



**AN EXPANDED CYBER INSURANCE FRAMEWORK TO MITIGATE CYBER  
INDUCED ECONOMIC LOSSES OF THE U.S. POWER INDUSTRY**

John P. Rosson, 1st Lt, USAF

AFIT-ENV-MS-17-M-219

**DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY**

**AIR FORCE INSTITUTE OF TECHNOLOGY**

**Wright-Patterson Air Force Base, Ohio**

**DISTRIBUTION STATEMENT A.**  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENY-MS-17-M-219

**AN EXPANDED CYBER INSURANCE FRAMEWORK TO MITIGATE CYBER  
INDUCED ECONOMIC LOSSES OF THE U.S. POWER INDUSTRY**

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cost Analysis

John P. Rosson

1st Lt, USAF

March 2017

**DISTRIBUTION STATEMENT A.**  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT-ENY-MS-17-M-219

**AN EXPANDED CYBER INSURANCE FRAMEWORK TO MITIGATE CYBER  
INDUCED ECONOMIC LOSSES OF THE U.S. POWER INDUSTRY**

John P. Rosson

1st Lt, USAF

Committee Membership:

Dr. Mason Rice  
Chair

Dr. Juan Lopez Jr., CISSP  
Member

Dr. R. David Fass  
Member

### **Abstract**

Cyber incidents are increasing in the United States and critical infrastructure is no exception. Aging operational technology is reliable, but much of it was not conceived in this century and lacks the security measures required to deal with worldwide interconnectivity. In order to bring security to the forefront of the critical infrastructure operator's priorities, there must be incentive. Insurance may provide the answer, as transferring risk is an attractive option which can be used to incentivize risk reduction, making it more attractive to both the insured and insurer. The incentives built into insurance contracts today, whether negative or positive reinforcement, have a profound effect on our behavior. This research explores the foundations of insurance theory and adopts behavioral manipulation methods used by mature insurance industries into cyber insurance. This cyber security framework builds on established research to incentivize security investment via insurance contracts by including coinsurance and deductible options. The model is validated by applying power industry performance data from 2013 through 2015. The results show how the addition of coinsurance and deductibles can serve as risk reduction incentives that create trade space in constrained budgets and ultimately make the power industry more secure from a cyber perspective if adopted.

## **Acknowledgments**

I would like to extend my undying gratitude to my wife for her constant support throughout our relationship. You are the best teammate I could imagine, even when I don't know it. Thank you.

To my children—even though you don't know it yet, your hugs, kisses, and tickling are a constant source of motivation. We are so excited to watch you grow.

I would also like to thank my thesis committee for providing support I needed, but also for letting me learn. This experience has contributed greatly to my growth as a person and a scholar, and hopefully it will contribute a little to the world as well.

John P. Rosson

## Table of Contents

|                                                         | Page |
|---------------------------------------------------------|------|
| Abstract.....                                           | iv   |
| Acknowledgments.....                                    | v    |
| Table of Contents.....                                  | vi   |
| List of Figures.....                                    | viii |
| List of Tables.....                                     | x    |
| I. Introduction.....                                    | 1    |
| Problem Statement.....                                  | 4    |
| Research Questions.....                                 | 5    |
| Methodology.....                                        | 6    |
| Assumptions/Limitations.....                            | 7    |
| Implications.....                                       | 8    |
| Preview.....                                            | 8    |
| II. Literature Review.....                              | 9    |
| Chapter Overview.....                                   | 9    |
| Insurance Theory.....                                   | 9    |
| Application of Theory: Incentivizing Good Behavior..... | 16   |
| State of the Industry.....                              | 21   |
| Summary.....                                            | 27   |
| III. Methodology.....                                   | 28   |
| Chapter Overview.....                                   | 28   |
| Operationalizing the Cyber Insurance Framework.....     | 29   |
| Baseline Conditions.....                                | 33   |
| Optimization.....                                       | 37   |

|                                                      |                                     |
|------------------------------------------------------|-------------------------------------|
| Data Diagnostics.....                                | 39                                  |
| IV. Analysis and Results.....                        | 43                                  |
| Chapter Overview.....                                | 43                                  |
| Pre-Treatment.....                                   | 43                                  |
| Major Disruptive Event (MED).....                    | 44                                  |
| Extended Insurance Model Policy Options .....        | 49                                  |
| Assessing the Extended Insurance Model .....         | 51                                  |
| Significant Factors in Extended Insurance Model..... | 54                                  |
| Post Treatment Industry Analysis .....               | 63                                  |
| Summary.....                                         | 75                                  |
| V. Conclusions and Recommendations .....             | 76                                  |
| Chapter Overview.....                                | 76                                  |
| Conclusions of Research .....                        | 76                                  |
| Limitations.....                                     | 78                                  |
| Hypotheses .....                                     | 79                                  |
| Recommendations for Future Research.....             | 80                                  |
| Summary.....                                         | 81                                  |
| Appendix.....                                        | <b>Error! Bookmark not defined.</b> |
| Bibliography .....                                   | 83                                  |
| Vita .....                                           | 94                                  |

## List of Figures

|                                                                                                                                           | Page |
|-------------------------------------------------------------------------------------------------------------------------------------------|------|
| Figure 1. Cyber incidents reported to US-CERT by federal agencies.....                                                                    | 2    |
| Figure 2. Reported cyber incidents at infrastructure control systems.....                                                                 | 2    |
| Figure 3. NERC Regions North America [91].....                                                                                            | 40   |
| Figure 4. Summary statistics for revenue, 2013-2015 (n = 240). ....                                                                       | 44   |
| Figure 5. Pre-treatment loss severity as a percentage of revenue. ....                                                                    | 46   |
| Figure 6. Commercial population comparisons between NERC regions. ....                                                                    | 47   |
| Figure 7. Residential population comparisons between NERC regions. ....                                                                   | 47   |
| Figure 8. SAIFI comparisons between NERC regions. ....                                                                                    | 48   |
| Figure 9. SAIDI comparisons between NERC regions. ....                                                                                    | 48   |
| Figure 10. Recommended insurance policy structure and security investment.....                                                            | 52   |
| Figure 11. Average pre-treatment losses and recommended direct self-security<br>investment. ....                                          | 53   |
| Figure 12. Average post-treatment loss and probability of a successful attack for each<br>insurance policy option. ....                   | 54   |
| Figure 13. Revenue comparison between recommended insurance policy options. ....                                                          | 56   |
| Figure 14. ANOVA analysis of pre-treatment severity by insurance policy options. ....                                                     | 57   |
| Figure 15. Residual plot and Tukey-Kramer HSD comparison test of pre-treatment loss<br>severity by insurance policy options. ....         | 58   |
| Figure 16. Non-parametric analysis of recommended direct security investment as a<br>percentage of revenue by insurance policy type. .... | 59   |
| Figure 17. ANOVA analysis of post-treatment losses as a percentage of revenue. ....                                                       | 60   |

