have thrown the switches (Smith, 2018).

A successful large scale cyberattack could have an impact similar to the 2003 Northeast Blackout, which lasted four days and cost the economy between $4 billion and $10 billion (Knake, 2017). With a widespread interconnected power grid controlled by thousands of companies (NERC, 2019b), the attack surface is too widespread to prevent every cyberattack. While most cybersecurity incidents are likely to be much smaller, the ability to respond to and recover from a cybersecurity incident is mandatory.

1.2 Problem Statement

The electric sector has focused on a variety of issues related to cybersecurity incident response, primarily through the North American Electric Reliability Corporation (NERC). The NERC Critical Infrastructure Protection Committee (CIPC) has focused on various issues including information sharing and situational awareness (Diebold et al., 2013; E-ISAC, 2018), mandatory incident response planning (NERC, 2019c), and large scale incident response exercises (NERC, 2012, 2014, 2016d, 2018a). Each of these components involves people who are receiving information, placing the information in context, and practicing incident response skills. Incident response is dependent on each of these skills to manage an incident. There is a clear need in the electric sector to understand how individuals perceive these topics and fit them together in preparation for a cybersecurity incident.

1.3 Research Goal and Objectives

The main objective of this study is to develop a model that can explain the causal relationship between incident response exercise learning, information sharing quality, situational awareness confidence, and adequacy of incident response plans by personnel in power grid utilities.

CHAPTER 2: LITERATURE REVIEW

The power grid consists of three major domains: generation, transmission, and local distribution. Each of these domains uses operational technologies (OT) and industrial control systems. For example, supervisory control and data acquisition systems (SCADA) are commonly used to open and close breakers that control the flow of power. Generation plants use the same types of control systems that are used broadly in manufacturing.

Planning is necessary before responding to an incident. These plans also require appropriate testing before use. The industry routinely develops plans for many types of events. In the 2008 to 2015 time period, nine of the ten most stressed days for the power grid we a result of weather (NERC, 2016f). Not only do common large-scale incidents such as weather have carefully prepared plans, cybersecurity incident response planning is regulatory mandated across the bulk power systems (NERC, 2019c). Further, these incident response plans are tested annually for critical portions of the power grid and once every three years for the remainder of the bulk electric system. A large portion of the industry participates in a biennial continental exercise simulating a broad cyber and physical attack against the bulk electric system (NERC, 2012, 2014, 2016d).

Situational awareness weaknesses are not new to the electric sector. The Northeast Blackout of 2003 included poor situational awareness and blindness to critical information as root causes (US-Canada Power System Outage Task Force, 2004). To maintain shared situational awareness across the industry, NERC operates the Electricity Information Sharing and

Analysis Center (E-ISAC) for the sharing of information in support of situational awareness (E-ISAC, 2018).

2.1 Cyberattacks in the Electric and Energy Sectors

Cyberattacks have been rare in the electric sector, with only two known attacks occurring in Ukraine that directly disrupted electrical services to customers, also referred to as loss of load. However, there have been attacks elsewhere in the energy sector and in other industrial sectors that use similar systems.

An early incident occurred in 2003 when the SQL Slammer worm infected the safety system at the Davis-Besse Nuclear power plant. The worm passed from a contractor's network through the business network at the plant and into the plant control systems network, where it crashed safety monitoring systems. The power plant was offline at the time of the attack (Nicol, 2011). Unlike many of the later attacks, this was a side effect of a poorly protected system and a random internet worm.

The first widely known attack was the famous Stuxnet attack discovered in 2010 that was performed by the U.S. and Israel against the Iranian nuclear enrichment facility at Natanz. The attack was performed by a contractor that supported the air-gapped Siemens control system used at the facility. The system went beyond basic protections by air-gapping the entire control system from the internet and other internal connections (Zetter & 3M Company, 2014).

A 2014 report discussed a German steel mill that sustained massive damage, killed two persons, and injured 13 others. The attack is the first known example after the Stuxnet attack against a control system that caused physical damage. The attack methodology included phishing of employees to gain entry, compromising a host on the corporate network, moved into the control system network, and then performance of the damaging attack (Lee, Assante, & Conway, 2014). Private discussions indicate that there have been other similar unpublished attacks. Each of these attacks follows the ideas adapted from the military in 2011, known as the Lockheed Martin® Cyber Kill Chain (Assante & Lee, 2015; Lockheed Martin, 2015). The motivations for these attacks are unknown.

Two successful attacks in 2015 and 2016 against the Ukraine power grid resulted in loss of electrical service to customers, the only known times that cyberattacks have disrupted electrical service. In 2015, approximately 225,000 customers lost power and as a result of a carefully targeted cyberattack against three power distribution companies in Ukraine. The attack path followed the cyber kill chain and partially made use of the BlackEnergy2 tool that was specifically targeting a control system. Additional supporting techniques enhanced the effectiveness of the attack including electronically destroying ("bricking") communications equipment to the attacked substations, attacks that took control of UPS in the control centers, denial of service attacks against the phone systems, and formatting the hard drives inside the control systems (Assante et al., 2016; Department of Homeland Security - CISA, 2016; Zetter, 2016). Private conversations with members of the investigation team that visited the Ukraine indicate that other industrial sectors had been prepared for an attack, but the attack was not executed. Later analysis by Dragos® indicates the attack had intentions of causing more

prolonged outages, but an attack against the relays that would have allowed the destruction of breakers when re-energizing the equipment failed (Greenberg, 2019). The 2016 attack took some of the ideas from 2015 and automated the attack by building a framework to carry out those attacks using a tool that has been dubbed CrashOverride by Dragos® and Industroyer by ESET®. This attack power disrupted generation in the capital region in Ukraine and disrupted 200 megawatts of transmission (Assante et al., 2017; Cherepanov & Lipovsky, 2017; Department of Homeland Security - CISA, 2017a; Dragos, 2017) .

In 2017, attacks continued against the energy sector, the electric sector, and nuclear power, in the Dragonfly 2.0 campaign using the Havex malware. The attack followed the above kill chain. (Symantec, 2017; Venkatachary, Prasad, & Samikannu, 2018). No destructive attacks occurred as a result of this campaign. In 2018 the Department of Homeland Security CISA team released an alert and briefed the industry in a set of non-public calls that the attackers had direct access to the control systems(Department of Homeland Security - CISA, 2018). However, that view was challenged by industry leaders during a meeting with Secretary of Homeland Security Nielsen and the Secretary of Energy Perry, where they stated the intrusion was limited to one or two wind turbine sites (Sobczak, 2018). That meeting also included information that the attack was discovered by the Department of Energy's Cyber Risk Information Sharing Program (CRISP), which includes a set of sensors that monitors internet traffic into many of the large power companies (Department of Energy, 2018).

While any attack against a control system can be dangerous, attacks are now targeting safety systems inside of production facilities. The Trisis attack (a.k.a. Tricon, Hatman) against

the Schneider Triconex® safety instrumentation system disrupted a Saudi Arabian petrochemical facility. This type of attack can be used to place a targeted facility in an unsafe condition and potentially threaten the general public (Department of Homeland Security - CISA, 2017b).

While public impact has so far been minimal, capabilities have advanced from random events, through Stuxnet as the first highly targeted control system attack, continuing through BlackEnergy 2 used maliciously against the power grid, further advancing to CrashOverride automating the attack, and then finally the Trisis attacking emergency shutdowns for safety systems. Whether the motivation is criminal profit, hacktivism to make a statement, or by countries to gain a political or military advantage, the attacks will become more capable. An extended power outage may be the desired outcome or just the side effect. Either way, when protection fails, the ability to effectively respond to a cyberattack is mandatory.

2.2 Electricity Sector Cybersecurity Regulatory Requirements

While distribution is locally regulated, the Federal Energy Regulatory Commission (FERC) regulates the bulk power system. However, the responsibility for developing the regulations is assigned to, and enforcement is shared with the industry through the North American Electric Reliability Corporation (NERC) under section 215 of the Federal Power Act. NERC grew up as an industry organization following the 1967 blackout that affected the northeast United States and eastern Canada (NERC, 2016e) and continues to play multiple roles as an enforcement body, developer of regulatory standards for the reliability and security of the

power grid, and as the reliability coordinator for the industry. All bulk generation and transmission owners are mandated to become a member of NERC by the Federal Power Act.

Bulk power system transmission substations, generation stations, and control centers are required to have and test a documented incident response plan. Standard CIP-008-5 for high and medium impact systems or CIP-003-6 for low impact assets mandates incident response plans (NERC, 2019c). These rules have been approved by the Federal Energy Regulatory Commission in Orders 791and 822. (Federal Energy Regulatory Commission, 2013, 2016). Canada generally adopts NERC standards and enforces these standards on a provincial basis (NERC, 2017). Additional requirements are continually in development.

2.3 Cybersecurity Incident Response Planning

Both power grid operators and the information technology industry have developed strong incident management skills. The power grid developed these skills because of significant natural events such as earthquakes, ice storms, hurricanes, and various power grid cascading failures. The computer security profession has formalized incident response standards.

2.3.1 Managing Events: Risk vs. Resilience

When considering cyberattacks, risk and resilience have slightly different meanings. Both are relevant to having an incident response process. Risk is defined by the likelihood and impact of an attack, whereas resiliency refers to the ability to continue operating during an attack

and return to the normal state following the attack (National Institute of Standards and Technology, 2012). Based on these definitions, risk assessment is performed to ensure the proper protections are in place before an attack occurs. Resilience needs to be designed into the system to ensure that it can continue operating.

Risk assessment in the electric sector is mandated in the Reliability Standards for the Bulk Electric System of North America in standard CIP-002-5.1 (NERC, 2019c). The analysis performed here defines minimum cybersecurity requirements for the power grid based on this risk. However, this standard only considers the impact on simplifying the analysis process. While standardized to define the needed protections, this view of risk reflects neither the evolving infrastructure used in power grid control systems nor the evolving capabilities of the attacker.

Cybersecurity resilience also receives significant attention in the electric sector. For example, both the NERC Critical Infrastructure Protection Committee's studies by the Cyber Attack Task Force and the Severe Impact Resilience Task Force considers resilience. As the North American power grid has a long history of dealing with "normal" emergencies such as weather events, resilience is not a new concept. However, following a severe event that causes massive damage, a "new normal" with degraded planning and operating conditions will be established that could last for months or years. In response to these events, operational parameters such as islanding portions of the power grid, changes to system operating parameters and protections systems, and degradation of communications may occur. The Cyber Attack Task Force focused on a prevent, detect, respond, recover model. The Severe Impact Resilience Task

Force focused on preparing the operational components for a severe event such as an attack or geomagnetic disturbance. This team considered topics such as system operations, monitoring communications, and planning during a major event (Abell et al., 2012; Bowe et al., 2012).

2.3.2 Cybersecurity Incident Response Handling

Cybersecurity incident response handling is a mature field from a process perspective. While the specific attacks and associated responses vary widely, the overall approach is well understood. NIST SP 800-61 Computer Security Incident Handling Guide defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski, Millar, Grance, & Scarfone, 2012).

Numerous incident response planning guides have been published (Tøndel, Line, & Jaatun, 2014). In addition to NIST SP 800-61 published in the U.S. (Cichonski et al., 2012), The European Network and Information Security Agency publishes Good Practice Guide for Incident Management (Maj, Reijers, & Stikvoort, 2010). ISO/IEC 27035 is also a widely used international standard (International Organization for Standardization [ISO], 2016). Numerous other organizations, such as SANS (Kral, 2011), publish guidance. While there are definite differences in the details of these guides, they all emphasize the same concepts.

Incident response guidelines that focus on information technology and industrial control systems are of specific interest for the power grid. NIST defines industrial control systems (ICS) as:

> Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)

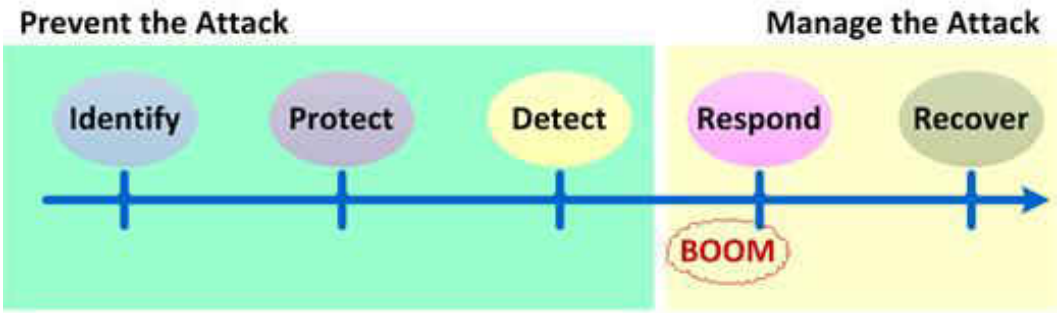
Industrial control systems (ICS) operate in a real-time environment, such as the power grid. As ICS controls physical equipment, incidents may not only result in production and service interruptions but present a risk to humans and the environment. Further, physical attacks on this equipment often can have a considerable impact. While the implementation of parts of the plan is different, the overall flow of incident response remains similar.

Table 1 identifies the overall process flows for several conventional processes and the NERC defined process. It highlights the similarities and differences between processes.

Table 1 Comparison of Cybersecurity Incident Response Handling Programs

ISO 27035	**NIST SP 800-61**	**ENISA**	**NERC Workshop**
1. Plan and prepare	1. Preparation		1. Preparation
2. Detection and reporting	2. Detection and Analysis	1. Detection 2. Triage	2. Identification
3. Assessment and decision		3. Analysis	
4. Responses	3. Containment, Eradication, and Recovery	4. Response	3. Containment 4. Eradication 5. Recovery
5. Lessons learned	4. Post-Incident Activity		6. Lessons Learned

NIST has identified an overall cybersecurity framework for critical infrastructure (National Institute of Standards and Technology, 2018). This framework identifies five functions that assist in preventing and responding to an attack with specific functions within each category and subcategories that identify the details of the model. While the identify, protect, and detect processes occur continuously, actual events trigger response and recovery. In the industry, the phrase "stay left of boom" focuses on prevention, while being prepared to deal with boom once it occurs.



Adapted from NIST Framework for Improving Critical Infrastructure Cybersecurity

Figure 1 Preventing and Managing an Attack

2.3.3 Incident Response Handling Structure

While a small event can often be quickly handled using these approaches, a larger scale event requires a generalized incident response protocol. Both physical and electronic damage may be present and impact the public.

The U.S. Government, under the Federal Emergency Management Agency (FEMA) has developed an incident response standard widely used by first responders in many other types of

events. This process is known as the National Incident Management System (NIMS). Due to the close tie between the electricity sector and various North American federal and state government agencies, an understanding of this program provides a planning approach (Department of Homeland Security, 2008).

The NIMS core process document includes specific information on the communication of information between different parties within the team. NIMS refers to a common operating picture that "is established and maintained by gathering, collating, synthesizing, and disseminating incident information to all appropriate parties." This understanding allows an understanding of available resources, requests, and priorities. The communications infrastructure focuses on interoperability, reliability, scalability, and resiliency.

A standardized format for information sharing ensures situational awareness. Maintaining communication begins with incident notification and continues through status reports in an easy to analyze format. Further, tracking this information allows a stronger after-action review. Of course, not everything will easily fit into the standard reporting format, and information will need to be available in the best manner to present the information. Clarity is more important than perfection when reporting and using information. Timely information is often more critical than complete information. The last little bit of perfection adds little to the decision-makers' ability to decide. Finally, the exchange of information needs to be appropriately secured. Through this, NIMS demonstrates a preplanned incident response system that reduces the complexity and time when responding to an event.

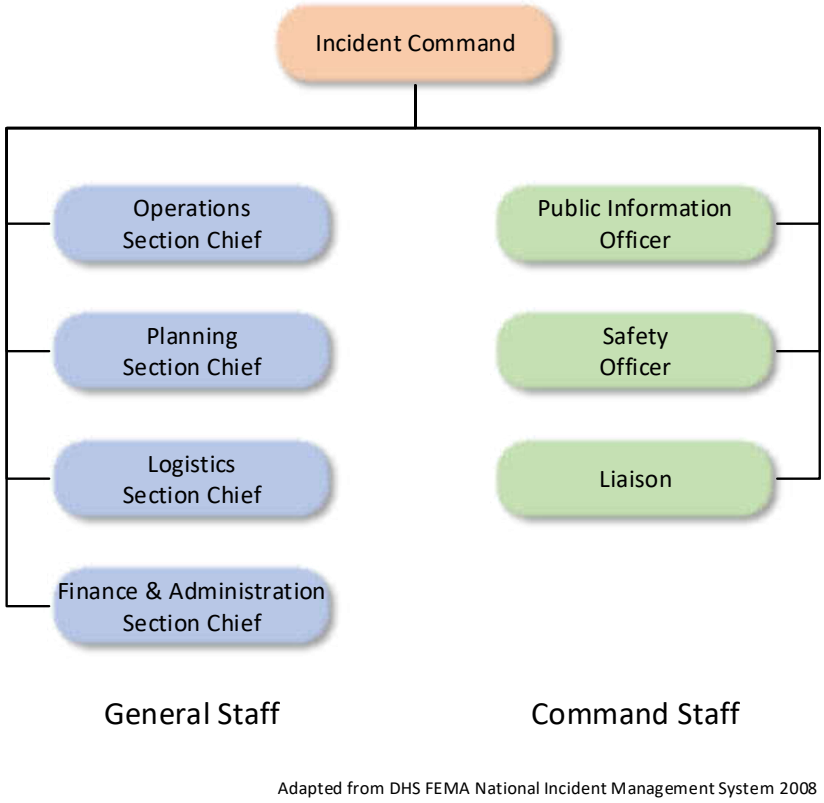


Figure 2 NIMS Incident Command Structure (Department of Homeland Security, 2008)

2.3.4 Cybersecurity Incident Response Team Effectiveness

Incident response is dependent on the integrated skills and capability of the cybersecurity incident response team. The Carnegie Mellon Software Engineering Institute summarizes several factors that affect response in the closing remarks of their Handbook for Computer Security Incident Response Teams (CSIRTs). As is true for security in general, the needs of each CSIRT are unique, and the CSIRT environment is dynamic. There is no chance of long-term stability, since technology, the constituency base, and the intruder community can change

any time. To ensure successful operation, a CSIRT must have the ability to adapt to the changing needs of the environment and exhibit the flexibility to deal with the unexpected. In addition, a CSIRT must simultaneously address funding issues and organizational changes that can affect its ability to either adapt to the needs or provide the service itself. (West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003)

2.3.5 An Incident Response Case Study: Gulf Oil Spill

These ideas are not unique to the electric sector. A real-world case study of an event in the Gulf of Mexico documents the practical implementation of incident response in the physical world. This document highlights the response in terms of strategy, tactics, and operational processes. The strategic level identifies the goals and determines the overall actions, which are set by the incident manager and supporting team. During the incident, the planning team identified the specific activities to be taken with adequate detail to carry the plan out. The operational team then carries out this plan.