|                                                                                                                                                           |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 18. Tukey-Kramer HSD comparison of post-treatment expected loss as a percentage of revenue by insurance policy type. ....                          | 61 |
| Figure 19. ANOVA and Tukey-Kramer HSD test of pre (left) and post treatment (right) losses by region. ....                                                | 64 |
| Figure 20. Standard deviation of loss pre and post treatment. ....                                                                                        | 64 |
| Figure 21. Variance comparisons, pre-treatment loss (left) and post-treatment loss (right) .....                                                          | 65 |
| Figure 22. Log transformed residuals of standard deviation of losses. ....                                                                                | 66 |
| Figure 23. ANOVA analysis of log transformed standard deviation in pre and post treatment categories. ....                                                | 67 |
| Figure 24. Residual plot and variance tests of standard deviation in pre and post treatment categories. ....                                              | 68 |
| Figure 25. Normality tests of standard deviation residuals. From left to right: 2013, 2014, and 2015. ....                                                | 69 |
| Figure 26. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2013. .... | 70 |
| Figure 27. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2014. .... | 71 |
| Figure 28. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2015. .... | 72 |
| Figure 29. Recommended security budget as a percentage of revenue. ....                                                                                   | 74 |
| Figure 30. Security spending as a percentage of revenue, post-treatment. ....                                                                             | 75 |

## List of Tables

|                                                                                            | Page |
|--------------------------------------------------------------------------------------------|------|
| Table 1. Critical infrastructure sectors and examples.....                                 | 3    |
| Table 2. Hypotheses.....                                                                   | 6    |
| Table 3. Summary of insurance industry surveys.....                                        | 22   |
| Table 4. Threat likelihood and reduction of threat likelihood variables.....               | 30   |
| Table 5. Insurance premium discount model.....                                             | 32   |
| Table 6. Calculated security investment effectiveness. ....                                | 36   |
| Table 7. Optimization constraints.....                                                     | 38   |
| Table 8 - Analytic Solver settings.....                                                    | 38   |
| Table 9. Data parsing process. ....                                                        | 41   |
| Table 10. Types of cost sharing options included in extended insurance model.....          | 50   |
| Table 11. Insured and insurer responsibilities given different cost sharing structures.... | 50   |

# **AN EXPANDED CYBER INSURANCE FRAMEWORK TO MITIGATE CYBER INDUCED ECONOMIC LOSSES OF THE U.S. POWER INDUSTRY**

## **I. Introduction**

Critical infrastructure systems are resources that provide essential services to our citizens. Power generation and distribution facilities, water treatment and wastewater treatment facilities, and the defense industrial base are examples. As managers of critical infrastructure companies continually assess and manage their company's risks, their primary concern is ensuring the availability and reliability of their systems, with security and risk reduction considered secondary objectives [1]. The conflict between availability and security is understandable, as security often complicates operations at critical infrastructure. However, as more systems are retrofitted for remote management, or connected to company networks, they are exposed to threats in ways that were never considered when they were built and implemented and therefore, vulnerable to cyber threats [2].

Any Internet connected system is a potential target for cyber attack, whether intentional or not. Iran's nuclear program was disrupted when 1,000 uranium enrichment centrifuges were destroyed via cyber attack. Despite the success of the attack, the operation nearly had disastrous unintended consequences when cyber security experts across the globe detected the same type of malware on untargeted systems. [3]. The Davis-Besse nuclear power plant in Ohio was inadvertently infected by malware from a consultant's laptop which prevented safety monitoring systems from broadcasting statuses and alerts for nearly five hours [4]. Figure 1 illustrates the increasing trend in

cyber incidents reported by federal agencies to the Department of Homeland Security U.S. Computer Emergency Readiness Team (US-CERT) [5], [6]. Federal Information Security Management Act (FISMA) reporting indicates that non-federal entities reported seven times as many cyber incidents to US-CERT in 2014 [5].

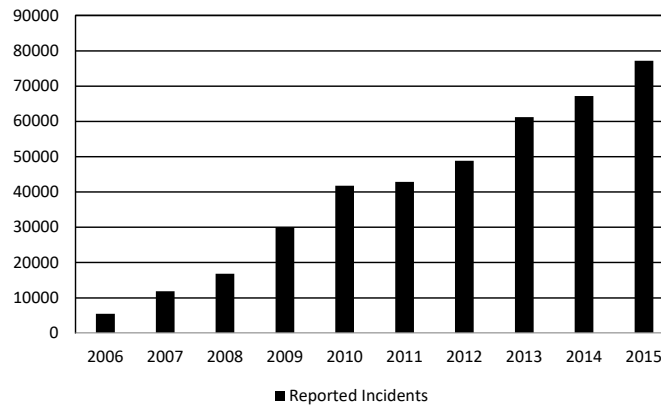


**Figure 1. Cyber incidents reported to US-CERT by federal agencies.**

Critical infrastructures, as outlined in Figure 2, are also experiencing an increasing trend in cyber incidents, as reported by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and depicted in Figure 2 [7].

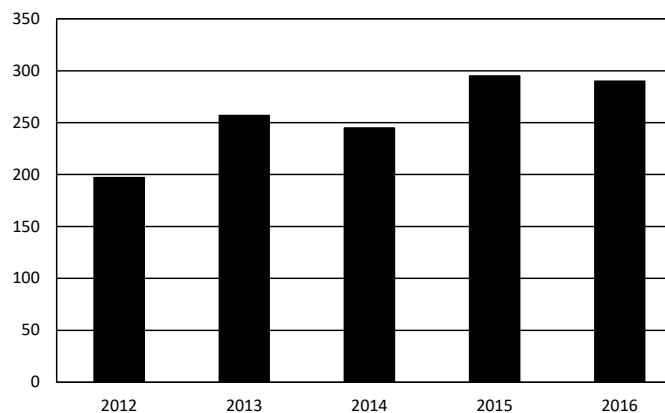


**Figure 2. Reported cyber incidents at infrastructure control systems.**

**Table 1. Critical infrastructure sectors and examples.**

| <b>Sector</b>                          | <b>Examples (not all inclusive of systems within a sector)</b>                             |
|----------------------------------------|--------------------------------------------------------------------------------------------|
| Chemical                               | Basic, Specialty, Agricultural, Pharmaceutical, and Consumer Product Chemicals             |
| Commercial Facilities                  | Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Sports Leagues  |
| Communications                         | Voice, Terrestrial, Satellite, and Wireless Transmission Systems                           |
| Critical Manufacturing                 | Primary Metals, Machinery, Electric Equipment, and Transportation Equipment Manufacturing  |
| Dams                                   | Water Retention and Control                                                                |
| Defense Industrial Base                | Department of Defense Contractor and Subcontractors                                        |
| Emergency Services                     | Law Enforcement, Fire and Emergency Services, Emergency Management, Public Works           |
| Energy                                 | Fuel, Electricity, and Natural Gas Facilities                                              |
| Financial Services                     | Depository Institutions, Insurance Companies                                               |
| Food and Agriculture                   | Farms, Restaurants, Food Manufacturing, Processing, and Storage Facilities                 |
| Government Facilities                  | General Use Office Buildings, Special Use Military Facilities                              |
| Healthcare and Public Health           | Hospitals                                                                                  |
| Information Technology                 | Production of Internet and Networking Hardware and Software                                |
| Nuclear Reactors, Materials, and Waste | Nuclear Power Plants, Nuclear Reactor and Component Manufacturers, Nuclear Fuel Facilities |
| Transportation Systems                 | Aviation, Mass Transit, Pipeline Systems Freight, Postal and Shipping                      |
| Water and Wastewater Systems           | Wastewater and Drinking Water Facilities                                                   |

To date, there have been relatively few verified examples of physical effects inflicted via cyber methods, but the physical impact of those events cannot be ignored. In 2007, the Idaho National Laboratory performed a demonstration that physically damaged a power generator by exploiting known software vulnerabilities [8]. A German steel mill owned by Thyssenkrupp AG was subjected to “massive damage” inflicted through tampering with the controllers of a blast furnace [7–12]. Ukraine has been subject to multiple cyber induced outages in recent years. In 2014 a suspected BlackEnergy malware attack that caused blackouts for approximately 225,000 customers across Ukraine and in 2016, a power distribution facility in Kiev lost the equivalent of a fifth of the city’s power consumption [3], [10], [15]–[17]. Incidents such as these continue to

surface, though more quietly than data breaches and identity theft, but security experts and company managers have taken notice.

### **Problem Statement**

This research is directed at solving the problem of under investment in cyber security in United States critical infrastructure, specifically, power companies. To do this, one of the four primary risk management methods, risk transfer via insurance, will be used to incentivize cyber security investment as way to mitigate risk. In order to do this, the conditions of the cyber insurance market must be addressed as well.

In light of the relative scarcity and lack of significant publicity of physical attacks executed through the cyber domain, many of the direct consequences and legal ramifications of successful cyber incidents remain relatively unknown [18]. The majority of the \$2 billion cyber insurance market today is designed for information technology (IT) risk—reputation control, lawyers, credit monitoring, and investigation expenses [19], [20]. Cyber insurance for IT does not meet the requirements of industrial control systems (ICS)—bodily injury, property damage, loss productivity in the economy, or even pollution [20]. Major power companies in the United States have already warned that their existing insurance coverage may not cover all aspects related to a cyber attack [17]. In other cases, when insurance policies do meet the requirements of critical infrastructure, the potential insured is turned away because their existing cyber defenses are deemed insufficient after the insurance company performs a cyber security assessment [21], [22]. To achieve the goal of increasing cyber security investment at power companies, this research will simultaneously address how to bridge the gap between power companies,

and insurance companies, to encourage more participation by both parties in the insurance industry.

### **Research Questions**

The questions posed in this research will address both how to incentivize investment and increase participation in the cyber insurance market suitable for ICS. In order for this research to be successful, the following questions must be answered:

- 1) What factors within an insurance policy incentivize the reduction of risk?
- 2) What factors affect the structure of the insurance policy?
- 3) Is there an optimal structure of insurance contract that electrical power companies will utilize to manage their risk more effectively?
- 4) How can insurance design incentivize insurers to offer the right types of insurance, and the insured to purchase insurance?
- 5) What effects will the proposed insurance framework have on the industry?

Initially, this research was exploratory in nature, executed by extending the Young et al. model and testing it using one third of the data used in the final research. The pilot testing process resulted in the formulation of the hypotheses designed to test the efficacy of the model and its impact on the entire power industry. The hypotheses are detailed in Table 2.

**Table 2. Hypotheses**

| Hypotheses:    |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| H <sub>1</sub> | Model insurance policy options                                                  |
| H <sub>0</sub> | No difference in policy options recommendations of z, C, or D                   |
| H <sub>a</sub> | Policy options are not equal                                                    |
| H <sub>2</sub> | Pre-treatment risk reduction                                                    |
| H <sub>0</sub> | No difference in risk profiles across NERC regions in pre-treatment conditions  |
| H <sub>a</sub> | Risk profiles in NERC regions are not equal in pre-treatment conditions         |
| H <sub>3</sub> | Post-treatment risk reduction                                                   |
| H <sub>0</sub> | No difference in risk profiles across NERC regions in post-treatment conditions |
| H <sub>a</sub> | Risk profiles in NERC regions are not equal in post-treatment conditions        |

## **Methodology**

This research will focus on extending the framework proposed by Young et al. that incentivized risk reduction through security investment using insurance premium discounts. Initial research will consist of an analysis of mature insurance industries to determine what behavior changing factors exist already and whether they can be incorporated into a cyber insurance framework. Once additional economic elements have been identified and incorporated into the Young et al. framework, the focus will turn to applying data collected from the U.S. Department of Energy (DOE) and the U.S. Energy Information Administration (EIA) to the model. The use of performance data reported by power companies will serve two purposes: (i) as a validation tool for the extended model by indicating whether or not the model effectively discriminates between power companies based on reported performance criteria and (ii) as a possible indicator of what can be done to more effectively manage risk across the power industry. Using the results

generated by the new model, implications for the power industry and avenues for future research will be generated.