Limited or inadequate information challenges response teams early in the process. Often, the first part of the process focuses on the tactical viewpoint and may be performed based on pre-planning and rule-based analysis. Typically, time and risk factors are most critical early in the process. Changing conditions will typically be seen, requiring personnel to adapt to the environment rapidly. As the process continues, the strategic actions gain importance (Crichton, Lauche, & Flin, 2005).

As demonstrated in this case study, there are three levels of decisions needed during a security event. Decisions occur at the real-time or operational level, the tactical level, and at a strategic level.

2.3.6 The Industrial Control System Cyber Kill Chain

Managing the attack requires a detailed understanding of the events to see how the attack occurs. A cyber kill chain, commercially developed by Lockheed Martin (Lockheed Martin, 2015), evaluates the processes an attacker uses to break in and cause damage. Assante and Lee (2015) extend this approach to industrial control systems. Based on private discussions with members of E-ISAC and others in the industry, many in the electric sector have adopted this approach.

There are two stages to this kill chain. Intrusion into the network occurs in the first stage. Developing and performing the attack on control system equipment occurs during the second stage. Cyber kill chain theory posits that the attack disruption may occur at any point in the kill chain. Figure 3 shows the individual steps typically used by the adversary. The highlighted steps are observable by the defender and present an opportunity to disrupt the attack. The further into the attack, the more difficult it is for the attacker to proceed without detection. The Stuxnet attacks on Iranian centrifuges highlights the attacker's approach.

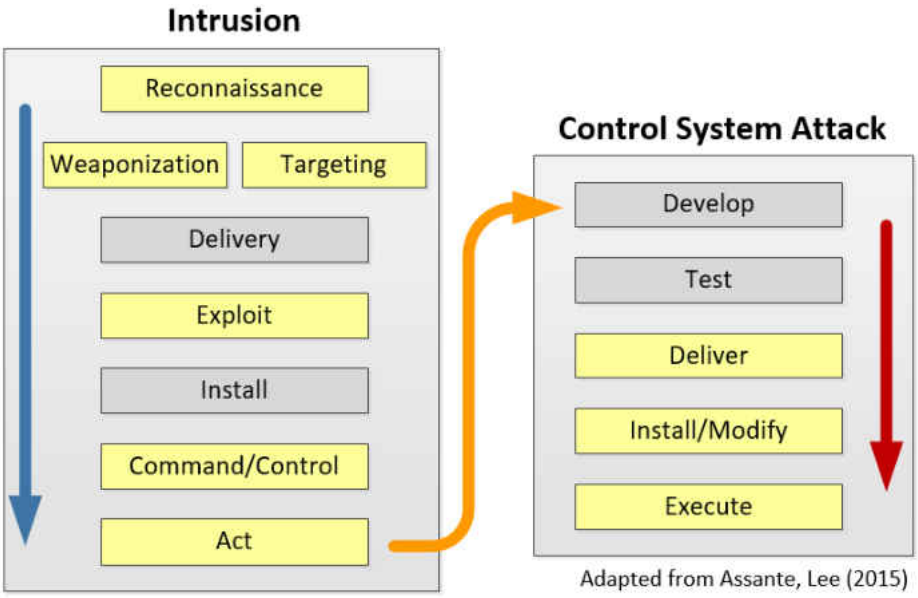


Figure 3 ICS Cyber Kill Chain (Assante & Lee, 2015)

The December 2015 Ukraine cyberattack also followed this approach (Assante et al., 2016). While the approach is straightforward, it effectively identifies opportunities to disrupt the attacks.

2.4 Situational Awareness

Early situational awareness research evolved from military and aircraft operations, with Mica Endsley widely published and cited in this research. She defines situational awareness as:

> Situation Awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future (Endsley, 1995).

2.4.1 Importance of Situational Awareness in the Bulk Power System

After the 2003 U.S. and Canada blackout affecting 50 million people and 61,800 MW of electric load, the U.S. and Canadian Task Force identified three groups of causes for the blackout directly related to situational awareness including (US-Canada Power System Outage Task Force, 2004):

- "FirstEnergy and ECAR failed to assess and understand the inadequacies of FE's system, particularly with respect to voltage instability and the vulnerability of the Cleveland-Akron area, and FE did not operate its system with appropriate voltage criteria."
- "Inadequate situational awareness at FirstEnergy. FE did not recognize or understand the deteriorating condition of its system."
- "Failure of the interconnected grid's reliability organizations to provide effective real-time diagnostic support."

Since this report, the industry has focused on real-time situational awareness and understanding within power grid operations.

2.4.2 Situational Awareness Overview

Endsley, in 2012 and 2013, presented an overview of situational awareness in the bulk power system at the NERC Human Performance Conference in 2012 and expanded the idea in a related journal article (Connors, Endsley, & Jones, 2007; Endsley, 2012). In the overview, Endsley highlighted the relationship between awareness and understanding in terms of perception of the current state, comprehension of this state, and projection of the potential future

state. Figure 4 places this in terms of "what," "so what," and "now what." Situational awareness provides the information for decision-making in the environment using this approach.

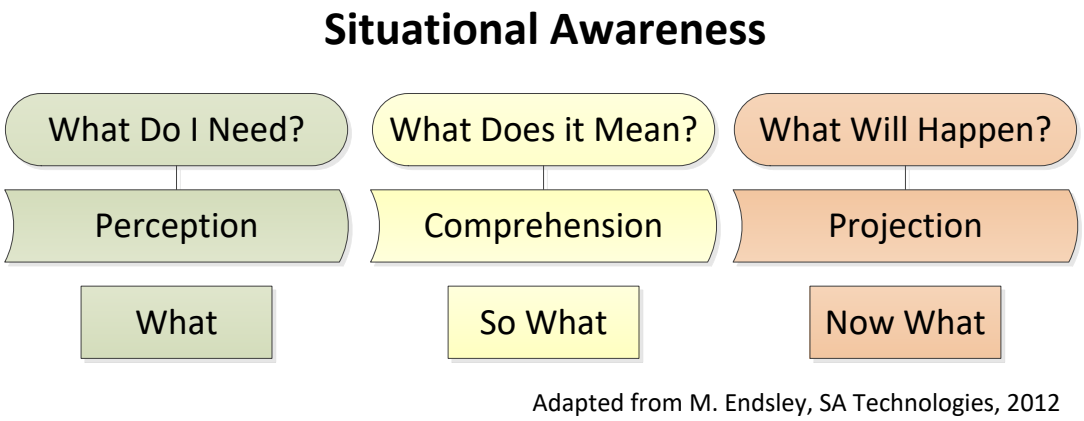


Figure 4 Situational Awareness (Endsley, 2012)

While the approach currently focuses on real-time decision-making concerning power grid operations, it also provides a useful basis for power grid cybersecurity. Perception begins with the detection of something interesting happening on the network. Once the information becomes available, possibly through automated alerts or an analyst's recognition of events, additional information allows the formation of a mental model of the event. Perception then evolves into comprehension of the current state of the event. Once attaining comprehension, analysts can finally project potential impacts (D'Amico, Whitley, Tesone, O'Brien, & Roth, 2005).

When the analyst has the right information for situational awareness, the analyst has the tools to utilize the Observe-Orient-Decide-Act (OODA) model (Blasch et al., 2009). This

approach combines both real-time and tactical information for the commander of an incident to make intuitive decisions under stress. Steps int OODA model includes:

- Observe the current incident and understand the threat
- Orient to the threat and understand alternatives and project the impact of various alternatives
- Decide among the options to select a response based on available information
- Act on the decision while continuing to make new observations

In addition to real-time situational awareness, tactical situational understanding also provides value when evaluating alternatives and opportunities. In essence, real-time situational awareness focuses on the immediate here and now. Tactical situational understanding orients the decision-maker to assess the environment and mission requirements.

One study identified six recommendations for incident command system design (Bigley & Roberts, 2001). Of specific interest is the recommendation "Institute protocols for mental model development and maintenance." The authors suggest several questions that can be adapted to cybersecurity events to obtain this shared mental model.

- "How much attention should be directed to situational comprehension?"
- "When and how should individuals initiate mental model development?"
- "What communication protocols would insure (sic) effective dissemination of information critical to mental models?"
- "How can representational responsibility be off-loaded?"

Another study in an information security focused article identified three deficiencies in situational awareness of risk information in their literature review (Webb, Ahmad, Maynard, & Shanks, 2014). First, risk identification is treated in a perfunctory manner. The authors propose that a lack of risk management training by professionals performing the risk assessment process

results in a non-consideration of information sources. They also propose that this review is treated more as a compliance requirement rather than using a granulated assessment. Next, they highlight that the risk assessment does not consider the organization's situation, but instead reflects the assessor's speculation rather than the evidence. Further, the assessment is often rendered as subjective numerical probability and risk values that do not consider the specific environment. Finally, the authors find that information is gathered on an intermittent basis rather than on a scheduled basis. As a result, the ability to analyze changes is limited.

2.4.3 Shared Situational Awareness

While the incident response commander leads the response, all participants need the appropriate information to make decisions consistent with the response. Essentially, there needs to be shared situational understanding around the event and the decisions made. After creating a shared understanding, the individual may apply this information to their situational awareness for their immediate responsibilities. Further, each individual's observations also need to be shared.

While obtaining shared situational awareness is critical, the challenges are far more significant for dispersed teams. Kaber and Endsley (1998), while reviewing shared situational awareness in process control systems, identified several barriers to achieving this awareness. Unavailable or low-quality information being collected and shared often results in weak situational awareness. Further, information that would be valuable to other teams may not be shared. The organizational culture and the capability to effectively share information are core to allowing this communication to happen. Organizational instability impairs this organizational

culture. Interpersonal conflicts, especially when the leader or another team member takes a dictatorial approach, impairs communication, and could result in decisions made for organizational cohesiveness rather than effectiveness. The lack of a shared environment and supporting non-verbal communications in dispersed teams adds complexity to developing a consistent operating picture.

One significant advantage the electric sector has is that E-ISAC operates as a central service for maintaining situational awareness. While the large investor-owned utilities may have the resources to assign resources to monitor the risk environment, smaller entities such as the municipal utilities and cooperatives do not have the same resources available. A centralized approach may be an appropriate approach as long as the collective situational awareness is shared.

2.5 Information Sharing

The ability to perform analysis is highly dependent on both the real-time information collected for both power grid operations and on the overall tactical cybersecurity status.

2.5.1 Information Sharing and Shared Situational Awareness

One study of command and control in a battlefield exercise identified that successful information sharing between command and control staff, each with their specific areas of expertise, permitted proactive actions during the battlefield exercise. Three types of individual

information support information sharing: current work goal and situation, work process, and specialized domain knowledge. The work process is related to the specific task procedures and informal practices. The handoffs not only occur between teams but within teams during shift changes (Sonnenwald & Pierce, 2000).

One of the challenges to obtaining shared situational awareness is sharing not just the right information, but the right amount of information to obtain a common operating picture. Information needs change as an incident evolves. Timeliness, accuracy, and quality of the information evolves during the situation. The real value is not the data, but the interpretation of the data (Harrald & Jefferson, 2007).

Information sharing between teams would seem simple using modern tools. However, each individual has an individual goal to obtain. People will often share information in a manner that helps them obtain their goal rather than the overall goal. As individuals determine personal goals, the results can be significantly changed by the planning and organizational structure that either rewards a positive information-sharing context or builds barriers to effective information sharing (Wittenbaum, Hollingshead, & Botero, 2004).

2.5.2 Information Sources

The Electricity Information Sharing and Analysis Center (E-ISAC) manages overall cybersecurity for the electricity sector. E-ISAC is a NERC organization that coordinates with utilities and government agencies to collect and share security information and coordinates incident management across the sector (Electricity Information Sharing and Analysis Center,

2016a). Overall, there are 21 Information Sharing and Analysis Centers for critical infrastructure that provide and collect information on cyber and physical security hazards (National Council of ISACs, 2016).

E-ISAC provides a private portal with daily reports, industry discussions, and a private monthly web conference. These non-public briefings typically include current event information from E-ISAC analysts, DHS Office of Intelligence and Analysis, and ICS-CERT on current events. Finally, events include the annual GridSecCon Power Grid Security Conference and quarterly updates provided to the NERC Critical Infrastructure Protection Committee. For the program to be successful, organizations need to share information with E-ISAC (Electricity Information Sharing and Analysis Center, 2016b). This information should also be shared with other appropriate resources.

In addition to E-ISAC, there are numerous other information sources with many organized in coordination with the U.S. Department of Energy and the U.S. Department of Homeland Security. Much of this information is general information security, though DHS maintains a specific Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). While information is often available, it comes from a wide variety of sources and takes significant work to coordinate.

While the above techniques handle the vast majority of cyber and physical security information, critical information is occasionally escalated to the NERC alert level. There are three levels of formal NERC alerts shown in Table 2 below (NERC, 2016a, 2016b). The highest level of alert, an essential action, has never been used.

Table 2 NERC Alerts

Alert Type	Description	Alerts issued since 2014
Industry Advisory	"Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary."	10
Industry Recommendation	"Recommends specific action be taken by registered entities. A response from recipients, as defined in the alert, is required."	5
Essential Action	"Identifies actions deemed to be "essential" to bulk power system reliability and requires NERC Board of Trustees' approval prior to issuance. Like recommendations, essential actions also require recipients to respond as defined in the alert."	0

2.5.3 Information Sharing Complexities in the Electric Sector

The NERC Critical Infrastructure Protection Committee produced a report entitled Recommendations for Improved Information Sharing that highlights the complexity of communications and the number of resources available (Diebold et al., 2013). The team highlighted seven agencies, 11 separate sources of documents, and nine sets of recipients that either request or require communication to occur.

The amount of complexity involved stresses the processes and requires significant planning during an incident to ensure information is shared with the right agencies and organizations. The report highlights the challenges in the following quote:

> The industry struggles to make correlations between information received from various information sources… Due to various requirements, industry must report the same or similar information to sources listed above. Having so many reporting

> and information sources results in duplicative information, and important information can be overlooked. The industry needs a central hub for reporting suspicious physical and cyber-related events. Consolidated reporting will greatly enhance the analysis and detection of emerging threats. (Diebold et al., 2013)

This report also identifies a sample of current information sources that need to be monitored and correlated, including:

- NERC Standards Announcements
- NERC Alerts
- NERC Standards Interpretation Requests
- DHS For Official Use Only
- DOE Sector-Specific Agency Information
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Alerts
- United States Computer Emergency Readiness Team (US-CERT) Alerts
- E-ISAC Notices
- Vendor Notices
- National Lab Research

2.5.4 Information Sharing Metrics

From the above research, information sharing and situational awareness are closely related. Effective information sharing supports good situational awareness, both before and during an event. As demonstrated in the industry's communication processes, information can be shared widely and rapidly across multiple groups and requires using many processes.

One component of the incident response plan is preparation. This information sharing identifies current risks and potential issues. The U.S. Department of Energy Sandia National

Lab has developed a threat model focused on energy (Mateski et al., 2012). This model focuses on the threat and the attackers. It evaluates threats across two major category groups, commitment, and resources. These groups are broken down into subcomponents:

- Commitment
  - Intensity – Diligence and perseverance to reach a goal
  - Stealth – higher secrecy reduces the defender's countermeasures
  - Time – More time spent on an attack increases potential devastation
- Resources
  - Technical Personnel – Number of skilled personnel increases capability
  - Knowledge – Higher specialized knowledge increases capability
  - Access – Infiltration of systems whether technical, insider, or coercion

2.6 Exercising the Incident Response Plan: NERC GridEx

Bulk electric system utilities are required to exercise their incident response plan annually for many facilities and at least once every three years for every facility (NERC, 2019c). From private discussions, most organizations use a standard cybersecurity incident response plan for all of their applicable facilities. When performing these exercises, each utility is required to follow their plan and identify deviations taken from the plan, identify lessons learned from the exercise, and develop and implement plans to address the lessons learned.

NERC has recognized that to respond to a cybersecurity event effectively, and companies must practice for the event. In addition to exercises run by individual utilities, NERC has performed four large-scale national exercises biennially, known as GridEx or the Grid Security Exercise. November 2019 marks the fifth incarnation of GridEx.

The initial exercise included 64 utilities, Reliability Coordinators, and Regional Entities in 2011, along with 19 government representatives. Participation has grown massively. In 2017 during GridEx IV, participation grew to include 238 power grid participants and 202 federal, state, and provincial teams (NERC, 2018a). In addition to utility participation, an executive tabletop exercise is held that includes utility CEOs and U.S. agencies, including the White House National Security Council, Department of Energy, Department of Homeland Security, Department of Defense, and National Security Agency.

GridEx III in 2015 simulated a continent-wide coordinated cybersecurity and physical security attacks with national scenario development performed by E-ISAC and CIPC with regional planning and exercise response managed by Reliability Coordinators. The incidents start slowly and build until the maximum effect is reached at the end of exercise day one, followed by recovery to sustainable operations on day two. Having led teams that included developing the scenarios, I have observed that the objective is to maximize learning capability using a set of reasonable events that includes considering historical events. The exercise scope excludes high-impact low-frequency events such as electromagnetic pulse and military attacks. Further, it is a simulation and does not involve shutting off power. This approach has continued through GridEx V.

The public version of the GridEx III final report included two groups of recommendations based on observations from the exercise that relates to this study. One example recommendation focuses on information sharing in support of situational awareness (NERC, 2016d).

> *Organizations should review documentation that describes their internal information-sharing processes in the context of a large-scale event. This will enhance current situation awareness of staff at system operations, field locations, security, and other business areas. Documentation should be examined to identify opportunities to align incident response by different parts of the organization*.

The right information needs to be collected and shared during a large-scale event to maintain situational awareness, both within individual organizations and across organizations.