### **Assumptions/Limitations**

In order to move forward with this research, three assumptions were made: (i) companies within the U.S. electric power industry will choose risk transfer as a method of managing risk if financially advantageous; (ii) the performance data used for application to the model may include cyber induced incidents, but is not limited to them. As reporting standards become more stringent moving forward, data may become available where cyber incident data is used exclusively, but for our purposes, power interruption events not resultant from cyber incidents will serve as proxies in this research; and (iii), the losses inflicted by a cyber event were estimated using the economic loss sustained by the customers within the power company's sphere of influence. While it may be unrealistic to expect that a power company would be responsible to provide compensation for the all economic losses sustained by an economy, we use this method for several reasons: given the proliferation of methods available to disrupt critical infrastructure systems, disregarding even the simplest of measures that could make a system considerably safer could be construed as an act of negligence, which could open the company up to lawsuits and consequently, extensive monetary reparations; second, the severity estimate has validity as a worst-case scenario for a cyber incident, which is the amount of coverage that ideally would be sought by the insured [23]. Using these assumptions the research can continue to move forward.

## **Implications**

A successful extension of Young et al.'s model will provide a path forward for U.S. power industry to increase its security posture through a variety of means. By incentivizing risk reduction through risk transfer, the mutual gains by the insured and insurer will generate more participation in the cyber insurance market (with a focus on meeting the needs of critical infrastructure). As more companies in the industry subscribe to risk transfer and reduction methods, the industry as whole will become more robust in rebuffing cascading incidents stemming from cyber incidents for the following reasons: (i) insurance policies will become more affordable to power companies as more information is collected by insurers; (ii) companies will become “more insurable” as they are incentivized to reduce risk by the structure of the insurance policies; (iii) as the number of companies utilizing risk transfer methods increases, the data available for cyber security analysis will increase and contribute to the evolution of cyber security best practices; and iv) the security posture of the overall industry will be enhanced as more companies continue to invest in effective security methods.

## **Preview**

The exploration of effective incentive measures via insurance policy structures will continue in following manner: Chapter 2 consists of a literature review where research relevant to the relationship between cyber security and cyber insurance will be identified; In Chapter 3, will describe the methodologies used to build the proposed model and apply real data to the framework; Chapter 4 will discuss the results generated by the framework and application of real data in Chapter 3, and perform an analysis of

the results; Finally, Chapter 5 will draw conclusions from the analysis, discuss implications for the industry, and provide recommendations for future research.

## **II. Literature Review**

### **Chapter Overview**

This chapter will present a literature review exploring insurance theory and relevant aspects for adoption into cyber security insurance. We will then examine the state of the cyber insurance industry and its implications to the critical infrastructure environment and operational technology. Finally, we will explore how current arms of insurance feature incentives using contract design and how this design may be applicable for incorporation into a cyber security strategy at power companies.

### **Insurance Theory**

#### **Risk Management**

Modern risk management principles have coalesced over the centuries into a relatively stable loop of identification, assessment, planning, and monitoring [24], [25]. Part of this process is determining the best method of handling risk—executed via transfer, avoidance, reduction, or acceptance of identified risks [24]. Of the four methods available, avoidance or acceptance of identified risks does nothing to further the security posture of the power industry, and for this reason, will be excluded from this research. Risk transfer and its application as an incentivize mechanism will be the focus of this research.

The Babylonians authored the first known insurance contract more than 6,000 years ago, documented on clay tablets in 4,000 BC [26]. Its structure and applications have evolved constantly through the millennia into the many arms available in the market today. However, linking the field of insurance theory to other fields of study did not begin in earnest until the middle 20th century, when economic and risk management theories were applied to insurance [27]. Since then, new lines of thought regarding insurance contract structure and how to effectively combat knowledge asymmetries in the market have bloomed. Using modern insurance theory, the framework presented in this research will provide companies with the ability to establish a stronger security posture utilizing risk transfer via market insurance designed to incentivize the reduction of risk through cyber security self-investment.

### **Insurance as a Regulator**

But why insurance? Shouldn't the federal government play a leading role in ensuring the viability of our national critical infrastructure? Given economic and bureaucratic challenges that face national governments every day, literature suggests that the answer is no. Typically, regulatory authorities lack incentives created through market pressure, the ability to respond to dynamic environments, or the resources to ensure that everybody behaves in a reasonable manner.

To start, Talesh argued that the insurance industry exerts a regulatory influence in the market by serving as a gatekeeper (an example would be automobile or mortgage insurance requirements) in some industries, or by providing payments for damages that would otherwise require the involvement of the civil court system (liability insurance pays damages to the injured in a car accident caused by another individual) [28]. The

gatekeeping function ensures a reasonably smooth operation of the marketplace by preventing high-risk individuals from engaging in activities in which they should not [28]. Codified liability insurance regulations serve as a tool that simplifies tort law into understandable action and consequences, with payments dependent on actions, which influence the insured [28] .

Kehne argued in 1986 that the imposition of conditional financial burdens and premium based incentives could significantly augment safety standards in the hazardous waste industry [29]. He also contended that the insurance companies have the capability to react quickly in a dynamic environment through market pricing, whereas regulatory authorities are hindered by bureaucracy and political considerations which contribute to faulty risk assessments [29]. Interestingly, Kehne concluded with the assertion that insurance based incentives would have positive effects in a variety of arenas, specifically where low-cost technologies can generate asymmetric damages within that particular sphere of influence. He cited genetic and chemical engineering as such arenas specifically due to their characteristics of rapid technological change outpacing the ability of regulatory abilities to maintain proper oversight [29]. Using Kehne's perspective, it could certainly be argued that the evolution of cyberspace and availability of asymmetric weapons in this sphere could benefit from regulation imposed by the insurance market.

While Kehne argued the financial responsibility of the insured could drive safety, Ben-Shahar and Logue argued from the perspective of the insurance companies themselves. Companies will act selfishly in order to contain costs once premiums are captured. They will use their resources to develop better information about the insured and offer incentives to reduce risk or mandate that the insured engage in self-protection

prior to initiating the contract [30]. In these cases, the insurers perform tasks tantamount to the regulation of public safety through rulemaking, claims investigation, and issuing verdicts on insurance claims—creating a set of rules and regulations by which the insured must operate or otherwise face financial consequences [30].

As the fiscal environment constrains the capabilities of all government bodies, capabilities available to an ever-widening population of potentially harmful actors continue to grow. As reviewed, the regulatory environment does not act as efficiently as the open market, nor does it possess the best tool with which to monitor the changes. However, the insurance market, with the capability to impose de facto regulations through insurance contracts—which if not abided by, will put the potential insured and public at risk, can use properly structured contracts to place responsibility on the insured and to monitor behavior more efficiently using resources that otherwise may not be available to the government. This in turn will create a safer environment using the private marketplace as a regulator.

### **Asymmetric Information**

In perfect markets, where all information is available to all parties, the optimal insurance contract can be obtained at will. In 1973, Rothschild and Stiglitz studied imperfect information in the insurance market and concluded that imperfect information had a significant impact on competitive insurance markets [31]. Continuing in this vein, the study of insurance markets with imperfect knowledge has led to a plethora of research on the topics of moral hazard and adverse selection. Adverse selection occurs when characteristics of the insured cannot be determined and the group of individuals seeking insurance are not the same, leading to the inability to discriminate between good actors

and bad actors [27]. The nature of the framework presented in this research, where security assessments are integral to the insurance policy structure, will inherently provide insurance companies with information that will allow them to discriminate between insurable and uninsurable power companies. For that reason, adverse selection is not considered further in this paper and we will focus on moral hazard as the sole form of asymmetric information.

The first empirical steps toward a modern definition of moral hazard in insurance can be traced back to 1865 when a correlation between insurance and the insured event was identified [32]. After a century of grappling with this state, Marshall defined moral hazard as “any misallocation of resources which results when risks are insured with normal insurance contracts and only with such contracts” [33, p. 880]. Winter built on the argument by asserting that the probability or size of the loss depends on the individual under contract and the driving force in any model of moral hazard is that the behavior of the insured is chosen after the contract is signed [34]. Consistent with the aforementioned descriptions, Loubergè identified two key elements for moral hazard to be present: the contract outcome can be influenced by the insured and the insurer cannot monitor the behavior of the insured without costs [27]. In the field of insurance, contrary to other disciplines, moral hazard has negative connotations and is something to be avoided [32]. As such, for the purposes of our research, moral hazard will be defined as engaging in behavior that willingly does nothing to reduce the probability of loss and in which the insured party would not otherwise engage in the absence of a risk transfer mechanism.

## **Insurance Economics and the Optimal Insurance Contract**

Initially, the application of economics to insurance began in 1963 when Karl Borch applied Kenneth Arrow's 1953 general equilibrium model to risk sharing among reinsurance markets [27]. However, Borch's work is only relevant to this application in that contributed to the beginning of growth in the field of what is now known as insurance economics. It was Arrow's work in the early 1960's that began to develop the insurance concepts that will be applied to cyber insurance in this research: First, while working for the RAND Corporation on resource allocation for research and development, he touched briefly on the relationship between market insurance and self-protection activities. He contended that the presence of insurance in the wrong form can weaken the incentive of the individual to protect against loss [35]. Second, while studying economics as applied to the medical field, he provided proofs for optimal insurance policies under different conditions. From the perspective of the individual, an insurance policy providing full coverage above some sort of deductible is the optimal policy. In cases where the insurance company is also risk averse, a deductible policy with additional cost sharing in the form of coinsurance is optimal. The final relevant point made for our application was his continued speculation on moral hazard. He contended that the relationship between the patient and doctor may serve as a natural check on moral hazard, which naturally led to the issuance of more insurance policies than in other fields because of the reduced risk of fraud [36]. Arrow's identification of policies associated with risk adverse individuals and insurers, and the relationship between them not only will play a role in the forthcoming proposed framework, but ignited a stream of research that will also be used in this research.

### **Self-Protection and Market Insurance**

In 1972, Ehrlich and Becker are credited with defining self-insurance and self-protection, and studying their relationship to market insurance [27]. In their research, they identified self-insurance as steps taken to reduce the size of a loss; self-protection was defined as a reduction in the probability of a loss [37]. Their studies are crucial to this paper's cyber insurance model in that they put forth the idea that self-protection can be encouraged by market insurance if the cost of the insurance is negatively related to the quantity of self-protection [37]. Schlesinger and Venezian take the idea of self-protection coupled with insurance a step further in suggesting that a profit-maximizing insurer may wish to invest its own money in loss prevention in a monopolistic market [38]. Similarly, Kleindorfer and Kunreuther use empirical evidence to show that lowering deductibles in exchange for consumer implementation of risk mitigation measures in risk-prone areas result in advantages for both the insured and insurer [39]. As research has evolved from the structure of insurance policies to taking an active role in pricing policies reliant on self-investment, there is direct support for our model that indicates a combination of risk transfer and direct self-investment reap net benefits for both the insured and insurer.

### **Connecting Operational Technology and Moral Hazard**

The manners of “optimized” insurance policies referenced above make use of cost sharing between the insured and the insurer. As Winter posits, there can be moral hazard when dealing with loss reduction, or loss prevention, each of which give rise to a market response of insurance policies with coinsurance or a deductible [34]. The elements of moral hazard noted by Marshall, Winter, and Loubergè are clearly present in the operational technology cyber security landscape: resources spent on measures, when

faced with a growing threat, other than to reduce the probability of loss to a reasonable level, could qualify as a misallocation of resources; the insurer cannot monitor the insured without costs to itself; and the probability of loss lays with the company through its cyber security practices [27], [33], [34]. Adopting the policy designs suggested by Arrow, Ehrlich and Becker, and Winter provide the theory behind how to incentivize security investment that will reduce the probability of a loss event or the size of the loss in light of a successful event. Moving forward, application of this theory will be examined.

### **Application of Theory: Incentivizing Good Behavior**

It is in the best interests of both the insured and insurer to reduce both the probability of an event. As literature has shown, risk management coupled with insurance has led to growth in the field insurance economics—designing contracts to induce individuals to act in their own best interests. Behavior altering incentives are featured in insurance policies in a variety of ways as companies attempt to prevent or reduce insured losses. Each field offers something that can be adopted into cyber insurance policies that will incentivize power companies to invest in their own security.