The second related recommendation states

> *Review the various tools and reporting processes used by the industry to identify opportunities to improve the efficiency and effectiveness of the information sharing process.*

There are numerous methods to share information, with some being mandatory. These include reporting requirements to E-ISAC and the Department of Energy and within the operations for sharing between Reliability Coordinators. Duplicate information and regulatory requirements can slow down the reporting of initial information. These tools need to be simplified and coordinated to ensure that the right people receive consistent information (Diebold et al., 2013).

There is little published cybersecurity research performed on whether incident response exercises improve an organization or industry's ability to respond. Organizations may treat the exercise as a minimal item to pass compliance requirements and limit participation. Resource

constraints or a belief that the risk is low due to a belief that attackers only target larger organizations may also limit participation (Line, Zand, Stringhini, & Kemmerer, 2014).

2.7 Partial Least Squares Structural Equation Modeling (PLS-SEM)

Structural equation modeling (SEM) is a technique used for studying causal models simultaneously in psychometric research. Two versions are commonly used. Both versions of SEM are second-generation multivariate statistical analysis techniques. First-generation techniques include exploratory tools such as cluster analysis and exploratory factor analysis and confirmatory tools such as multiple regression and logistic regression. Second-generation tools include covariance-based structural equation modeling (CB-SEM) and partial least squares structural equation modeling (PLS-SEM) (Joseph F. Hair, Hult, Ringle, & Sarstedt, 2014; Lowry & Gaskin, 2014).

These techniques are ideal for research where measurements cannot be directly taken but are instead inferred from other variables. Latent variables are unmeasured variables that are estimated using a linear combination of measured variables (Bentler & Weeks, 1980).

CB-SEM, also known as factor-based SEM, uses the maximum likelihood approach to minimize the difference between the estimated and observed covariance matrices (Astrachan, Patel, & Wanzenried, 2014). To do this, the variance of each measured variable includes the common variance shared with other variables in the measurement model and the unique variance consisting of specific variance and error (J. Hair, Hult, Ringle, Sarstedt, & Thiele, 2017).

PLS-SEM differs from CB-SEM in that PLS-SEM focuses on variance. A challenge of PLS-SEM is that multicollinearity, which is expected when combining factors that are measuring the same latent variable, tends to either overestimate or underestimate path coefficients resulting in false or false negatives. To overcome this, the consistent PLS algorithm (PLSc) calculates the reliability coefficient ρ_A and uses this value to correct for attenuation before performing ordinary least squares. When used with normally distributed data, PLSc reduced the likelihood of false-positive errors in exchange for an increase in the likelihood of false-negative errors (Sarstedt, Hair, Ringle, Thiele, & Gudergan, 2016).

A study of the differences tested the typical reasons one approach was chosen over another using Monte Carlo simulation (Reinartz, Haenlein, & Henseler, 2009). This study identified that while PLS-SEM makes no assumptions regarding distribution, CB-SEM is also robust to non-normal distributions. PLS-SEM does not suffer from identification and convergence problems. However, CB-SEM only rarely suffers from these problems. PLS-SEM is more appropriate than CB-SEM for small samples as sample populations of about 100 can obtain a reasonable result and is often more appropriate for sample sizes of less than 250. Based on the sample size, this study used PLS-SEM for data analysis.

2.8 Applications of PLS-SEM

PLS-SEM has been widely used in causal studies using structural equation modeling. No studies were identified that focused on organizational preparation for a cybersecurity incident. Incident response is a component of cybersecurity. A computer security study of behavior

reviewed 430 university students concerning protection motivation, social bond theory, awareness, and anti-malware protection (Berthevas, 2018). The relationship between self-assessment of controls, cloud security, and cloud-related business performance was established using PLS-SEM (Au, Fung, & Tses, 2016). A study of 183 bank employees identified relationships between information security awareness programs, employees' intent for compliant behavior, perceived level of monitoring, and actual compliant behavior (Bauer & Bernroider, 2015).

Safety and loss prevention is another related concept. One study established several relationships between safety and health rules, safety procedures, first aid support and training, organizational safety support, and occupational hazard prevention (Kaynak, Toklu, Elci, & Toklu, 2016). Another safety study established relationships across eight latent variables to identify factors influencing safe workplace behavior (Hald, 2018).

PLS-SEM has also been used to address organizational climate. A study of 264 nurses found that factors such as autonomy and control of the work environment improved perception, whereas burnout reduced perception and safety climate required special attention as an opportunity to improve the environment (dos Santos Alves, da Silva, & de Brito Guirardello, 2017). A small study in Malaysia surveyed 74 people identified that management commitment, safety training, and safety rules and procedures were related to safety behavior (Subramaniam, Hassana, Mohd. Zin, Sri Ramalu, & Shamsudin, 2016).

CHAPTER 3: METHODOLOGY

This study evaluates a set of human factors necessary for an incident response plan in the electric sector. A hypothesized causal model based on the literature review is tested using a set of factors represented by latent variables and indicators. The model is analyzed using partial least squares analysis structural equation modeling (PLS-SEM).

3.1 Summary of Selected Methodology

The process used to collect and analyze data involved multiple tools and techniques includes the following steps:

1. Identify a proposed research model, hypotheses, and associated measured variables
2. Collection of data via survey instrument
3. Analyze collected measured data for skewness, kurtosis, and Cronbach's alpha
4. Identify a causal path model using partial least squares structural equation modeling (PLS-SEM) for model validation

Step 1 involves developing a set of measured variables and associated questions to be analyzed by personnel with the responsibility to respond to a power grid cybersecurity incident and operate the power grid during an incident. These variables were based on the five groups of topics identified in the literature review. Each evaluated statement addressed a separate point identified in the literature.

Step 2 involves promoting and circulating the questions to personnel in the electric sector using a Likert style survey. The collected data included 29 measured variables addressing five sets of ideas represented by latent variables documented in the literature review.

Step 3 involves analyzing the collected survey data to identify the actual relationships and associated factors that describe the relationships using principal component analysis. These relationships may differ from the original proposed model.

Step 4 involves applying PLS-SEM to the collected data to verify the causal model.

3.2 Proposed Research Model and Hypotheses

This research focuses on a set of factors necessary for a successful incident response plan. The selected factors were based on areas emphasized by the electric sector through work by the North American Electric Reliability Corporation (NERC). These areas of focus include information sharing, situational awareness, incident response exercises, and their impact on incident response planning.

The following hypotheses are proposed to test the structural relationships among the model constructs.

H1: Perceived information sharing quality has a positive and significant effect on perceived situational awareness confidence.

H2: Perceived situational awareness confidence has a positive and significant effect on the perceived incident response plan adequacy.

H3: Perceived information sharing quality has a positive and significant effect on the perceived incident response plan adequacy.

H4: Perceived exercise response learning has a positive and significant effect on the perceived incident response plan adequacy.

The tests for the hypotheses are performed using the structural model shown in Figure 5 using the variables shown in Table 3

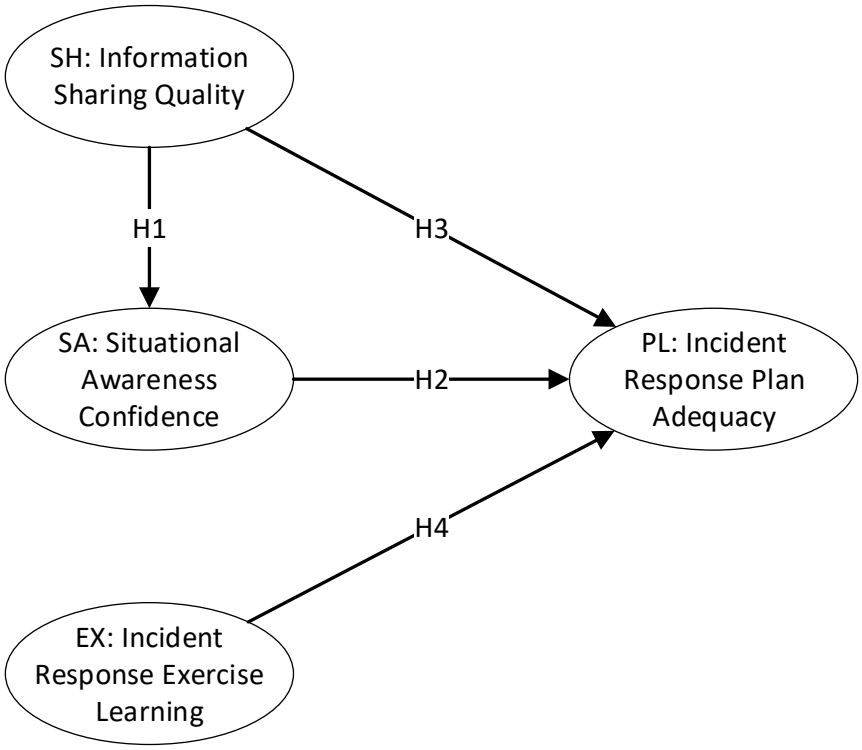


Figure 5 Structural Model

Table 3 Latent Variables

Variable	Type	Description
EX	Exogenous Latent	Incident Response Exercise Learning
SH	Exogenous Latent	Information Sharing Quality
SA	Endogenous Latent	Situational Awareness Confidence
PL	Endogenous Latent	Incident Response Plan Adequacy

The overall research model, including the identified indicators, also referred to as measured variables, is shown in Figure 6.

3.3 Survey Instrument

A set of questions was developed and distributed to personnel in the electric sector that would be involved in some manner during a cybersecurity incident. These surveys were distributed to participants at various industry meetings, primarily meetings related to critical infrastructure security, and through emails using purchased email lists.

The survey contained six sections and a total of 31 questions. The first four sections included the factors evaluated in the model, incident response exercise learning, information sharing quality, situational awareness confidence, and incident response plan adequacy. The fifth section address perceived readiness for a cybersecurity incident and is not used here. The final section collected limited demographic data.

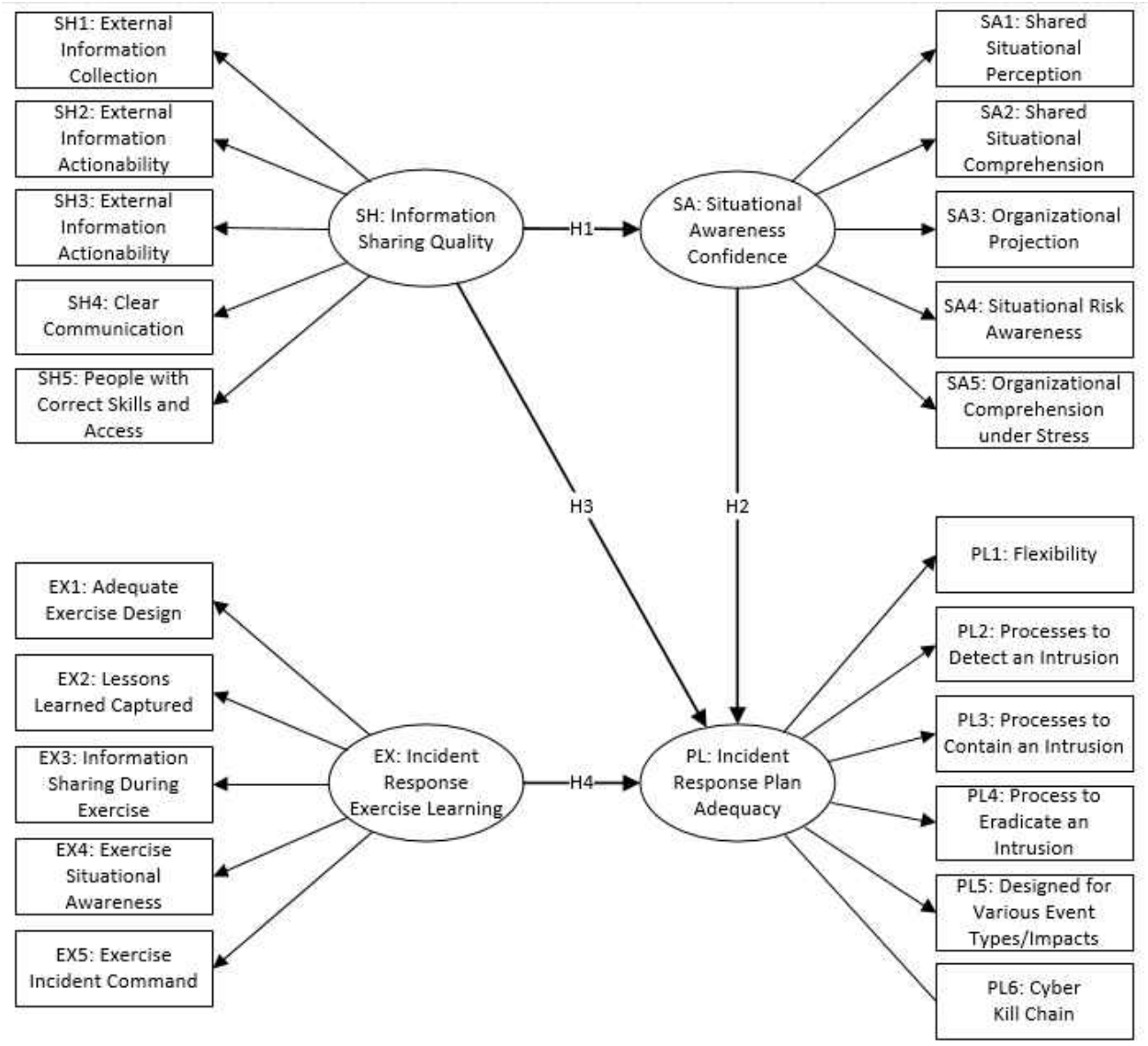


Figure 6 Proposed Research Model

Respondents evaluated the statement associated with each indicator variable via a Likert scale with the range of: Strongly disagree, Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree, and Strongly Agree. The survey was distributed via the web using Qualtrics®

software and in paper form. The electronic survey instrument, which includes additional questions not used in this model, is shown in Appendix 2.

There are specific regulations in NERC Reliability Standard CIP-011 (NERC, 2019c)that requires " procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use." BES Cyber System Information is defined as (NERC, 2019a);

> *Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.*

The survey was carefully constructed not to ask questions related to BES Cyber System Information and privately reviewed to ensure no infringement. Further, all information was collected anonymously by the survey tool, not through de-identification, but instead by non-collection. Finally, extremely limited demographic information was collected to ensure no potential reverse identification of respondents. Anonymity was assured in survey announcements.

3.4 Study Variables

3.4.1 Structural Model

Table 3 identifies four latent variables to assess the structural model. Figure 6 shows the structural model.

3.4.2 Incident Response Exercise Learning Measurement Model

Table 4 identifies five measurements surveyed that assesses the incident response exercise learning latent variable. Figure 7 shows the measurement model. Incident response exercise learning is an exogenous latent variable with indicators related to this study that may be tested during an exercise.

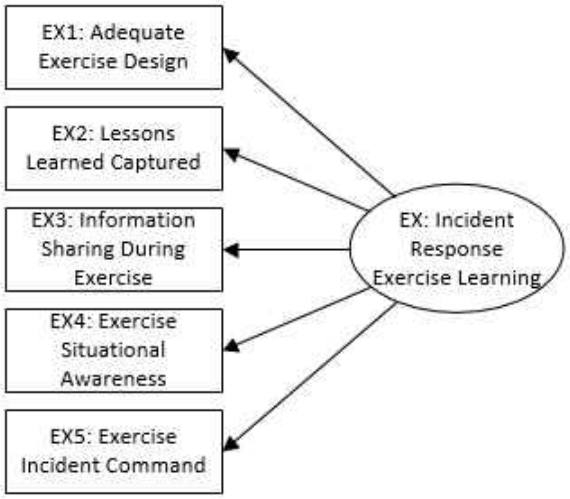


Figure 7 Incident Response Exercise Learning Measurement Model

Table 4 Incident Response Exercise Learned Indicators

Indicator	Variable Type	Dimension	Survey Statement (1=disagree, 7=agree) (References related to the exercise statement)
EX1	Measured	Adequate Exercise Design	Our team performs incident response exercises that test how well information is shared between teams. (NERC, 2012, 2014, 2016d)
EX2	Measured	Lessons Learned Captured	After an exercise, we carefully reviews and documents the lessons learned. (NERC, 2019c)
EX3	Measured	Information Sharing During Exercise	Our exercises effectively test the sharing of information. (Diebold et al., 2013; NERC, 2016d)
EX4	Measured	Exercise Situational Awareness	Our exercise effectively test the ability of teams to develop a shared situational awareness of events. (Kaber & Endsley, 1998; NERC, 2016d)
EX5	Measured	Exercise Incident Command	Our exercises effectively exercise the incident command structure and support staff to ensure clear responsibility and authority. (Department of Homeland Security, 2008)

3.4.3 Information Sharing Quality Measurement Model

Table 5 identifies five measurements to survey that assesses the incident sharing quality exercise learning latent variable. Figure 8 shows the measurement model. The measurement objectives highlight the organization's ability to collect and share information needed to prevent a cybersecurity incident and respond to an incident. While the focus is on incident response, practical use of information often requires awareness of the information before responding to an incident.

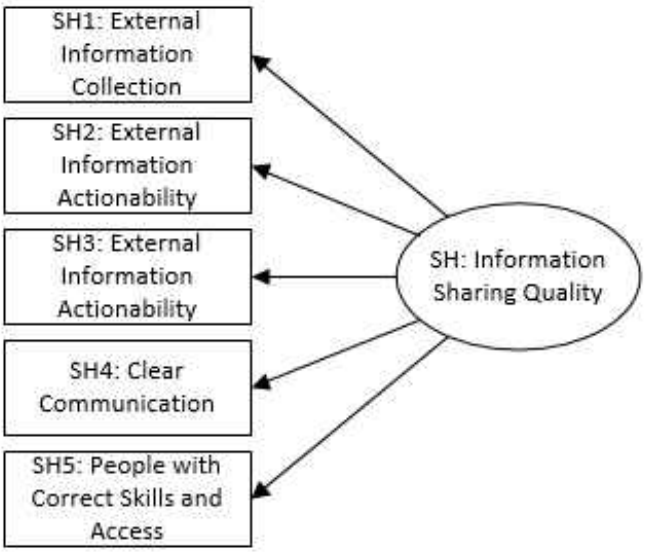


Figure 8 Information Sharing Quality Measurement Model

Table 5 Information Sharing Quality Indicators

Indicator	Variable Type	Dimension	Survey Statement (1=disagree, 7=agree)
SH1	Measured	External Information Collection	Our team gets appropriate information from industry sources to recognize risks, threats, and vulnerabilities to our system (Diebold et al., 2013)
SH2	Measured	External Information Actionability	Our team can take effective action using security information we receive from external sources, such as E-ISAC. (Diebold et al., 2013)
SH3	Measured	Outbound Information Sharing	Our team shares security information that we have with our partners such as E-ISAC and the Reliability Coordinator (Diebold et al., 2013)
SH4	Measured	Clear Communication	Our team shares security information effectively between teams and with incident response leaders in a standardized format. (Bigley & Roberts, 2001; Department of Homeland Security, 2008)
SH5	Measured	People with Correct Skills and Access	Our team shares security information to the correct personnel that can make effective use of the information. (Mateski et al., 2012)

3.4.4 Situational Awareness Confidence Measurement Model

Table 6 identifies five measurements to survey that assesses the situational awareness confidence latent variable. Figure 9 shows the measurement model. The measurement objectives highlight the ideas of Endsley's model (2012) of situational awareness, which is based around perception, comprehension, and projection. The indicators target a shared situation awareness viewpoint, based on the idea that a cybersecurity incident response team and not individuals respond to an incident.

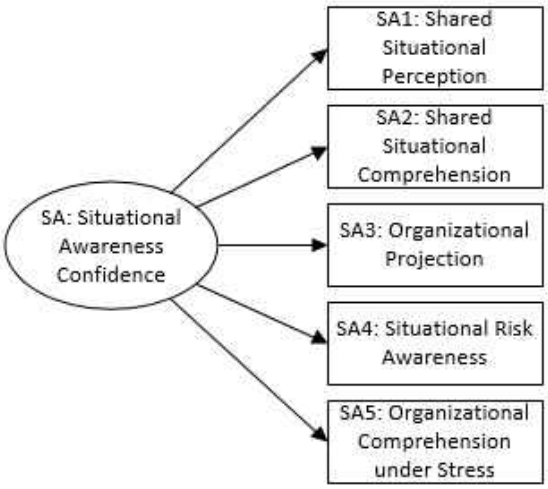


Figure 9 Situational Awareness Confidence Measurement Model

3.4.5 Incident Response Plan Adequacy Measurement Model

Table 7 identifies six measurements to survey that assesses the situational awareness confidence latent variable. Figure 10 shows the measurement model. The measurement

objectives highlight that adequate skilled people, appropriate tools, and resources are necessary to respond to an incident. Additionally, the questions address confidence in the plan to detect, contain, and eradicate an intrusion into the network and to appropriately address various types of events with different impacts.

Table 6 Situational Awareness Confidence Indicators

Indicator	Variable Type	Dimension	Survey Statement (1=disagree, 7=agree)
SA1	Measured	Shared Situational Perception	Our organization is unable to assess and understand security issues as they happen allowing the situation to deteriorate. (reverse encoded question) (US-Canada Power System Outage Task Force, 2004)
SA2	Measured	Shared Situational Comprehension	Our organization has the ability to develop a strong shared comprehension of the situation that is free of conflicts. (Kaber & Endsley, 1998)
SA3	Measured	Organizational Projection	Our team would struggle to forecast what could happen next during an incident. (reverse encoded question) (D'Amico et al., 2005)
SA4	Measured	Situational Risk Awareness	Our team has the appropriate skills and training to respond to most incidents that could be identified. (Webb et al., 2014)
SA5	Measured	Organizational Comprehension under Stress	Our team is able to effectively communicate and receive information from disparate sources and draw effective conclusions during an incident. (Bigley & Roberts, 2001)

3.4.6 Summarized Survey Statements and Indicators

Table 8 presents a summarized version of the statements evaluated by respondents for each indicator variable and the associated latent variable.

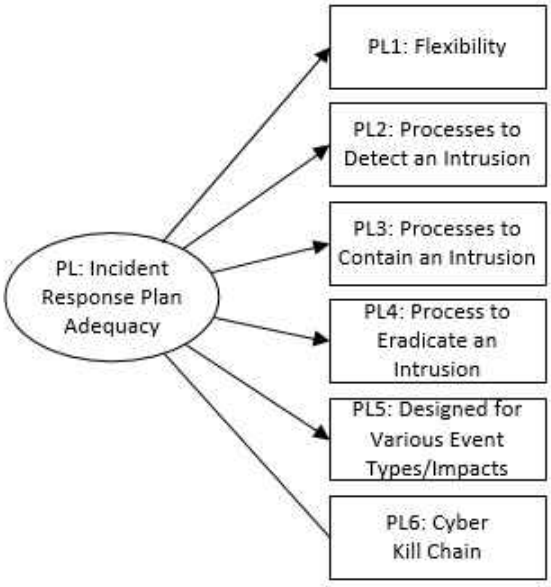


Figure 10 Incident Response Plan Adequacy Measurement Model

Table 7 Incident Response Plan Adequacy Indicators

Indicator	Variable Type	Dimension	Survey Statement (1=disagree, 7=agree)
PL1	Measured	Flexibility	Our team's incident response plan is flexible and able to deal with a wide variety of cyber-attacks. (West-Brown et al., 2003)
PL2	Measured	Processes to Detect an Intrusion	Our team understands how it would detect an intrusion in a timely manner when it occurs using the tools available. (Cichonski et al., 2012)
PL3	Measured	Processes to Contain an Intrusion	Our team is able to detect an intrusion in a timely manner when it occurs using the tools available. (Cichonski et al., 2012)
PL4	Measured	Process to Eradicate an Intrusion	Our team has planned how to eliminate an intrusion or malware. (Cichonski et al., 2012)
PL5	Measured	Designed for Various Event Types/Impacts	Our team knows how to adjust and adapt plans for both small and large scale cyber-attacks (NERC, 2019c)
PL6	Measured	Cyber Kill Chain	Our team's incident response plan considers the various stages of an attack from initial intrusion through the attack that could crash the power grid. (Assante & Lee, 2015)

3.4.7 Demographics, Information Protection, and Data Privacy

Demographic information that could be used to identify individuals or companies could place companies at risk either through the audit processes or investigations if a cybersecurity incident later occurs. Additionally, information such as the IP address of the respondent cannot be maintained. While limiting certain types of analysis that could be performed, it is a necessary limitation on the study.

Demographic data collected includes the type of company, which included investor-owned utilities, public power companies, and cooperative power companies. The self-identified role during a cybersecurity incident was also asked.

3.5 Procedures

3.5.1 Institutional Review Board (IRB) Approval

The survey instrument was reviewed and determined to be exempt by the University of Central Florida Institutional Review Board. A copy of this determination is in Appendix A. The survey presented am All persons responding to the survey did so voluntarily.

3.5.2 Anonymity

Due to the nature of the industry, anonymity was considered a paramount priority due to the nature of the regulations the industry operates under, specifically including reliability

standard CIP-011-2 (NERC, 2019c) addressing Bulk Electric System Cyber System Information (BCSI). All questions were carefully worded not to include questions related to BCSI. No opportunity was given to provide information on the electronic survey that could disclose anonymity.

3.5.3 Participant Recruitment

Volunteers were recruited using various methods. The recruiting approach used public and or personal invitations at electric sector meetings, including:

- NERC Critical Infrastructure Protection Committee
- Florida Reliability Coordinating Council Critical Infrastructure Protection Subcommittee
- Reliability First Infrastructure Protection Committee
- NERC Grid Security Conference
- Indiana Electric Cooperatives Technical Committee
- Illinois Electric Cooperatives Technical Committee
- NRECA TechAdvantage Conference
- SANS Industrial Control Systems Conference

As many of these conferences specifically focused on power grid cybersecurity and therefore included personnel with companies pre-disposed to good security practices, two targeted mailing lists were used to invite additional participants. A total of 229 complete and usable surveys were collected. Due to the method of recruitment, it is impossible to determine an overall response rate.

Table 8 Summarized Surveys Statement for Indicators and Latent Variables

Variable	Variable Type	Dimension	Survey Statement (1=disagree, 7=agree)
SH	Exogenous Latent	Information Sharing Quality	
SH1	Measured	External Information Collection	Our team gets appropriate information from industry sources to recognize risks, threats, and vulnerabilities to our system (Diebold et al., 2013)
SH2	Measured	External Information Actionability	Our team can take effective action using security information we receive from external sources, such as E-ISAC. (Diebold et al., 2013)
SH3	Measured	Outbound Information Sharing	Our team shares security information that we have with our partners such as E-ISAC and the Reliability Coordinator (Diebold et al., 2013)
SH4	Measured	Clear Communication	Our team shares security information effectively between teams and with incident response leaders in a standardized format. (Bigley & Roberts, 2001; Department of Homeland Security, 2008)
SH5	Measured	People with Correct Skills and Access	Our team shares security information to the correct personnel that can make effective use of the information. (Mateski et al., 2012)
SA	Endogenous Latent	Situational Awareness Confidence	
SA1	Measured	Shared Situational Perception	Our organization is unable to assess and understand security issues as they happen allowing the situation to deteriorate. (reverse encoded question) (US-Canada Power System Outage Task Force, 2004)
SA2	Measured	Shared Situational Comprehension	Our organization has the ability to develop a strong shared comprehension of the situation that is free of conflicts. (Kaber & Endsley, 1998)
SA3	Measured	Organizational Projection	Our team would struggle to forecast what could happen next during an incident. (reverse encoded question) (D'Amico et al., 2005)
SA4	Measured	Situational Risk Awareness	Our team has the appropriate skills and training to respond to most incidents that could be identified. (Webb et al., 2014)
SA5	Measured	Organizational Comprehension under Stress	Our team is able to effectively communicate and receive information from disparate sources and draw effective conclusions during an incident. (Bigley & Roberts, 2001)
	Exogenous Latent	Incident Response Exercise Learning	
EX1	Measured	Adequate Exercise Design	Our team performs incident response exercises that test how well information is shared between teams. (NERC, 2012, 2014, 2016d)
EX2	Measured	Lessons Learned Captured	After an exercise, we carefully reviews and documents the lessons learned. (NERC, 2019c)
EX3	Measured	Information Sharing During Exercise	Our exercises effectively test the sharing of information. (Diebold et al., 2013; NERC, 2016d)
EX4	Measured	Exercise Situational Awareness	Our exercise effectively test the ability of teams to develop a shared situational awareness of events. (Kaber & Endsley, 1998; NERC, 2016d)
EX5	Measured	Exercise Incident Command	Our exercises effectively exercise the incident command structure and support staff to ensure clear responsibility and authority. (Department of Homeland Security, 2008)
PL	Endogenous Latent	Incident Response Plan Adequacy	
PL1	Measured	Flexibility	Our team's incident response plan is flexible and able to deal with a wide variety of cyber-attacks. (West-Brown et al., 2003)
PL2	Measured	Processes to Detect an Intrusion	Our team understands how it would detect an intrusion in a timely manner when it occurs using the tools available. (Cichonski et al., 2012)
PL3	Measured	Processes to Contain an Intrusion	Our team is able to detect an intrusion in a timely manner when it occurs using the tools available. (Cichonski et al., 2012)
PL4	Measured	Process to Eradicate an Intrusion	Our team has planned how to eliminate an intrusion or malware. (Cichonski et al., 2012)
PL5	Measured	Designed for Various Event Types/Impacts	Our team knows how to adjust and adapt plans for both small and large scale cyber-attacks (NERC, 2019c)
PL6	Measured	Cyber Kill Chain	Our team's incident response plan considers the various stages of an attack from initial intrusion through the attack that could crash the power grid. (Assante & Lee, 2015)

3.5.4 Review of Descriptive Statistics

Descriptive statistics are analyzed to determine internal consistency and normality. The reviewed statistics include range, mean, standard deviation, skewness, kurtosis, and Cronbach's alpha. As the format of the survey is a Likert scale, it is expected the range for all variables, excluding categorical demographic data, will be between 1-7. IBM SPSS® Version 26 is used to perform these tests.

The means and standard deviation identify the average response and extent of deviation of the responses assuming a normally distributed response. Skewness is a measure of symmetry or the distortion of the data set with a value of 0, indicating the data matches a normal curve exactly. High kurtosis indicates that the data has heavy tails, with the extreme case being a uniform distribution. Significant skewness and kurtosis indicate the data is not normally distributed. Skewness and kurtosis should both be less than 2.0 if the data are normally distributed (Cameron, 2004). Normality is preferred, but not explicitly required for PLS-SEM (Joseph F. Hair et al., 2014).

Cronbach's alpha is a measure of internal consistency, or a measure of how consistently individuals rate items in a scale. The data is further reviewed to consider the effect of eliminating any single term to identify if removal of a variable increases the alpha to identify if the responses to the statement are inconsistent with the remaining terms (Vaske, Beaman, & Sponarski, 2017). While Cronbach's alpha will also be calculated as part of the PLS-SEM

analysis, it is separately performed first to ensure that the collected data is appropriate for analysis.

Inter-item correlation is an alternative measure of internal consistency. Inter-item correlation indicates an overall view of how well the items are correlated. inter-item correlations above 0.4 indicate the items address the same characteristic (Gliem & Gliem, 2003).

Excessive collinearity is an additional concern. Pearson's coefficient identifies if a linear relationship is present between two values based on normally distributed variables (Akoglu, 2018). Values above 0.85 indicate a higher likelihood of issues related to collinearity.

3.5.5 PLS-SEM Model

SmartPLS 3 is used to identify and test the final model using PLS-SEM using the consistent PLS model. Calculations are initially performed on the outer model using the factor weighting scheme and then followed up with the path weighting scheme for evaluation of the final model. Bootstrapping is used to identify statistical significance and p-values. Complete bootstrapping with 5000 samples was selected.

The first set of targets is related to the outer measurement model. There are four sets of tests to evaluate the model. Indicator reliability is measured using the outer loadings in the model. Loadings need to be adequate to add value to the model. Hair et al. (2019) have identified that loadings above 0.7 are preferred, and loadings above 0.5 are appropriate for use in the model.

Indicator reliability is assessed using the outer loadings (indicator loadings) that represent the simple correlations between measured variables and the associated latent variable. The preferred minimum of 0.7 comes from the fact that a loading of 0.708 is representative of 50% of an item's variance (Joseph F Hair, Risher, Sarstedt, & Ringle, 2019). However, it is common to find a few outer loadings in a measurement model to be less than 0.7. Indicators with loadings less than 0.4 should be dropped (Hulland, 1999).

Three different measures are commonly used to measure internal consistency (Joseph F Hair et al., 2019). Each of these are related and has targets between 0.7 and 0.9, with values above 0.95 considered representative of redundant items. Cronbach's alpha is considered a conservative measure of reliability, whereas composite reliability (Jöreskog, 1971) is considered a liberal measure of reliability. The difference is that composite reliability is weighted based on the indicator's loadings. The ρ_A measure (Dijkstra & Henseler, 2015)is used as a compromise between Cronbach's alpha and composite reliability (Joseph F Hair et al., 2019).

Convergent validity is measured using the average variance extracted (AVE). An acceptable AVE is considered 0.5, indicating that at least half of the variance in the items is explained (Joseph F Hair et al., 2019). These assessments are summarized in Table 9.

The second set of assessments relates to the structural model include collinearity, model fit, effect size, and the statistical significance of the path coefficients.

Table 9 Summary of the Measurement Model Validity Assessments

	Measurement	**Target**	**Supporting Literature**
Indicator reliability	Outer loadings	> 0.7 Preferred > 0.5 Acceptable	Hair et al. (2019)
Internal consistency	Cronbach's alpha	0.7 – 0.9	Hair et al. (2019)
	ρ_A	0.7 – 0.9	Hair et al. (2019)
	Composite reliability	0.7 – 0.9	Hair et al. (2019)
Convergent validity	Average variance extracted (AVE)	> 0.5	Hair et al. (2019)
Discriminant validity	Heterotrait-monotrait ratio (HTMT)	< 0.85 Preferred 0.85 - 0.90 Acceptable	Hair et al. (2019)

Collinearity is present when the predictor variables are correlated and can bias model results and is measured using variance inflation factors (VIF). Values above 5.0 indicate collinearity issues, and values between 3.0 and 5.0 indicate concern. Ideally, values should be below or at least near 3.0 (Joseph F Hair et al., 2019).

For model fit, the coefficient of determination or R^2 for endogenous variables should have values of at least 0.75, 0.50, and 0.25, which are considered substantial, moderate, and weak while an R^2 value (Joseph F Hair et al., 2019). R^2 greater than 0.9 indicates an overfit that includes noise in the model. For this model, the incident response plan adequacy has a strong coefficient of determination, while situational awareness confidence has a moderate coefficient of determination.

Model fit in covariance-based SEM is often analyzed using the standardized root mean square error (SRMR), which measures the Euclidean distance between the empirical correlation matrix and the model implied matrix model implied. Hu and Bentler (1999) defined a cutoff of

0.8 for covariance-based SEM models. No defined value is widely accepted, though the acceptable value for PLS-SEM would likely be higher than 0.8. (Joseph F. Hair et al., 2014) Another journal article takes the position that a cutoff value of 0.08 is considered reasonable (Henseler, Hubona, & Ray, 2016). For this analysis, an SRMR will be reported, but no applicable target value will be applied.

Cohen (1988) identified the f^2 statistic to measure effect sizes with at least 0.02 for a small effect, 0.15 for a medium effect, and 0.35 for a large effect.

The capability of model prediction can be evaluated using the blindfolding procedure. Stone-Geisser's Q^2 criterion evaluates the capability of the model to predict endogenous latent variables. Q^2 values greater than zero indicates predictive value for the model path, while values of less than zero indicate the path does not have predictive value.

Table 10 summarizes the assessment parameters for the structural model validity assessments.

Table 10 Summary of the Structural Model Validity Assessments

	Measurement	**Target**	**Supporting Literature**
Collinearity	Variance inflation factor (VIF)	< 3 Preferred 3 – 5 Acceptable	Hair et al. (2019)
Model fit	R^2	> 0.90 Overfit > 0.75 Substantial > 0.50 Moderate > 0.25 Weak	Hair et al. (2019)
	SRMR	<0.08 Preferred	Henseler, Hubona, & Ray (2016)
Effect size	f^2	> 0.02 Small > 0.15 Medium > 0.35 Large	Cohen (1988)
Path Coefficient for direct and indirect effects	p-value	< 0.05	Hair et al. (2019); Hulland (1999)
Model Prediction Capability	Q^2	>0	Hair, Ringle, & Sarstedt (2011); Shanmugapriya & Subramanian (2016)

CHAPTER 4: RESEARCH FINDINGS

4.1 Introduction

Research findings include the responses, demographics, data, and associated descriptive statistical results from the survey are reported. Path analysis using partial least squares analysis is used, which bases estimates on explaining the maximum amount of variance.