#### **Automobile Industry**

When it comes to incentivizing behavior, the auto insurance industry is continuously evolving. Generally speaking, the typical American cannot watch television without seeing insurance commercials touting “safe-driving discounts” in some form or another. Companies across the world are attempting to incentivize better behavior through a variety of means. Premium discounts and altering deductibles are two

prevalent methods cited in literature. The development of Pay-as-You-Drive insurance premiums is a significant shift in the insurance market that may allow for reduced insurance costs as a trade-off for increased monitoring by the insurance company. An experiment in 2015 showed a 50% decrease in speeding behavior across all ages when Pay-as-You-Drive feedback was provided immediately and tied to the consumer's insurance premium [40]. In other cases, simple penalties, levied as increases in the premiums for bad driving have reduced claims incidents by 6.5% [41].

The topic of moral hazard is actively researched in car insurance. Wang, Chung, and Tzeng studied the car insurance market in Taiwan in 2008, looking for evidence of moral hazard to determine whether increasing deductibles for every claim reduced its presence. Their findings indicated that increases in deductibles limited moral hazards in the industry [42]. In 2013, Dionne, Michaud, and Dahchour found empirical evidence of moral hazard in drivers with less than 15 years of driving experience [43]. The presence of deductibles in the automobile insurance market indicate that companies have some idea of how to combat moral hazard, but the existence of recent literature seeking to prove its presence indicates that there is not yet a definitive answer on what to do about it [44].

Automobile insurance is relevant to cyber insurance in that the insurance companies are negatively relating performance on the road to dollars paid for risk transfer. Active efforts to incentivize the insured to drive more safely through increased monitoring can be equated to active efforts to prevent cyber incidents at power companies—increased investment by the power company is an active effort to perform better. Combating moral hazard by increasing the amount of deductible could have the

same effect—power companies faced with a higher percentage of the loss will be incentivized to take a more active stance in securing their systems.

### **Earthquake Insurance**

The state of California created the California Earthquake Authority (CEA) in 1996 to reinvigorate the housing insurance market in the aftermath of the California Northridge Earthquake in 1994 [45]. Recently, the CEA has been experimenting with incentivizing risk mitigation measures in a variety of ways. Over the past three years, residents in earthquake prone counties in California, are eligible to receive up to \$3,000 to offset the costs of retrofitting their homes [46]. Additionally, the CEA has significantly boosted premium discounts from 5% to 20% if an insured proves that they have retrofitted their housing [46]. Finally, the CEA has been offering flexible deductibles through The Choice program. This program allows the insured to pick the percentage of deductible in their policies for both structure and personal property (now separate coverages within the policy). Many consumers have taken advantage of these new insurance designs, moving away from the old design of a single, flat deductible [46]. Since 2012, earthquake insurance that the CEA has underwritten has grown by 4.5% [46].

The incentives associated with earthquake insurance policies offered by the CEA offer viable methods that could be adopted into cyber security practices. Reductions in premiums based on risk mitigation is a common incentive offering, however, the use of a flexible deductible and coverage through The Choice program, designed to increase availability and affordability also seem to be successful in the aim of increasing earthquake coverage in California [46]. The flexible deductible is a key feature adopted into the proposed framework.

## **Flood Insurance**

Flood insurance is a volatile insurance product that exhibits an increasing trend of policies in force over a 30 period, but decreasing trend since 2009 [47]. Incentives in the U.S. are extremely limited, exercised via community participation in flood risk rating programs offered through FEMA [48], [49]. However, experience seems to act as an incentive at the state level, where empirical data shows that flood insurance purchases are highly correlated with flood losses in that state from the prior year [50]. A study by Hudson, Botzen, Feyen, and Aerts examined the growing flood threat in France and Germany. They determined that the implementation of risk mitigation measures implemented at the owner's expense in exchange for premium discounts could reduce expected flood damage in France by 24% and in Germany by 12% [51].

With experience as the only incentive for an individual to buy flood insurance, written flood insurance policies are trending downwards in America [47]. The critical infrastructure of our nation cannot afford to wait experience to learn a painful lesson in cyber security. The empirical results in the proposed public-private insurance programs in France and Germany using risk mitigation methods to spur incentive premiums are included in the framework proposed by Young et al. and incorporated into the framework proposed in this research [51].

## **Value Based Insurance Design**

Value based insurance design (VBID) language was signed into law in March 2010, authorizing insurers to pursue insurance designs that incentivize consumers to use high value health services over low value services [52]. While health insurance is structured somewhat differently than property and liability insurance due to the presence of co-pays,

behavioral incentives remain prevalent. It was developed with the long term objective of emphasizing value in healthcare rather than embarking on strict cost reduction measures that lead to decreases in social welfare while ultimately increasing long term health costs [53]. Practically, the focus on value is executed by insurance companies reducing or eliminating co-pays on services that treat chronic disorders which could result in more harmful complications in the future if left untreated [53].

Ultimately, the design is relatively new, but empirical evidence has been published that supports the continuation of this type of insurance into the future: pediatric care using VBID indicated that well-child visits and the use of recommended vaccinations increased while emergency department and specialist visits decreased, resulting in no significant increase in overall cost of total healthcare [54]. In a study of 275,000 patients across 76 different plans, medication adherence under VBID increased, and better drug adherence led to an predicted cost savings over a five year period going forward [55], [56]. In the long term, VBID may actually generate cost savings by incentivizing smart healthcare selections by insured and ultimately creating a healthier population [57].

VBID incentives involve reducing costs on desirable behaviors. This form of positive reinforcement was initially used in the Young et al. model through premium discounts based on security investment and remains in the extended model.

Each of the mature insurance industries examined have institutionalized behavior-altering incentives in their insurance design. The automobile industry uses deductibles extensively and is developing more robust monitoring measures. The CEA in California not only subsidizes risk reduction, but rewards consumers for it through reduced

premiums. The nationalized flood insurance industry offers no incentives and the impacts can be seen in decreasing trends. The only true incentive in flood insurance is loss, which is reactionary and generally not recommended as a robust security strategy. VBID seeks to incrementally build a more stable healthcare environment through incentivizing desirable behaviors using copays. From insurance economics theory to application, literature has proven that the behavior of the insured can be altered through insurance policy elements, specifically cost sharing measures. Using a combination of theory and economic elements borrowed from other industries, Young et al.'s framework will be extended using the additional cost sharing elements of coinsurance and deductibles in order to incentivize insured companies to actively engage in risk reduction measures as a condition of the insurance contract.