4.2 Survey Results

Respondents evaluated the 21 survey statements previously shown in Table 8 on a seven-point Likert scale ranging from strongly disagree (1) through neutral (4) to strongly agree (7). Two questions were reverse encoded in the language, and those responses were inverted after data collection. Each of these statements was treated as measured variables and associated with a hypothesized latent variable. The survey also included eight additional statements related to perceived organizational readiness, but those statements are not used in this analysis.

Data were filtered using three factors to remove any unengaged responses using three techniques. First, at least 28 of the original 29 survey statements needed to be evaluated and responses. Second, rejected responses included those with a standard deviation across all evaluated statements of less than 0.4 either before or after inverting the reverse encoded questions. Third, data excluded cases where the respondent did not recognize that the reverse encoded questions. As shown in Table 11, 229 surveys are used in the analysis. Six respondents

that omitted evaluating one statement had the omitted response imputed by inspection of the associated evaluated statements.

Table 11 Survey Responses

Web-based responses during e-mail campaign	41
Other electronic responses	202
Paper responses	20
Total surveys received	263
Abandoned surveys with at least one and less than 28 of 29 statements evaluated (all discarded surveys had 24 or fewer responses)	32
All 29 statements evaluated	231
Non-engaged responses (standard deviation < 0.4) or clearly did not recognize reverse encoded questions	8
28 statements evaluated with one imputed response	6
Surveys analyzed in the study	229

A portion of the emails sent during the email campaign used a targeted mailing service provided by a media company that provided response rate information. They reported that 5.7% of emails were opened, and the survey link was clicked on in 0.4% of email messages. Overall, 64 surveys were opened and started resulting in 41 surveys completed during the email campaign.

Demographic questions included asking the role in the company and whether the company was an investor-owned utility, municipal utility, or cooperative. As can be seen in Tables 12 and 13, responses from electric cooperatives are over-represented in the responses, and personnel that directly operated the power grid is under-represented.

Table 12 Role Played in Incident Response

Role	Respondents
Power Grid Manager	12
Power Grid Operator	10
Cyber Incident Response Manager	33
Cyber Incident Responder	40
Overall Management	73
Other	59
No response	2

Table 13 Type of Company

Type of Company	Respondents
Investor owner utility	55
Electric cooperative	126
Municipal or other government electric power company	42
No Response	6

Many of the surveys were completed during industry events such as conferences and meetings. To ensure anonymity was maintained, no records were kept of specific invitations. Some invitations were general announcements, and others were direct invitations.

While it is not possible to fully characterize a typical respondent that completed the survey at an industry event, it is possible to draw some summary conclusions about those that participated. The groups of participants can be divided into two types. There are two typical participant type. These descriptions are clearly generalizations based on the observation of participants in meetings.

The first group are those that participated at NERC and other large meetings. These participants may have from all regions of mainland United States and the Provinces of Canada, but do not typically include representatives of Baja California, the Territories of Canada, or the U.S. Territories. Respondents are more likely to be male. They typically included motivated personnel with responsibility either for cybersecurity or regulatory compliance. In general, respondents are likely to at least ten years of professional and management experience and predominantly male.

Participation at other meetings were predominantly from a single type of company or region of the country. They were more likely to be individual contributors, though managers would be represented as well. They likely had at least five years of experience, more likely to be technically focused and more likely male.

While survey participation was clearly not viral, it is known that invitations were passed along by others to members of the Canadian Electricity Association, and at least four cooperative associations, and at least two NERC regions. At least one vendor in the industry also shared invitations with their customers.

4.3 Descriptive Statistics - Normality, Internal Consistency, and Collinearity

Normality is measured using skewness and kurtosis. All variables are normally distributed, with absolute values less than 2.0 (Cameron, 2004), as shown in Table 14.

Cronbach's alpha is a test of internal consistency that measures if the respondents as a group responded consistently (Vaske et al., 2017), as shown in Table 14. Values above 0.7 demonstrate internal consistency, while values above 0.9 indicate potential collinearity due to redundancy (Joseph F Hair et al., 2019). Both incident response plan adequacy and incident response exercise lessons learned have values above 0.9. Cronbach's alpha concerns will be addressed during model evaluation by removing indicator variables.

Inter-item correlations, another test of internal consistency, indicates that the items address the same characteristic with all values above the 0.4 minimum (Gliem & Gliem, 2003).

Table 14 Descriptive Statistics

	Range	Mean	Standard deviation	Skewness	Kurtosis	Cronbach's alpha	Cronbach's alpha with item excluded	Mean inter-item correlation
EX1	1-7	5.15	1.594	-0.935	-0.127		0.910	
EX2	1-7	5.34	1.597	-1.080	0.323		0.900	
EX3	1-7	4.76	1.587	-0.555	-0.639	0.921	0.890	0.701
EX4	1-7	4.79	1.621	-0.598	-0.642		0.896	
EX5	1-7	4.82	1.697	-0.593	-0.705		0.919	
SH1	1-7	5.29	1.495	-1.131	0.721		0.809	
SH2	1-7	5.14	1.507	-0.589	-0.453		0.781	
SH3	1-7	4.72	1.626	-0.744	-0.263	0.838	0.813	0.510
SH4	1-7	4.31	1.593	-0.419	-0.793		0.804	
SH5	1-7	5.20	1.442	-0.968	0.534		0.818	
SA1	1-7	5.28	1.481	-0.899	-0.198		0.795	
SA2	1-7	4.80	1.295	-0.620	0.120		0.785	
SA3	1-7	4.58	1.495	-0.289	-0.792	0.820	0.791	0.481
SA4	1-7	5.24	1.414	-0.968	0.535		0.773	
SA5	1-7	5.08	1.283	-0.960	0.763		0.780	
PL1	1-7	5.19	1.467	-0.934	0.324		0.884	
PL2	1-7	5.25	1.319	-1.127	1.160		0.886	
PL3	1-7	5.27	1.365	-1.014	0.500		0.883	
PL4	2-7	5.36	1.396	-1.079	0.583	0.904	0.887	0.614
PL5	1-7	4.97	1.360	-0.983	0.660		0.883	
PL6	1-7	4.68	1.549	-0.726	-0.250		0.896	

Pearson's coefficients for all measured variables in each of the hypothesized latent variables have a significant p-value of 0.000, indicating correlation is present. Pearson's coefficient identifies if a linear relationship is present between two values for normally distributed variables (Akoglu, 2018). The bivariate Pearson's coefficient for each group of variables is shown in Tables 15-18, demonstrating that a linear relationship is present for all variables in each latent variable.

Table 15 Pearson's Correlation for Incident Response Exercise Learning

		EX1	EX2	EX3	EX4	EX5
Adequate Exercise Design (EX1)	Pearson Correlation	1				
	Sig. (2-tailed)					
Lessons Learned Captured (EX2)	Pearson Correlation	0.736	1			
	Sig. (2-tailed)	0.000				
Exercise Information Sharing (EX3)	Pearson Correlation	0.791	0.779	1		
	Sig. (2-tailed)	0.000	0.000			
Exercise Situational Awareness (EX4)	Pearson Correlation	0.628	0.713	0.787	1	
	Sig. (2-tailed)	0.000	0.000	0.000		
Exercise Incident Command (EX5)	Pearson Correlation	0.554	0.621	0.639	0.764	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	

Table 16 Pearson's Correlation for Information Sharing Quality

		SH1	SH2	SH3	SH4	SH5
External Information Collection (SH1)	Pearson Correlation	1				
	Sig. (2-tailed)					
External Information Actionability (SH2)	Pearson Correlation	0.673	1			
	Sig. (2-tailed)	0.000				
Outbound Information Sharing (SH3)	Pearson Correlation	0.442	0.553	1		
	Sig. (2-tailed)	0.000	0.000			
Outbound Information Sharing (SH3)	Pearson Correlation	0.426	0.556	0.533	1	
	Sig. (2-tailed)	0.000	0.000	0.000		
People with Correct Skills and Access (SH5)	Pearson Correlation	0.468	0.478	0.434	0.533	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000

Table 17 Pearson's Correlation for Situational Awareness Confidence

		SA1	SA2	SA3	SA4	SA5
External Information Collection (SA1)	Pearson Correlation	1				
	Sig. (2-tailed)					
Shared Situational Comprehension (SA2)	Pearson Correlation	0.440	1			
	Sig. (2-tailed)	0.000				
Organizational Projection (SA3)	Pearson Correlation	0.503	0.456	1		
	Sig. (2-tailed)	0.000	0.000			
Situational Risk Awareness (SA4)	Pearson Correlation	0.479	0.452	0.486	1	
	Sig. (2-tailed)	0.000	0.000	0.000		
Organizational Comprehension under Stress (SA5)	Pearson Correlation	0.399	0.577	0.418	0.601	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	

Table 18 Pearson's Correlation for Incident Response Plan Adequacy

		PL1	PL2	PL3	PL4	PL5	PL6
Flexibility (PL1)	Pearson Correlation	1					
	Sig. (2-tailed)						
Processes to Detect an Intrusion (PL2)	Pearson Correlation	.626	1				
	Sig. (2-tailed)	0.000					
Processes to Contain an Intrusion (PL3)	Pearson Correlation	.654	.716	1			
	Sig. (2-tailed)	0.000	0.000				
Process to Eradicate an Intrusion (PL4)	Pearson Correlation	.628	.570	.698	1		
	Sig. (2-tailed)	0.000	0.000	0.000			
Designed for Various Event Types (PL5)	Pearson Correlation	.631	.597	.601	.624	1	
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		
Cyber Kill Chain (PL6)	Pearson Correlation	.581	.567	.494	.534	.686	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	

4.4 Partial Least Squares Structural Equation Modeling (PLS-SEM) Model

The hypothesized structural causal path model was identified from the survey data collected and is shown in Figure 11.

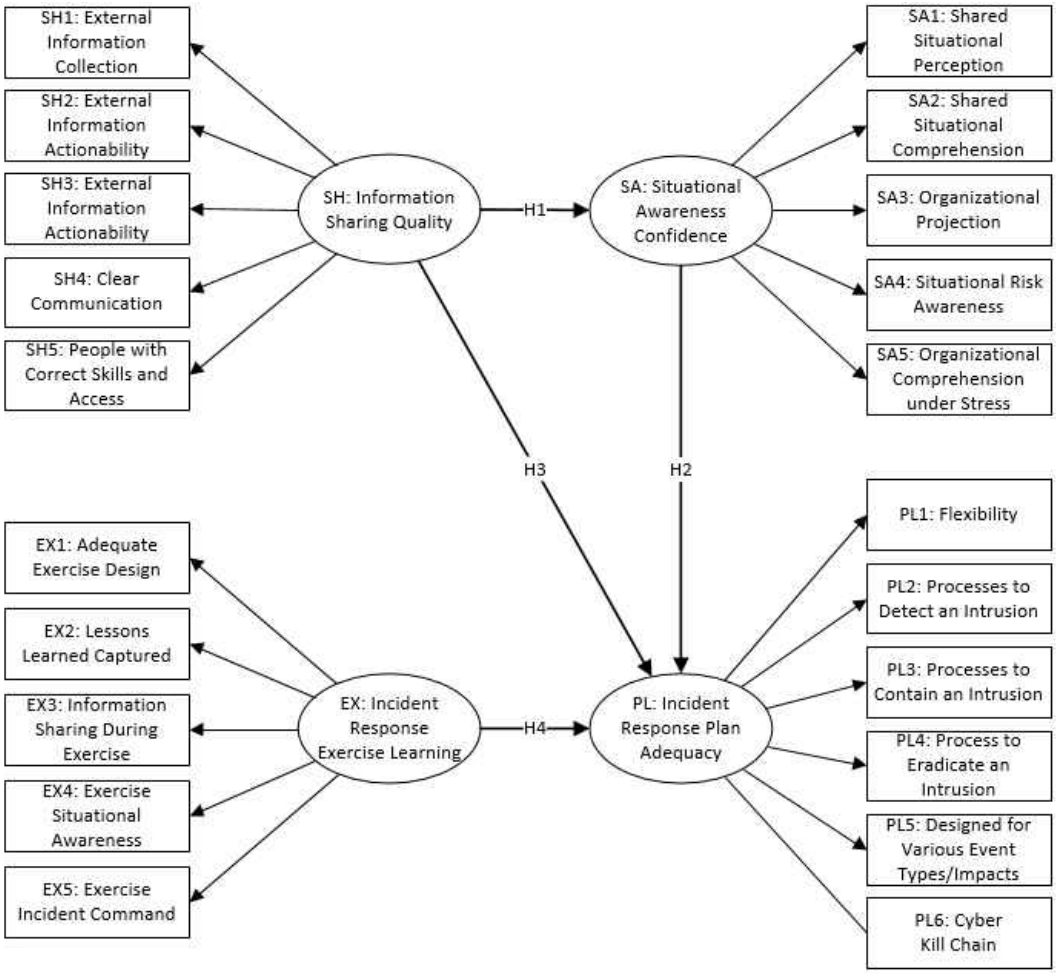


Figure 11 Hypothesized PLS-SEM Causal Model

The associated hypotheses for the model include:

- H1: Perceived information sharing quality has a positive and significant effect on perceived situational awareness confidence
- H2: Perceived situational awareness confidence has a positive and significant effect on perceived incident response plan adequacy
- H3: Perceived information sharing quality has a positive and significant effect on perceived incident response plan adequacy
- H4: Perceived exercise response learning has a positive and significant effect on perceived incident response plan adequacy

The hypothesized identified model represents two exogenous variables representing information sharing quality (SH) and incident response exercise lessons learned (EX). The model also includes two endogenous variables representing situational awareness confidence (SA) and incident response plan adequacy (PL).

Thee variables were discarded during model analysis.:

- EX3 removed to address excess collinearity and to reduce overall Cronbach's alpha
- PL5 removed to address excess collinearity and to reduce overall Cronbach's alpha.
- SA1 removed to address low average variance extracted

SmartPLS version 3 is used to perform the PLS analysis. The basic PLS algorithm used includes (SmartPLS):

1. Outer approximation of the latent variable scores,
2. Estimation of the inner weights,
3. Inner approximation of the latent variable scores
4. Estimation of the outer weights

The consistent PLS (PLSc) algorithm adds a correction to address for inconsistency in PLS estimates for reflexive variables by adding a correction for path coefficients, inter-construct correlations, and indicator loading. The PLSc algorithm extends the base PLS algorithm by adding additional steps (Dijkstra & Henseler, 2015):

5. Estimate reliability
6. Correct for attenuation
7. Estimate consistent coefficients

The data is analyzed using the PLSc algorithm. Where needed, bootstrapping with the complete bootstrapping option with 1000 iterations is used to provide p-values for tests where a p-value is needed.

4.5 Model Results

Structural equation models include two submodels, an inner structural model and an outer measurement model. The measurement identifies the linear relationship between the measured indicator variables and the associated latent variables. The structural model identifies the linear relationship between endogenous and exogenous latent variables (Wong, 2013). Note that all results shown except where noted reflect the final model, including only statistically significant paths and indicators retained in the final model.

4.5.1 Measurement Model Analysis

The indicators being analyzed are reflexive, which was previously confirmed by Cronbach's alpha and mean inter-item correlation. When using reflexive variables, PLS-SEM factors to consider include indicator reliability, internal consistency, convergent validity, and discriminant validity (Joseph F Hair et al., 2019).

Indicator reliability is assessed using the outer loadings (indicator loadings) that represent the simple correlations between measured variables and the associated latent variable. The preferred minimum is 0.7. However, it is common to find a few outer loadings in a measurement

model to be less than 0.7. Indicators with loadings less than 0.4 should be dropped (Hulland, 1999). Table 19 shows the outer loadings with 13 measured variables having a loading above 0.7, and the remaining five measured variables have a loading above 0.6.

Three related calculations measure internal consistency and reliability, including Cronbach's alpha, ρ_A, and composite reliability, with targets between 0.7 and 0.9 with values above 0.95 indicative of redundant items (Joseph F Hair et al., 2019). Cronbach's alpha is considered a conservative measure of reliability, whereas composite reliability (Jöreskog, 1971) is considered a liberal measure of reliability. The ρ_A measure used to adjust results in the consistent PLS algorithm (Dijkstra & Henseler, 2015) compromises between Cronbach's alpha and composite reliability (Joseph F Hair et al., 2019). All variables have values for each of these measures between 0.7 and 0.9, as shown in Table 20.

Convergent validity is measured using the average variance extracted (AVE). An acceptable AVE is considered 0.5, indicating that at least half of the variance in the items is explained (Joseph F Hair et al., 2019). The average variance is at or above 0.5 for all variables. The results for internal consistency and convergent validity are shown in Table 20.

Table 19 Outer loadings of the Measured Variables on the Latent Variables

Endogenous Variable	Exogenous Variable	Outer Loading
Information Sharing Quality (SH)	External Information Collection (SA1)	0.654
	External Information Actionability (SH2)	0.678
	Outbound Information Sharing (SH3)	0.666
	Clear Communication (SH4)	0.724
	People with Correct Skills and Access (SH5)	0.825
Situational Awareness Confidence (SA)	Shared Situational Perception (SA1)	Discarded
	Shared Situational Comprehension (SA2)	0.641
	Organizational Projection (SA3)	0.630
	Situational Risk Awareness (SA4)	0.757
	Organizational Comprehension under Stress (SA5)	0.797
Incident Response Exercise Learning (EX)	Adequate Exercise Design (EX1)	0.822
	Lessons Learned Captured (EX2)	0.766
	Exercise Information Sharing (EX3)	Discarded
	Exercise Situational Awareness (EX4)	0.856
	Exercise Incident Command (EX5)	0.825
Incident Response Plan Adequacy (PL)	Flexibility (PL1)	0.840
	Processes to Detect an Intrusion (PL2)	0.744
	Processes to Contain an Intrusion (PL3)	0.741
	Process to Eradicate an Intrusion (PL4)	0.776
	Designed for Various Event Types/Impacts (PL5)	Discarded
	Cyber Kill Chain (PL6)	0.786

Table 20 Internal Reliability and Convergent Validity Statistics

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Incident Response Exercise Learning	0.890	0.891	0.890	0.669
Information Sharing Quality	0.839	0.842	0.836	0.507
Situational Awareness Confidence	0.799	0.809	0.801	0.504
Incident Response Plan Adequacy	0.885	0.886	0.885	0.606

Discriminant validity is assessed using the heterotrait-monotrait ratio. Values above either 0.85 for more distinct measures or 0.90 for less distinct measures are suggested as limits. As this is a theoretical model using related reflexive factors, 0.9 would be considered a targeted limit acceptable, and 0.85 is the preferred limit. All values are below 0.85. A summary of these targeted values and values for the structural model addressed next is shown in Table 21.

Table 21 Discriminant Validity HTMT Ratios

	Incident Response Exercise Learning	Information Sharing Quality	Situational Awareness Confidence
Information Sharing Quality	0.709		
Situational Awareness Confidence	0.646	0.804	
Incident Response Plan Adequacy	0.726	0.767	0.832

4.5.2 Structural Model Analysis

Items to assess in the structural model include collinearity, model fit, effect size, and the statistical significance of the path coefficients. Collinearity is present when the predictor variables are correlated and can bias model results and is measured using variance inflation factors (VIF). Values above 5.0 indicate collinearity issues, and values between 3.0 and 5.0 indicate concern (Joseph F Hair et al., 2019). Table 22 shows that one measurement model variable, EX4, has a VIF value of 3.15, with the remaining values below 3.0. Table 23 shows that all structural model VIF values are below 3.0.

Table 22 Measurement Model Collinearity Tests using VIF

	VIF
External Information Collection (SA1)	1.934
External Information Actionability (SH2)	2.349
Outbound Information Sharing (SH3)	1.647
Clear Communication (SH4)	1.800
People with Correct Skills and Access (SH5)	1.585
Shared Situational Comprehension (SA2)	1.646
Organizational Projection (SA3)	1.446
Situational Risk Awareness (SA4)	1.756
Organizational Comprehension under Stress (SA5)	1.923
Adequate Exercise Design (EX1)	2.303
Lessons Learned Captured (EX2)	2.858
Exercise Situational Awareness (EX4)	3.150
Exercise Incident Command (EX5)	2.481
Flexibility (PL1)	2.253
Processes to Detect an Intrusion (PL2)	2.422
Processes to Contain an Intrusion (PL3)	2.887
Process to Eradicate an Intrusion (PL4)	2.262
Cyber Kill Chain (PL6)	1.752

Table 23 Structural Model Collinearity Tests using VIF

	Situational Awareness Confidence	Incident Response Plan Adequacy
Incident Response Plan Adequacy		1.732
Information Sharing Quality	1.000	
Situational Awareness Confidence		1.732

For model fit, the coefficient of determination or R^2 for endogenous variables should have values of at least 0.75, 0.50, and 0.25, which are considered substantial, moderate, and weak while an R^2 value (Joseph F Hair et al., 2019). R^2 greater than 0.9 indicates an overfit that includes noise in the model. For this model, the incident response plan adequacy has a

substantial coefficient of determination, while situational awareness confidence has a moderate coefficient of determination, as shown in Table 24. Model fit may also be analyzed using the standardized root mean square error (SRMR), which measures the Euclidean distance between the empirical correlation matrix and the model implied matrix model implied. While no cutoff A cutoff value of 0.08 is considered reasonable (Henseler et al., 2016). The estimated model had an SRMR of 0.061.

Table 24 Coefficient of Determination for Endogenous Variables

	R^2	R^2 Adjusted
Incident Response Plan Adequacy	0.754	0.752
Situational Awareness Confidence	0.653	0.652

The effect size is measured using the f^2 statistic. Cohen (1988) identified effect sizes for the f^2 statistic of at least 0.02 for a small effect, 0.15 for a medium effect, and 0.35 for a large effect. Incident response exercise lessons learned to incident response plan adequacy has a medium effect. Table 25 shows that incident response exercise lessons learned to incident response plan adequacy has a medium effect, and information sharing quality to situational awareness and situational awareness to incident response plan adequacy each has a large effect.

Table 25 Effect Size for Model Paths

	f^2
Incident Response Exercise Learning → Incident Response Plan Adequacy	0.247
Information Sharing Quality → Situational Awareness Confidence	1.883
Situational Awareness Confidence → Incident Response Plan Adequacy	0.907

Once the model is developed, the capability of model prediction can be evaluated using the blindfolding procedure. Stone-Geisser's Q^2 criterion evaluates the capability of the model to predict endogenous latent variables. Q^2 values greater than zero indicates predictive value for the model path, while values of less than zero indicate the path does not have predictive value. Incident response planning has a Q^2 value of 0.378, and situational awareness confidence has a Q^2 value of 0.267, indicating that the exogenous variables have predictive relevance on the associated endogenous variables. For PLS-SEM, the cross-validated redundancy approach to measuring the Q^2 value for each of the endogenous variables is used (Joe F Hair, Ringle, & Sarstedt, 2011; Shanmugapriya & Subramanian, 2016).

4.5.3 Hypothesis Testing

The selected causal model meets are validity assessments for both the measurement model and the structural model, as shown in Tables 26-27. All assessments are acceptable.

Table 26 Summary of the Measurement Assessment Results

	Measurement	**Target**	**Model results**	**Supporting Literature**
Indicator reliability	Outer loadings	> 0.7 Preferred > 0.5 Acceptable	13 variables preferred 5 variables acceptable	Hair et al. (2019)
Internal consistency	Cronbach's alpha	0.7 – 0.9	All variables in range	Hair et al. (2019)
	ρ_A	0.7 – 0.9	All variables in range	Hair et al. (2019)
	Composite reliability	0.7 – 0.9	All variables in range	Hair et al. (2019)
Convergent validity	Average variance extracted (AVE)	> 0.5	All variables in range	Hair et al. (2019)
Discriminant validity	Heterotrait-monotrait ratio (HTMT)	< 0.85 Preferred 0.85 - 0.90 Acceptable	All variables preferred	Hair et al. (2019)

Table 27 Summary of the Structural Model Assessment Results

	Measurement	**Target**	**Model results**	**Supporting Literature**
Collinearity	Variance inflation factor (VIF)	< 3 Preferred 3 – 5 Acceptable	17 variables preferred 1 variable acceptable	Hair et al. (2019)
Model fit	R^2	> 0.90 Overfit > 0.75 Substantial > 0.50 Moderate > 0.25 Weak	No variables overfit 1 variable substantial 1 variable moderate No variables weak	Hair et al. (2019)
	SRMR	<0.08 Preferred	0.061	Henseler, Hubona, & Ray (2016); Hair et al. (2019)
Effect size	f^2	> 0.02 Small > 0.15 Medium > 0.35 Large	None 1 in range 2 in range	Cohen (1988)
Path Coefficient for direct and indirect effects	p-value	< 0.05	All coefficients in range (all variables ≤ 0.001)	Hair et al. (2019); Hulland (1999)
Model Prediction Capability	Q^2	>0	All endogenous variables above 0	Hair, Ringle, & Sarstedt (2011); Shanmugapriya & Subramanian (2016)

The overall objective of this approach is to identify a significant set of paths in a causal model that addresses an incident response plan's adequacy. The structural model with results shown in Table 26 is significant, with P-values of 0.001 or less for both direct and indirect effects.

Table 28 Causal Model Path Coefficients and Hypothesis Testing

	Hypothesized Path	Original Sample	Sample Mean	Standard Deviation	T statistic	P-Value
H1	Information Sharing Quality → Situational Awareness Confidence	0.808	0.808	0.052	15.505	0.000
H2	Situational Awareness Confidence → Incident Response Plan Adequacy	0.622	0.626	0.100	6.247	0.000
H3	Information Sharing Quality → Incident Response Plan Adequacy	0.547	0.568	0.167	0.754	0.451
H4	Incident Response Exercise Learning → Incident Response Plan Adequacy	0.324	0.319	0.099	3.271	0.001
	Results shown for H1, H2, and H4 are calculated after removal of H3 from model					

Hypothesis testing for the model is shown in Table 29. The final model is shown in Figure 12.

Table 29 Hypothesis Testing Results

	Hypothesis	Result
H1	Perceived information sharing quality has a positive and significant effect on perceived situational awareness confidence	Accepted
H2	Perceived situational awareness confidence has a positive and significant effect on perceived incident response plan adequacy	Accepted
H3	Perceived information sharing quality has a positive and significant effect on perceived incident response plan adequacy	Rejected
H4	Perceived exercise response learning has a positive and significant effect on perceived incident response plan adequacy	Accepted

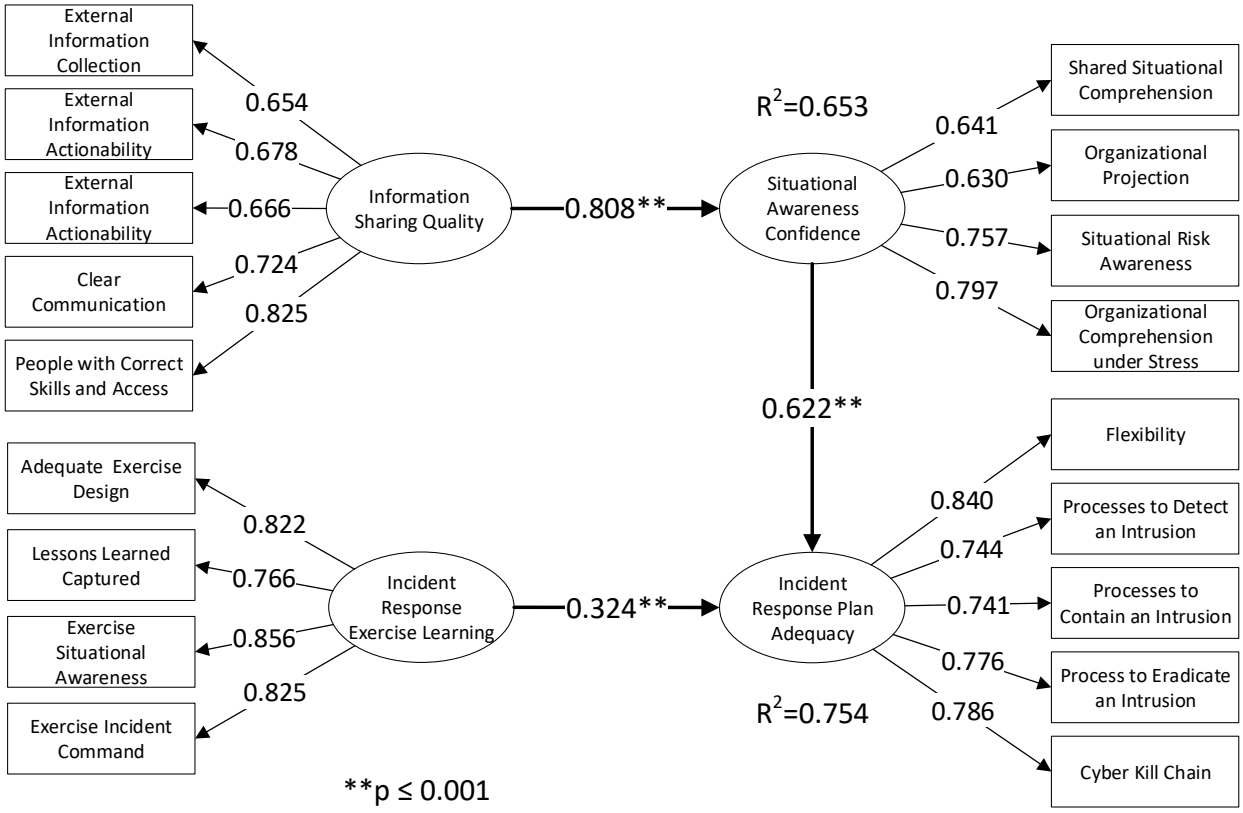


Figure 12 PLS-SEM Causal Model

4.5.4 Importance Performance Map Analysis (IMPA)

With a demonstrated model, additional analysis can be performed to identify improvement opportunities. Importance-performance map analysis is an analytical technique that identifies where to focus future work to gain the most improvement in the target latent variable. IPMA is used to identify predecessors that have a low performance but high importance. A one-unit point Increasing the performance of the predecessor by 1 point increases the performance of target by the total effect size of the predecessor (Farooq, Salam, Fayolle, Jaafar, & Ayupp, 2018; Ringle & Sarstedt, 2016). In this case, improvements to incident response plan adequacy would likely be

the targeted improvement. SmartPLS reports performance in a standardized manner on the Y-axis and the total effect size of a 1-point increase on the X-axis. As can be seen from Figure 13 and Table 30, the most valuable area to focus on to improve incident response plan adequacy is situational awareness confidence. Increasing the overall situational awareness confidence score by 1 point would increase the incident response plan adequacy by 0.542 points.

In addition to reviewing the map at the latent variable, the impact of measured variables can also be mapped. These results for the most important latent variable, situational awareness, are also reported in Table 31. Within situational awareness confidence, variable SA5 representing organizational comprehension under stress has the most impact, with each 1-point increase in the measured variable increasing perceived incident response plan adequacy by 0.16 points.

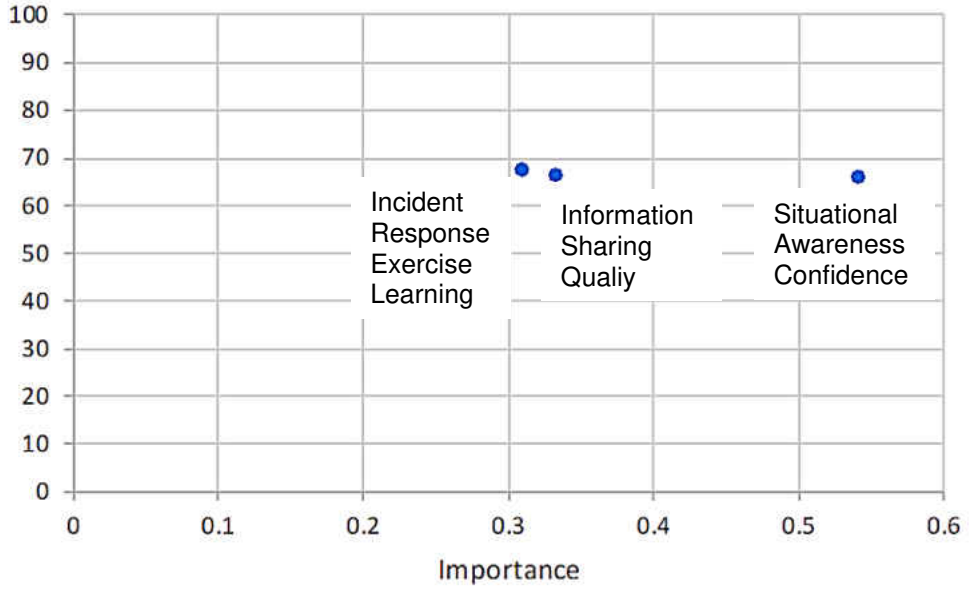


Figure 13 Importance Performance Map for Incident Response Plan Adequacy

Table 30 Importance Performance Results for the Latent Variables

Latent Variable	Importance (Total Effects)	Performance
Incident Response Exercise Learning	0.310	67.177
Situational Awareness Confidence	0.542	65.816
Information Sharing Quality	0.334	66.122

Table 31 Importance Performance Results for Situational Awareness Confidence

Importance (Total Effects)	Importance (Total Effects)	Performance
Shared Situational Comprehension (SA2)	0.118	59.68
Organizational Projection (SA3)	0.138	70.670
Situational Risk Awareness (SA4)	0.160	68.049
Organizational Comprehension under Stress (SA5)	0.067	71.543

CHAPTER 5: CONCLUSION

This research focused on finding a causal path model to understand the relationships between perceived readiness for a cybersecurity incident considering the adequacy of the incident response plan; incident response exercises such as the national GridEx; the perceived quality of information sharing within the electric sector related to cybersecurity risks; and the perceived confidence of situational awareness that would be gained during an incident. This section discusses what can be learned from these results, the implications of the study, and recommendations for future research.

5.1 Discussion

The industry focuses on cybersecurity to ensure grid reliability and resiliency. The electric sector has numerous teams that actively perform research and education, including the NERC Critical Infrastructure Protection Committee, the Electric Power Research Institute, private organizations such as the SANS Industrial Control Systems team, and the Department of Energy National Labs. While extensive research is performed on cybersecurity, no similar study was identified to review how the industry personnel perceive incident response plans.

This study identified that personnel in the electric sector perceive that information sharing quality has a statistically significant causal impact on situational awareness confidence and situational awareness has a significant impact on incident response plan adequacy for cybersecurity incidents in the electric sector. Further, learning from incident response exercises has a significant effect on incident response planning.

These findings demonstrate that the efforts to improve information sharing and situational awareness by the electric sector have been beneficial. These efforts should continue to be enhanced by the electric sector and by other critical infrastructure information sharing and analysis centers. These additional efforts should target improving the situational risk confidence of personnel, especially in the area of situational risk assessment.

The study also verifies that incident response exercises such as GridEx are perceived to improve incident response planning. The exercise requires tremendous effort within NERC, E-ISAC, and electric sector companies. Based on the increasing participation in exercises, the industry recognizes the benefits(NERC, 2012, 2014, 2016d, 2018a).

5.1.1 Information Must Be in Context to Be Useful

A direct path from information sharing to incident response planning was hypothesized as so much emphasis is placed on information sharing in the industry. In retrospect, the non-significance of this path and instead significance of the indirect path through situational awareness is satisfying. Information is critical, but it does not improve the incident response planning process. Instead, it is the ability to analyze and place the information in context that matters. Blindly reacting to information without this context and an understanding of its importance can lead to suboptimal real-time decisions.

5.1.2 Low Response Rates

It is difficult to obtain responses to this type of survey due to real and perceived limitations on responding to a survey that addresses cybersecurity. Controlling information is essential as reconnaissance is the first step in any attack. Each piece of information publicly available that shows a weakness guides the attackers. This survey was carefully constructed to not infringe on the regulatory requirements. The methods used to recruit volunteers resulted in an overrepresentation of cooperatives.

One topic of this research is information sharing. However, one challenge of this survey was an unwillingness to participate in the survey. Response rates were extremely low for emailed surveys, about 0.3%, requiring the use of direct recruitment. As personal interviews were not a survey technique and those that declined never agreed to participate, no records were kept. From an anecdotal viewpoint, one reason people declined to participate was that they were not authorized to discuss anything that may disclose security vulnerabilities.