### **State of the Industry**

Recent surveys conducted by the insurance industry, outlined in Table 2, indicate that cyber liability insurance is increasing. However, cyber insurance policies primarily target the information technology domain rather than the operational technology domain relied upon by critical infrastructure [17], [20], [58]–[61]. Of the four reports examined, only one considers physical property in addition to intellectual property—with less than one third of the companies surveyed indicating physical property damage was a concern [58].

**Table 3. Summary of insurance industry surveys.**

| Firm                 | Year | Report Name                                            | Percentage Using Cyber Insurance |
|----------------------|------|--------------------------------------------------------|----------------------------------|
| Zurich Financial     | 2011 | Information Security & Cyber Liability Risk Management | 35%                              |
| Chubb North America  | 2012 | Cyber Risk: Threat and Opportunity                     | 36%                              |
| Zurich Financial     | 2012 | Information Security & Cyber Liability Risk Management | 44%                              |
| Willis North America | 2013 | Willis Fortune 1000 Cyber Disclosure Report            | 6%*                              |
| Willis North America | 2013 | Willis Fortune 500 Cyber Disclosure Study              | 6%*                              |
| Zurich Financial     | 2013 | Information Security & Cyber Liability Risk Management | 52%                              |
| Zurich Financial     | 2014 | Information Security & Cyber Liability Risk Management | 52%                              |
| Zurich Financial     | 2015 | Information Security & Cyber Liability Risk Management | 61%                              |

The cyber insurance industry is estimated to grow from \$2 billion in premiums in 2015, to more than \$20 billion in premiums by 2025 [19], [20], [62]–[64]. But the reports indicate that while the adoption of cyber insurance policies appears to be trending upwards, there is little to no evidence to support the idea that cyber insurance policies are tailored or specifically customized to protect critical infrastructure. Furthermore, the existence of the Cyber Attack Exclusion Clause (CL380) excludes reimbursement for physical damage inflicted via cyber methods in property and general liability policies [10]. The existence of CL380 and current cyber insurance policy design are not adequate to protect critical infrastructure in general, and the power industry in particular.

Existing literature has provided the foundation required to develop a cyber insurance model that will aid our efforts to develop a framework for implementing cyber insurance into the operational technology environment, but a broad view of the state of the cyber insurance market must be evaluated in an effort to further understand why the power industry has not experienced a widespread adoption of cyber insurance products.

### **Threats and Vulnerabilities**

Extensive literature has been dedicated to the identification of vulnerabilities, threats and mitigation of risks facing OT systems in general. Hahn and Govindarasu

developed a network exposure metric to be used as a measure of effectiveness of security mechanisms employed on a network. The system identified the interdependencies between security measures, which allowed the tester to assess vulnerabilities on their network [65]. Nicholson, Webber, Dyer, Patel, and Janicke identified the need for to review threats facing the critical infrastructure community. Their work acknowledged the vast variety of operational technology systems used to control our national infrastructure and performed a sweeping analysis to include the classification of bad actors, a history of relevant attacks, risks, threats, flaws, exploits, and prevention methods that can be used to secure OT [66]. Knowles, Prince, Hutchison, Disso, and Jones focused on security management in industrial control systems. Their major contribution was to combine functional assurance and security metrics when implementing security OT systems, laying the groundwork for future research in the area of component security. The metrics they examined were: (i) system-wide assessments; (ii) the interdependency of networks across physical, cyber, geographical, and logical systems; (iv) real-time security monitoring; and (v) defining security controls more effectively [67].

Recent research has focused on the power grid specifically. Mohajerani, Farzan, Jafary, Lu, Wei, Kalenchits, Boyer, Muller, and Skare introduced a model for detecting and mitigating the vulnerabilities on the power grid. Their model suggested a hierarchy of processes designed to identify the most vulnerable asset in the system and then the most vulnerable sub-asset using a two pass risk assessment method [68]. Vellaithurai, Srivastava, Zonouz, and Berthier conducted research using stochastic Bayesian network models to develop the “CPIndex,” designed to assess the effectiveness of security measures in both the cyber and physical domains of a power company’s infrastructure

[69]. As threat assessment research continues to evolve and counter measures are developed, the foundation of a highly participatory cyber insurance market is being built. A deeper understanding of what types of cyber security investment will be most effective can guide the industry to create and communicate best practices continuously to enhance the industry's security posture.

### **Government Efforts**

The Department of Homeland Security has been working towards an information sharing solution designed to facilitate cyber defense strategies critical infrastructure companies [70]. However, this large-scale coordination effort designed to share private and potentially sensitive information with competitors within an industry has already taken several years and has resulted in no concrete solutions. The Cyber Incident Data Analysis Working Group (CIDAWG) at the Department of Homeland Security is working with critical infrastructure companies to develop a data-sharing arrangement that will provide value to insurance customers, however, not directly. Three white papers have been published to further the mission of developing said repository. In June 2015, "Value Proposition for a Cyber Incident Data Repository," outlined the benefits of a private/public relationship. This document outlined the six key benefits of a shared data repository: (i) the identification of top risks and effective controls, (ii) the development of benchmarks in the industry, (iii) return on investment in the program, (iv) allowing for differentiation of each sector, (v) preparedness for future incidents by the development of modes and trends, and (vi) advancing the culture of risk management in the industry [71]. In September 2015, the working group published, "Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository." This paper provided a

framework for the sharing of cyber incident data, creating 16 categories aligned with the “Value Proposition” white paper published the previous June [72]. The latest work by the CIDAWG was published in December 2015, outlined the perceived obstacles that a centralized data repository will face within and across industries. “Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository,” addressed anonymity, security, cultural challenges, commercial threats, process streamlining, uniform participation, and technical design challenges in an effort to acknowledge the issues and create a system for overcoming them [70]. These white papers began the process of justifying a framework for sharing information that will be useful to insurance consumers and policy makers; however, said framework can only provide value once it becomes common practice and companies can digest the data to develop products that fill the need for consumers. Ideally, participation in the insurance industry will create a de facto data sharing arrangement as insurance companies with a broad portfolio share institute their own standards that they will impose on the insured. The framework outlined by the DHS takes this idea a step further by creating a data sharing arrangement between the insurance companies, which will further increase the data pool.