The target audience of the survey and the difficulty in obtaining responses resulted in overall low variance in the data collected, confounding the results of the survey. This can be seen in the low standard deviation of responses in Table 14, Descriptive Statistics, and also in the high internal reliability for each latent variable in Table 20, Internal Reliability, and Converging Validity Statistics. This low variance may be a result of consistent shared views on the topics by those participating in the survey. Alternatively, it may have resulted from respondents believing

they must respond a certain way should the information ever become public, or they may experience career issues. These are just two possible causes for the consistent viewpoints.

5.1.3 Information Sharing: Public Good vs. Public Right to Know

The industry writes and enforces the Reliability Standards for the bulk power system, and the regulations are generally approved by the Federal Energy Regulatory Commission. In February 2018, NERC issued a $2.7 million penalty (NERC, 2018b) for a significant violation of the information protection requirement against Pacific Gas and Electric (Smith, 2019) under a prior version of Reliability Standard CIP-003 (NERC, 2019c). Typically, the company names of violators are not released as part of the penalty notice by NERC or FERC. In this case, the company was identified by journalists.

This balance of public good, denying critical information to attackers, industry learning from violations, and the public right to know needs to be considered. This obligation needs to be considered by both government agencies and the power grid companies. FERC Commissioner Glick in a statement summarized some of the factors needing to be balanced (Glick, 2019)

- Lack of transparency in the NERC Notice of Penalty process
- Disclosure of company names would act as a further deterrent to violations
- Need to ensure that information useful to an attacker is not released

While the company name has previously not been identified, the specific violations were identified. Companies may, and from personal observation, frequently use this information to improve their programs. A joint FERC and NERC white paper in response to this review would

eliminate detailed violation information and replace this information with the name of the violator, the penalty amount, and the NERC CIP Reliability Standards violated. The specific requirements in Standards would not be released. Otherwise, the attackers would know specific weaknesses to exploit.

5.1.4 Benefits of Confidential Information Sharing

While it is critical for power grid companies not to disclose vulnerabilities, the sharing of information allows all companies to work together to improve security and, therefore electric reliability. This ability to share makes it possible for the industry as a whole to improve capabilities. Other industries have seen similar successes related to safety. NASA, the National Aeronautics and Space Administration, through its Aviation Safety Reporting System, provides confidential reporting and enforcement immunity to those that report incidents (NASA, 2011). Factors in the success of the system include trust, anonymity, and confidentiality. The information collected is used to identify and address safety issues (O'Leary & Chappell, 1996). This system is highly successful, with 94,302 reports received in 2017 (Hooey, 2018). By providing immunity, confidentiality, and trust to controllers, pilots, and companies for information reported, NASA has created a system that encourages reporting of events and therefore increases safety.

Other industries have various reporting systems that have enhanced safety. The MedWatch Safety Information and Adverse Event Reporting System performs this role in the health care sector. The voluntary information from the public and mandatory information from

manufacturers provides a basis for identifying safety risks from products (Craigle, 2007; Han, Ball, Pamer, Altman, & Proestel, 2017). Ahmad (2003) demonstrates the success of the program by listing a dozen different regulatory actions taken by the Food and Drug Administration.

The electric sector collects some of this information through the Electricity Information Sharing and Analysis Center using their private portal. However, personal observation is that only a limited amount of voluntary information gets reported. To make the best use of this tool, increasing the amount of information and useful tools to automate the analysis of information once adequate information is available will improve electric sector capabilities. For electronically collected data, this task is currently performed using the Cybersecurity Risk Information Sharing Program (CRISP), where suitable information is available to analyze. Department of Energy specialists perform this analysis (Department of Energy, 2018). Increased speed identifying events is critical. Just as important is identifying risks to the power grid. The lack of information sharing due to fears of risks becoming public both impedes attackers and the companies.

5.1.5 Lack of History for Cyberattacks with Power Outages

Cyberattacks are frequent in information technology, including the business side of the electric companies. Ransomware has been the prevalent high-profile attack in 2017-2019. In 2019, more than 70 cities have suffered from ransomware (Brumfield, 2019). Utilities have been targeted as well, with one ransomware attack in Johannesburg disrupting the ability for residents to pre-purchase power (Cimpanu, 2019; Manos, 2017; Walton, 2018). However, there have only

been two attacks that have disrupted the power grid, with both occurring in Ukraine (Assante et al., 2016; Assante et al., 2017). The respondents to the survey were communicating their beliefs for a potential power grid cyberattack, not an actual cyberattack.

So far, cyberattacks on the power grid have been high-impact low-frequency events. NERC and the Department of Energy studied three types of these events: coordinated cyber and physical attack, pandemic illness, and geomagnetic and electromagnetic events while acknowledging there are others such as natural disasters, meteor strikes, and war (North American Electric Reliability Corporation & Department of Energy, 2010). Since experience is limited or non-existent in the current environment, other techniques are required. The most damaging effect would be a complete collapse of the power grid.

One study technique focuses on identifying different scenarios that could cause a collapse, hardening those weak points, and taking steps to mitigate these risks. For example, a physical attack on as few as nine strategically placed substations could collapse the power grid under the right circumstances (Tweed, 2014). An additional reliability standard, CIP-014, was added to address this risk (NERC, 2019c). Geomagnetic storms require different types of protections for the power grid, but also focus on vulnerabilities and weak points. The biggest mitigation for both of these events is engineering resilience into the system. Additional power grid resilience contains the impact of an event. Reducing this impact simplifies response and recovery.

Systems and technology are not the only risk. This study focused on people. A severe curtailment of people and resources, such as a pandemic event, would challenge the electric

sector. The power grid depends on a large number of people with specialized skill sets such as power engineers, linemen, and system operators. It is incumbent on electric utilities to understand who the most critical staff are and ensure they and their families get the most protection. People will place family before the power grid.

Further, cyberattacks take advantage of opportunity due to loss of response capability. The simplest example is the increase in fraudulent fund-raising emails following an event such as a hurricane. In the power grid, nation-states take steps to be implanted inside of other countries' power grids should an attack be needed. These capabilities will likely remain unused unless a specific need arises. Resilience, the ability to recover from an event, must consider people as well as processes and technology.

5.2 Study Limitations

In addition to the low response rate previously discussed, the predominant limitation is the homogeneity of the study. The study population was primarily collected through survey invitations at meetings due to the low email response rate. As a result, motivated professionals, especially managers, were the primary respondents. The sample is somewhat biased and resulted in shared, consistent views. Homoscedasticity can lead to imprecise estimates and sensitivity to the choice of the indicators used (Crump, Hotz, Imbens, & Mitnik, 2009). This homoscedasticity is also seen in the Cronbach's alpha statistics shown in Table 14, Descriptive Statistics. Shifting this study from specific research in the electric sector to the broader group of companies that use industrial control systems could address the low response rate and homoscedasticity.

Restricting the sample to the electric sector and focusing so heavily on the power grid also limits the ability to extend the results of the study to other technology sectors. However, the electric sector is unique in the manner it chooses to respond to cybersecurity incidents. Whether or not this uniqueness in its approach is needed can be debated. This debate will become even more important as more sectors take a regulatory approach to information security.

Incident response is just one component of cybersecurity. The Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2018) also addresses risk identification, system protection, attack detection, and recovery. By focusing on a single component, the study is only applicable to incident response. Pairing these results with additional studies that address the remaining framework domains would add context and contribute to a fully functional method to improve cybersecurity in critical infrastructure.

5.3 Future Research

The present study researched specific areas that have been targeted by the industry for improvement. Future work may need to address other areas such as the cybersecurity culture in organizations and the workforce in general. Safety research has demonstrated the importance of safety culture (Lawrie, Parker, & Hudson, 2006; Noort, Reader, Shorrock, & Kirwan, 2016; Shirali, Shekari, & Angali, 2016). Cybersecurity culture is an extension of these well-proven ideas (Da Veiga & Eloff, 2010; Flores, Antonsen, & Ekstedt, 2014).

Another potential research area is to identify how incident response exercises can more effectively build confidence for cybersecurity personnel that would be responding to a power

grid incident. Some in the industry are of the opinion that many smaller companies see these tabletop exercises more as a regulatory checkbox than a learning process. To effectively exercise, these responders need to be pushed beyond the response plan and challenge their capabilities, such as in a GridEx exercise. Through these challenges, people learn how to adapt to the specific event, communicate effectively, and make appropriate decisions.

The recruitment methods and survey statements focused on power grid personnel that would respond to a cybersecurity incident. While these teams focus on the technical aspects, a similar study of system operations personnel responsible for operating the power grid could shed insights. For example, how well do these operators have the ability to recognize a cybersecurity and understand how an incident would affect their operations? Do they distinguish how a cybersecurity incident is different from other significant power grid events? Do they trust their company's cybersecurity capabilities if an incident occurs?

While the data that was collected is inadequate to perform a multigroup analysis based on demographics, another potential approach may be to perform predictive tree analysis. This technique identifies individuals with similar views as clusters and analyzes the difference in the clusters using automatic indicator detector analysis (Wan & Shasky, 2012).

While response is critical, recovery back to the normal state, or at least to a condition that is as near normal as possible, is the end goal. A potential follow-up would be to adapt this type of survey towards recovery and focus more on the people who would be responsible for bringing the attacked portion of the power grid back to life. Significant work has been done related to weather events and blackouts (Duffey & Ha, 2012; Sun, Liu, & Liu, 2011). Understanding the

confidence that the personnel have towards power grid recovery during a cybersecurity event could highlight additional areas of improvement. A critical aspect of this study would be the higher distrust of information provided by control systems in a cybersecurity event than a weather event.

5.4 Conclusion

The results of this study revealed that personnel in the electric sector believe that information sharing quality has an impact on situational awareness confidence, and situational awareness has an impact on incident response plan adequacy for cybersecurity incidents in the electric sector. Further, learning from incident response exercises has an effect on incident response planning.

These findings demonstrate that the efforts by the electric sector to enhance information sharing and situational awareness by NERC and the Electricity Information Sharing and Analysis Center have been beneficial and that these efforts should continue to be enhanced by the electric sector and by other critical infrastructure information sharing and analysis centers. These additional efforts are recommended to focus on improving the situational risk confidence of personnel and that these efforts need to focus on situational risk assessment and training.

The most important aspect of this model is that it is not limited to cyberattacks. The framework developed tying incident response to situational awareness, information sharing, and event exercises would be appropriate to extend to other event types and event response

disciplines. The indicators would need to be customized to the discipline, and no preexisting framework is available.

This study contributes to the body of knowledge by presenting a model that ties together the human factors in power grid incident response. Through this model, the industry can identify where and how to direct future efforts to improve people's capabilities to respond to a cyberattack. While the model developed focused in this limited area, the ideas are readily extensible to other related domains.

APPENDIX A: IRB APPROVAL LETTER

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Joseph Garmon**

Date: **May 29, 2018**

Dear Researcher:

On 05/29/2018, the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination
Project Title:	A Study of Organization Readiness to Respond to a Cyber Security Incident in Power Grid Utilities
Investigator:	Joseph Garmon
IRB Number:	SBE-18-14000
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:

Signature applied by Gillian Morien on 05/29/2018 03:48:56 PM EDT

Designated Reviewer

APPENDIX B: SURVEY INSTRUMENT

Title of research study:
A Study of Organization Readiness to Respond to a Cybersecurity Incident in Power Grid Utilities

Principal Investigator(s): Joe Garmon
Faculty Supervisor: Dr. Waldemar Karwowski

You are being invited to take part in a research study. Whether you take part is up to you.
We invite you to take part in a research study because due to your involvement in or supporting operation of the North American Power Grid. You must be 18 years of age or older to participate in this study.

The purpose of this research is to determine is to study organization readiness to respond to a cyber security incident in power grid utilities. For this research, you are requested to complete the following survey questionnaire.
- All information is collected anonymously
- This survey should take approximately 10 minutes to complete.
- Whether or not you take part is up to you.

Who can I talk to?
Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints is Joe Garmon at 407-718-6542 or jgarmon@knights.ucf.edu

IRB contact about your rights in the study or to report a complaint.
Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been determined to be exempted from IRB review unless changes are made. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901.

Yes, I consent

No, I do not consent

Please indicate how much you agree with the following statements on learning from an incident response exercise.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Our team performs incident response exercises that test how well information is shared between teams.	○	○	○	○	○	○	○
After an exercise, we carefully reviews and documents the lessons learned.	○	○	○	○	○	○	○
Our exercises effectively test the sharing of information.	○	○	○	○	○	○	○
Our exercise effectively test the ability of teams to develop a shared situational awareness of events.	○	○	○	○	○	○	○
Our exercises effectively exercise the incident command structure and support staff to ensure clear responsibility and authority.	○	○	○	○	○	○	○

→

Please indicate how much you agree with the following statements on how well your team shares information.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Our team gets appropriate information from industry sources to recognize risks, threats, and vulnerabilities to our system	○	○	○	○	○	○	○
Our team can take effective action using security information we receive from external sources, such as E-ISAC.	○	○	○	○	○	○	○
Our team shares security information that we have with our partners such as E-ISAC and the Reliability Coordinator	○	○	○	○	○	○	○
Our team shares security information effectively between teams and with incident response leaders in a standardized format.	○	○	○	○	○	○	○
Our team shares security information with the correct personnel that can make effective use of the information.	○	○	○	○	○	○	○

→

Please indicate how much you agree with the following statements on your confidence of your team's situational awareness.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Our organization is unable to assess and understand security issues as they happen allowing the situation to deteriorate.	○	○	○	○	○	○	○
Our organization has the ability to develop a strong shared comprehension of the situation that is free of conflicts.	○	○	○	○	○	○	○
Our team would struggle to forecast what could happen next during an incident.	○	○	○	○	○	○	○
Our team has the appropriate skills and training to respond to most incidents that could be identified.	○	○	○	○	○	○	○
Our team is able to effectively communicate and receive information from disparate sources and draw effective conclusions during an incident.	○	○	○	○	○	○	○

→

Please indicate how much you agree with the following statements on the adequacy of your incident response plan.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Our team's incident response plan is flexible and able to deal with a wide variety of cyber-attacks.	○	○	○	○	○	○	○
Our team understands how it would detect an intrusion in a timely manner using the tools available.	○	○	○	○	○	○	○
Our team is able to contain an intrusion to keep it from spreading using the tools available.	○	○	○	○	○	○	○
Our team has planned how to eliminate an intrusion or malware.	○	○	○	○	○	○	○
Our team knows how to adjust and adapt plans for both small and large scale cyber-attacks.	○	○	○	○	○	○	○
Our team's incident response plan considers the various stages of an attack from initial intrusion through the attack that could crash the power grid.	○	○	○	○	○	○	○

→

Please indicate how much you agree with the following statements on our organization's readiness for an incident.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Our response processes and procedures are able to respond to a detected cybersecurity incident in a timely manner.	○	○	○	○	○	○	○
Our incident response team has access to our support teams, NERC, and appropriate outside agencies allowing a coordinated response.	○	○	○	○	○	○	○
Our incident response team has the capability to analyze and understand an event.	○	○	○	○	○	○	○
Our incident response team learns from our exercises and incidents to improve our capabilities	○	○	○	○	○	○	○
Our cybersecurity team implements the appropriate cyber protections to ensure delivery of power to customers.	○	○	○	○	○	○	○
Our team can recognize that a cybersecurity event is occurring.	○	○	○	○	○	○	○
Our cybersecurity team can effectively respond to an event.	○	○	○	○	○	○	○
Our teams can quickly and effectively recover from a cybersecurity event.	○	○	○	○	○	○	○

→

What role do you play in Incident Response?

- Power Grid Manager
- Power Grid Operator
- Cyber Incident Response Manager
- Cyber Incident Responder
- Overall Management
- Other

What type of company do you work with? To ensure anonymity, do not identify the specific company.

- Investor owner utility
- Electric cooperative
- Municipal or other government electric power company

→

We thank you for your time spent taking this survey.
Your response has been recorded.

REFERENCES

Abell, C., Allen, R., Assante, M., Baumken, D., Barrett, D., Bowe, T., . . . Whitney, T. (2012). *Cyber Attack Task Force Final Report*. Retrieved from https://www.nerc.com/pa/CI/news/CIP/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Bd_Accpt_0521.pdf

Ahmad, S. R. (2003). Adverse drug event monitoring at the Food and Drug Administration: your report can make a difference. *Journal of general internal medicine, 18*(1), 57-60. Retrieved from https://doi.org/10.1046/j.1525-1497.2003.20130.x

Akoglu, H. (2018). User's guide to correlation coefficients. *Turkish journal of emergency medicine, 18*(3), 91-93. Retrieved from https://doi.org/10.1016/j.tjem.2018.08.001

Assante, M., Conway, T., Lee, R. M., & E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Assante, M., Conway, T., Lee, R. M., & E-ISAC. (2017). *ICS Defense Use Case No. 6: Modular ICS Malware*. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdfS

Assante, M., & Lee, R. M. (2015). *The Industrial Control System Cyber Kill Chain*. Retrieved from https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Astrachan, C. B., Patel, V. K., & Wanzenried, G. (2014). A comparative study of CB-SEM and PLS-SEM for theory development in family firm research. *Journal of Family Business Strategy, 5*(1), 116-128. Retrieved from https://doi.org/10.1016/j.jfbs.2013.12.002

Au, C. H., Fung, W. S., & Tses, A. (2016). *An investigation on the relationship between control self-assessment, cloud security, and cloud-related business performance-using partial least squares*. Paper presented at the 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). https://doi.org/10.1109/IEEM.2016.7798204

Bauer, S., & Bernroider, E. W. (2015). *The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring*. Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust. https://dx.doi.org/10.6028/NIST.SP.800-61r2

Bentler, P. M., & Weeks, D. G. (1980). Linear structural equations with latent variables. *Psychometrika, 45*(3), 289-308. doi:10.1007/BF02293905

Berthevas, J.-F. (2018). *Students' computers safety behaviors, under effects of cognition and socialization: when gender and job experience influence information security behaviors*. Paper presented at the 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), Marrakech, Morocco, Morocco Conference retrieved from https://doi.org/10.1109/ITMC.2018.8691175

Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. *Academy of Management Journal, 44*(6), 1281-1299. Retrieved from https://doi.org/10.5465/3069401

Blasch, E., Valin, P., Bosse, E., Nilsson, M., Van Laere, J., & Shahbazian, E. (2009). Implication of culture: user roles in information fusion for enhanced situational understanding. *Information Fusion, 2009. FUSION'09. 12th International Conference on*, 1272-1279. Retrieved from http://ieeexplore.ieee.org/document/5203715/

Bowe, T., Johnson, P. B., Bacik, S., Bernabeu, E., Brindley, S., Julie Couillard, . . . Young, B. C. (2012). *Severe Impact Resilience: Considerations and Recommendations*. Retrieved from http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf

Brumfield, C. (2019). Regional municipal ransomware attacks soar; MS-ISAC can help. *CSO Online*. Retrieved from https://www.csoonline.com/article/3433930/regional-municipal-ransomware-attacks-soar-ms-isac-can-help.html

Cameron, A. C. (2004). Sage encyclopedia of social science research methods. In M. S. Lewis-Beck, A. Bryman, & T. F. Liao (Eds.), *The SAGE Encyclopedia of Social Science Research Methods* (pp. 544-545): Sage Publications, Inc.