### **Cyber Insurance Inhibitors**

Bandyopadhyay, Mookerjee, and Rao identified asymmetric knowledge and adoption rates as cyber insurance inhibitors. Their analysis asserted that the interdependence and cascading effects of a cyber attack could lead to unforeseeable secondary losses, which would contribute to higher premium and therefore inhibited adoption [73]. Around the same time, Bolot and Lelarge used simple models to illustrate that generally, self-investment in self-protection is generally not attractive to cyber based

companies, but insurance could be used as a mechanism designed to incentivize self-protection [74]. Marotta, Martinelli, and Yautsiukhin conducted a literature survey of the cyber insurance market. Interestingly, their main findings indicate that investment in self-protection is not attractive if insurance is available, but determined that a regulatory mechanism offering fines and rebates could encourage self-investment [75]. Biener, Eling, and Wirfs performed an empirical analysis of the insurability of cyber risk. They note that there are significant issues with the insurability of cyber risk, but concluded that increasing the size of the risk pool and consequently, the data pool, the information technology sector is ultimately insurable [76]. In many cases, the literature reviewed seems paradoxical—cyber insurance is not feasible due to the risk created by the dearth of information available to the market. However, more participation will lead to more information. Furthermore, if structured correctly, cyber security literature has theorized that risk transfer can incentivize risk reduction, leading to a more stable cyber security landscape. This would achieve concurrent goals of attracting more consumers and suppliers of insurance resultant from more data and less risk leading to more efficient pricing of the product.

### **Building Risk into Cyber Insurance Pricing**

Within the last six years, research has begun to price risk into insurance policies. Herath and Herath recommend a premium pricing strategy using a Copula-based method combined with an actuarial approach and introduced coinsurance and deductibles as elements of the insurance contract [77]. Their inclusion of deductibles and coinsurance in this model was limited to its effect on premium pricing, and to the best of our knowledge, is the only model to date that incorporates deductibles and coinsurance into a pricing

strategy. Continuing with the Copula-based model development, Mukhopadhyay, Chatterjee, Saha, Mahanti, and Sadhukhan presented a Copula-aided Bayesian Belief Network combined with a utility model to measure not only an information technology network's vulnerabilities, but ultimately justified investment by information technology companies in cyber insurance using a net present value calculation [78]. These research areas focus quantifying the risks associated with information technology systems and incorporating them into insurance premiums. This research will undoubtedly be built upon and used as cyber insurance becomes more prevalent in the market. Young et al. completed work on a model that featured the insurance policy as an incentive device for direct self-investment in cyber security. Their framework proposed premium reductions contingent on security investment to develop an optimal security budget, achieving dual goals of reducing and transferring cyber risk at critical infrastructure companies [79]. The preceding literature has made the case that insurance policies in the cyber landscape could be viable. Using established research, we will take build on these foundations to create a more robust incentive device.

## **Summary**

This review of literature described how the role of insurance as a de facto regulatory authority could be applied in the modern cyber arena. Building on the idea that insurance companies have the capability to influence those seeking insurance, we described how insurance theory has evolved into a new field of insurance economics through the application of risk management and reduction principals. The description of how insurance policies were developed in theory and applied in different industries today

to combat asymmetric information in the market, specifically moral hazard, has provided a reference point on which to build our insurance model.

A review of the current state of the industry developed an understanding of why standalone cyber insurance policies are having trouble gaining momentum. However, the review did support the use of insurance as an incentive device in the cyber security arena with both theory and proposals for specific cyber models. The first research question can be answered using by the literature review. Cost sharing factors, such as coinsurance and deductibles can be used to incentivize the insured to act in a manner in which they may not otherwise act. By adding an economic responsibility associated with the behavior of the insured, the insurer gains some assurance that the insured will participate in reducing risk. Using this information, our model will provide a framework that will encourage both the reduction and transfer of risk simultaneously through the use of cyber insurance policies. In the proceeding chapters, the methodology of building the model will be described, the application of data and results will be discussed, and we will consider the implications of the research and recommendations for future work.

### **III. Methodology**

#### **Chapter Overview**

The purpose of this chapter is to describe the two stages of the research methodology. The first stage describes the approach used to develop additional insurance components in order to extend the cyber insurance framework previously developed by Young et al. The second stage describes the statistical approach used to validate the

extended model's functionality using real-world reliability data provided by the power industry through regulatory self-reporting. The model development was guided by insurance economic theory and moral hazard principles described by Young et al. This research will evaluate if the extended cyber insurance model can account for incentivizing self-investment in cyber security and risk transfer as a mitigation strategy to reduce risk. Of particular interest is assessing risk reduction to a particular region of the U.S. served by the power industry and/or across the enterprise (i.e., all U.S. regions). The cyber insurance framework is represented mathematically along with variable definitions. Next, the model is described in detail—baseline conditions, variables, calculations embedded in the model, and optimization settings. Finally, a description of the data used in the analysis is provided.

### **Operationalizing the Cyber Insurance Framework**

Young's et al. framework integrated four distinct models resulting in a quantitative cyber risk framework based on the principles of identifying, assessing, planning and monitoring risk. The framework includes a: (i) threat likelihood and severity model; (ii) reduction of threat likelihood and severity model; (iii) Gordon-Loeb Model class II security breach function; and (iv) an insurance premium discount model. The proposed extension to the cyber insurance framework presented here incorporates insurance components available in a wide range of insurance policy offerings but not previously considered by Young et al. namely, (i) coinsurance and (ii) deductible. The variables in the framework are defined in Table 3 and Table 4.

The wealth of a firm in a loss scenario can be projected using Equation (1). The initial wealth ( $W$ ) will be reduced by the costs of the insurance premium, ( $P$ ), direct security investment, ( $z$ ), deductible payment,  $\min(S(z, v)\lambda * D, (D * \lambda))$ , coinsurance payment,  $(S(z, v)\lambda - (\min(S(z, v)\lambda * D, (D * \lambda))) * C)$ , and residual risk not accounted for.

$$Wealth = W - (P + z + \min(S(z, v)\lambda * D, (D * \lambda)) + (S(z, v