Cherepanov, A., & Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. Retrieved from https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *SP 800-61 Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cimpanu, C. (2019). Ransomware incident leaves some Johannesburg residents without electricity. *ZDNet*. Retrieved from https://www.zdnet.com/article/ransomware-incident-leaves-some-johannesburg-residents-without-electricity/

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences, Second Edition*. New York: Lawrence Erlbaum Associates.

Connors, E. S., Endsley, M. R., & Jones, L. (2007). Situation awareness in the power transmission and distribution industry. *Proceedings of the Human Factors and*

Ergonomics Society Annual Meeting, 51(4), 215-219. Retrieved from https://doi.org/10.1177%2F154193120705100415

Craigle, V. (2007). MedWatch: The FDA safety information and adverse event reporting program. *Journal of the Medical Library Association, 95*(2), 224. Retrieved from https://dx.doi.org/10.3163%2F1536-5050.95.2.224

Crichton, M. T., Lauche, K., & Flin, R. (2005). Incident command skills in the management of an oil industry drilling incident: A case study. *Journal of Contingencies and Crisis Management, 13*(3), 116-128. Retrieved from https://doi.org/10.1111/j.1468-5973.2005.00466.x

Crump, R. K., Hotz, V. J., Imbens, G. W., & Mitnik, O. A. (2009). Dealing with limited overlap in estimation of average treatment effects. *Biometrika, 96*(1), 187-199. Retrieved from https://doi.org/10.1093/biomet/asn055

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the human factors and ergonomics society annual meeting, 49*(3), 229-233. Retrieved from https://doi.org/10.1177%2F154193120504900304

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi:10.1016/j.cose.2009.09.002

Department of Energy. (2018). Cybersecurity Risk Information Sharing Program. Retrieved from https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf

Department of Homeland Security - CISA. (2016). ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved from https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

Department of Homeland Security - CISA. (2017a). Alert (TA17-163A): CrashOverride Malware. Retrieved from https://www.us-cert.gov/ncas/alerts/TA17-163A

Department of Homeland Security - CISA. (2017b). *HatMan—Safety System Targeted Malware (MAR-17-352-01 Update B).* Retrieved from https://www.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

Department of Homeland Security - CISA. (2018). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

Department of Homeland Security. (2008). *National Incident Management System*. Retrieved from https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

Diebold, S., Freese, J., Vangoor, A., Buckley, B., Zimmet, B., Retz, C., . . . Canada, B. (2013). Recommendations for improved Information Sharing. Retrieved from http://www.nerc.com/comm/CIPC/Electricity%20Sector%20Information%20Sharing%20Task%20For1/Electricity%20Sector%20Information%20Sharing%20Task%20Force%20(ESISTF)%20Draft%20Report.pdf

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. *MIS quarterly, 39*(2). Retrieved from https://misq.org/consistent-partial-least-squares-path-modeling.html

dos Santos Alves, D. F., da Silva, D., & de Brito Guirardello, E. (2017). Nursing practice environment, job outcomes and safety climate: a structural equation modelling analysis. *Journal of nursing management, 25*(1), 46-55. Retrieved from https://doi.org/10.1111/jonm.12427

Dragos. (2017). CrashOverride: Analysis of the threat to electric grid operations. Retrieved from https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Duffey, R. B., & Ha, T. (2012). The probability and timing of power system restoration. *IEEE Transactions on power Systems, 28*(1), 3-9. Retrieved from https://doi.org/10.1109/TPWRS.2012.2203832

E-ISAC. (2018). E-ISAC End of Year Report. Retrieved from https://www.wecc.org/Administrative/TLP%20Green%20E-ISAC%20End%20of%20Year%20Report.pdf

Electricity Information Sharing and Analysis Center. (2016a). The Electricity Information Sharing and Analysis Center offers security services to owner and operator organizations of the Bulk Power System across North America. Retrieved from https://www.esisac.com/

Electricity Information Sharing and Analysis Center. (2016b). Understanding Your E-ISAC. Retrieved from http://www.nerc.com/pa/CI/ESISAC/Documents/Understanding%20Your%20E-ISAC_June%2028%202016_FINAL.PDF

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*(1), 32-64. Retrieved from https://doi.org/10.1518%2F001872095779049543

Endsley, M. R. (2012). Situation Awareness in the Bulk Power System. *NERC Human Performance Conference*. Retrieved from

http://www.nerc.com/pa/rrm/hp/2012%20Human%20Performance%20Conference/SA%20Technologies%20NERC%20human%20perf%20conf.pdf

Farooq, M. S., Salam, M., Fayolle, A., Jaafar, N., & Ayupp, K. (2018). Impact of service quality on customer satisfaction in Malaysia airlines: A PLS-SEM approach. *Journal of Air Transport Management, 67*, 169-180. Retrieved from https://doi.org/10.1016/j.jairtraman.2017.12.008

Federal Energy Regulatory Commission. (2013). *Version 5 Critical Infrastructure Protection Reliability Standards* Washington, D.C.: U.S. Government Publishing Office Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2013-12-03/pdf/2013-28628.pdf

Federal Energy Regulatory Commission. (2016). *Revised Critical Infrastructure Protection Reliability Standards* Washington, D.C.: U.S. Government Publishing Office Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2016-01-26/pdf/2016-01505.pdf

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110. doi:10.1016/j.cose.2014.03.004

Glick, R. (2019). *Docket NP19-4-000: Glick, Commissioner, concurring*. Washington, DC Retrieved from https://ferc.gov/media/statements-speeches/glick/2019/08-29-19-glick.pdf

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales.* Paper presented at the Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

Greenberg, A. (2019). New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. *Wired*. Retrieved from https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

Hair, J., Hult, G., Ringle, C., Sarstedt, M., & Thiele, K. (2017). Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. *Journal of the academy of marketing science, 45*(5), 616-632. doi:10.1007/s11747-017-0517-x

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Australia, Australia/Oceania: SAGE.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152. Retrieved from https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2-24. Retrieved from https://doi.org/10.1108/EBR-11-2018-0203

Hald, K. S. (2018). Social influence and safe behavior in manufacturing. *Safety science, 109*, 1-11. doi:10.1016/j.ssci.2018.05.008

Han, L., Ball, R., Pamer, C. A., Altman, R. B., & Proestel, S. (2017). Development of an automated assessment tool for MedWatch reports in the FDA adverse event reporting system. *Journal of the American Medical Informatics Association, 24*(5), 913-920. Retrieved from https://doi.org/10.1093/jamia/ocx022

Harrald, J., & Jefferson, T. (2007). Shared situational awareness in emergency management mitigation and response. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 23-23. Retrieved from https://doi.org/10.1109/HICSS.2007.481

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial management & data systems, 116*(1), 2-20. doi:/10.1108/IMDS-09-2015-0382

Hooey, B. (2018). "NASA Aviation Safety Reporting System (ASRS). Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190002751.pdf

Hu, L. t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal, 6*(1), 1-55. Retrieved from https://doi.org/10.1080/10705519909540118

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic management journal, 20*(2), 195-204. Retrieved from https://doi.org/10.1002/(SICI)1097-0266(199902)20:2%3C195::AID-SMJ13%3E3.0.CO;2-7

International Organization for Standardization [ISO]. (2016). Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (ISO/IEC 27035-1:2016). Retrieved from https://www.iso.org/standard/60803.html

Jöreskog, K. G. (1971). Simultaneous factor analysis in several populations. *Psychometrika, 36*(4), 409-426. Retrieved from https://doi.org/10.1007/BF02291366

Kaber, D. B., & Endsley, M. R. (1998). Team situation awareness for process control safety and performance. *Process Safety Progress, 17*(1), 43-48. Retrieved from https://doi.org/10.1002/prs.680170110

Kaynak, R., Toklu, A. T., Elci, M., & Toklu, I. T. (2016). Effects of occupational health and safety practices on organizational commitment, work alienation, and job performance: Using the PLS-SEM approach. *International Journal of Business and Management, 11*(5), 146-166. Retrieved from http://dx.doi.org/10.5539/ijbm.v11n5p146

Knake, R. K. (2017). A cyberattack on the US power grid. Retrieved from https://www.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf

Koppel, T. (2015). *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*: Crown Publishers.

Kral, P. (2011). The incident handlers handbook. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.642.8488

Lawrie, M., Parker, D., & Hudson, P. (2006). Investigating employee perceptions of a framework of safety culture maturity. *Safety science, 44*(3), 259-276. Retrieved from https://www.sciencedirect.com/science/article/pii/S0925753505001190

Lee, R. M., Assante, M. J., & Conway, T. (2014). *German steel mill cyber attack*. Retrieved from https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Line, M. B., Zand, A., Stringhini, G., & Kemmerer, R. (2014). Targeted attacks against industrial control systems: Is the power industry prepared? *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, 13-22. Retrieved from https://doi.org/10.1145/2667190.2667192

Lockheed Martin. (2015). *GAINING THE ADVANTAGE: Applying Cyber Kill Chain® Methodology to Network Defense*. Retrieved from http://www.lockheedmartin.com//content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE transactions on professional communication, 57*(2), 123-146. Retrieved from https://doi.org/10.1109/TPC.2014.2312452

Maj, M., Reijers, R., & Stikvoort, D. (2010). Good Practice Guide for Incident Management. Retrieved from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Manos, P. A. (2017). Utility Companies Among Those Impacted by Ransomware Attack. *T&D World*. Retrieved from https://www.tdworld.com/grid-security/utility-companies-among-those-impacted-ransomware-attack

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). Cyber threat metrics. *Sandia National Laboratories*. Retrieved from https://fas.org/irp/eprint/metrics.pdf

NASA. (2011). Advisory Circular 00-46E. Retrieved from https://asrs.arc.nasa.gov/docs/AC%2000-46E.pdf

National Council of ISACs. (2016). National Council of ISACs. Retrieved from http://www.nationalisacs.org/

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments*. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018

NERC. (2012). *2011 NERC Grid Security Exercise: After Action Report*. Retrieved from http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC_GridEx_AAR_16Mar2012_Final.pdf

NERC. (2014). *Grid Security Exercise (GridEx II): After-Action Report*. Retrieved from http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20Public%20Report.pdf

NERC. (2016a). About Alerts. Retrieved from http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx

NERC. (2016b, 6/8/2016). Alerts. Retrieved from http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx

NERC. (2016c). Critical Infrastructure Protection Committee (CIPC), March 8-9, 2016. Retrieved from http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC%20Combined%20Presentations%20March%202016.pdf

NERC. (2016d). *Grid Security Exercise: GridEx III Report*. Retrieved from http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf

NERC. (2016e). NERC Operating Manual: August 2016. Retrieved from https://www.nerc.com/comm/OC/Operating%20Manual%20DL/Operating_Manual_20160809.pdf

NERC. (2016f). *State of Reliability 2016*. Retrieved from http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2016_SOR_Report_Final_v1.pdf

NERC. (2017). Filings & Orders > Canada. Retrieved from http://www.nerc.com/FilingsOrders/ca/Pages/default.aspx

NERC. (2018a). *Grid Security Exercise GridEx IV: Lessons Learned*. Retrieved from Atlanta, GA: https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf

NERC. (2018b). NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP18-_-000. Retrieved from http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf

NERC. (2019a). *Glossary of Terms Used in NERC Reliability Standards Updated August 12, 2019*. Retrieved from http://www.nerc.com/files/glossary_of_terms.pdf

NERC. (2019b). NCR Active Entities List 10/11/2019. In NERC_Compliance_Registry_Matrix_Excel20160422.xls (Ed.).

NERC. (2019c). *Reliability Standards for the Bulk Electric Systems of North America: June 5, 2019*. Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

NERC. (2019d). *State of Reliability 2019*. Retrieved from https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf

Nicol, D. M. (2011). Hacking the lights out. *Scientific American, 305*(1), 70-75. Retrieved from https://www.jstor.org/stable/26002714

Noort, M. C., Reader, T. W., Shorrock, S., & Kirwan, B. (2016). The relationship between national culture and safety culture: Implications for international safety culture assessments. *Journal of occupational and organizational psychology, 89*(3), 515-538. Retrieved from https://doi.org/10.1111/joop.12139

North American Electric Reliability Corporation, & Department of Energy. (2010). High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. Retrieved from https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf

O'Leary, M., & Chappell, S. L. (1996). Confidential incident reporting systems create vital awareness of safety problems. *ICAO journal, 51*(8), 11. Retrieved from https://www.researchgate.net/profile/Sheryl_Chappell/publication/11804282_Confidential_incident_reporting_systems_create_vital_awareness_of_safety_problems/links/5bc27acba6fdcc2c91fb786c/Confidential-incident-reporting-systems-create-vital-awareness-of-safety-problems.pdf

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332-344. doi:10.1016/j.ijresmar.2009.08.001

Ringle, C. M., & Sarstedt, M. (2016). Gain More Insight from Your PLS-SEM Results: The Importance-Performance Map Analysis. *Industrial management & data systems, 116*(9), 1865-1886. Retrieved from http://doi.org/10.1108/IMDS-10-2015-0449

Sarstedt, M., Hair, J. F., Ringle, C. M., Thiele, K. O., & Gudergan, S. P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research, 69*(10), 3998-4010. Retrieved from https://doi.org/10.1016/j.jbusres.2016.06.007

Shanmugapriya, S., & Subramanian, K. (2016). Developing a PLS path model to investigate the factors influencing safety performance improvement in construction organizations. *KSCE Journal of Civil Engineering, 20*(4), 1138-1150. Retrieved from https://doi.org/10.1007/s12205-015-0442-9

Shirali, G. A., Shekari, M., & Angali, K. (2016). Quantitative assessment of resilience safety culture using principal components analysis and numerical taxonomy: A case study in a petrochemical plant. *Journal of Loss Prevention in the Process Industries, 40*, 277-284. Retrieved from https://doi.org/10.1016/j.jlp.2016.01.007

SmartPLS. (2019). PLS Algorithm. Retrieved from https://www.smartpls.com/documentation/algorithms-and-techniques/pls

Smith, R. (2018). Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110

Smith, R. (2019). PG&E Among Utilities Cited for Failing to Protect Against Cyber and Physical Attacks. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/pg-e-among-utilities-cited-for-failing-to-protect-against-cyber-and-physical-attacks-11554821337

Sobczak, B. (2018). Grid leaders clear the air around Russian hacking. *E&E News*. Retrieved from https://www.eenews.net/stories/1060091819

Sonnenwald, D. H., & Pierce, L. G. (2000). Information behavior in dynamic group work contexts: interwoven situational awareness, dense social networks and contested collaboration in command and control. *Information Processing & Management, 36*(3), 461-479. Retrieved from https://doi.org/10.1016/S0306-4573(99)00039-4

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Subramaniam, C., Hassana, Z., Mohd. Zin, M. L., Sri Ramalu, S., & Shamsudin, F. M. (2016). The Influence of Safety Management Practices On Safety Behavior: A Study Among Manufacturing SMES In Malaysia. Retrieved from https://pdfs.semanticscholar.org/b95c/ef3f64cd56737180ee21b80ddf08e27b8139.pdf

Sun, W., Liu, C.-C., & Liu, S. (2011). *Black start capability assessment in power system restoration*. Paper presented at the 2011 IEEE Power and Energy Society General Meeting. http://dx.doi.org/10.1109%2FPES.2011.6039752

Symantec. (2017). Dragonfly: Western energy sector targeted by sophisticated attack group. Retrieved from https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security, 45*, 42-57. Retrieved from https://doi.org/10.1016/j.cose.2014.05.003

Tweed, K. (2014). Attack on nine substations could take down US grid. *IEEE spectrum*. Retrieved from https://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid

US-Canada Power System Outage Task Force. (2004). *Final report on the August 14, 2003 blackout in the United states and Canada: causes and recommendations*. Retrieved from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

Vaske, J. J., Beaman, J., & Sponarski, C. C. (2017). Rethinking Internal Consistency in Cronbach's Alpha. *Leisure Sciences, 39*(2), 163-173. doi:10.1080/01490400.2015.1127189

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism-in energy sector–a review. *Journal of Cyber Security Technology, 2*(3-4), 111-130. Retrieved from https://doi.org/10.1080/23742917.2018.1518057

Walton, R. (2018). North Carolina Utility Hobbled by Ransomware Attack in Wake of Florence. Retrieved from https://www.power-eng.com/2018/10/18/north-carolina-utility-hobbled-by-ransomware-attack-in-wake-of-florence/#gref

Wan, T. T., & Shasky, C. A. (2012). Mining medical claims data with exploratory to confirmatory statistical methods. *International Journal of Public Policy, 8*(1-3), 122-135. Retrieved from https://doi.org/10.1504/IJPP.2012.045877

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). *A situation awareness model for information security risk management* (0167-4048). Retrieved from https://doi.org/10.1016/j.cose.2014.04.005

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (csirts)*. Retrieved from https://www.sei.cmu.edu/reports/03hb002.pdf

Wittenbaum, G. M., Hollingshead, A. B., & Botero, I. C. (2004). From cooperative to motivated information sharing in groups: Moving beyond the hidden profile paradigm. *Communication Monographs, 71*(3), 286-310. Retrieved from https://doi.org/10.1080/0363452042000299894

Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*(1), 1-32. Retrieved from http://marketing-bulletin.massey.ac.nz/V24/MB_V24_T1_Wong.pdf

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Retrieved from http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zetter, K., & 3M Company. (2014). *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown.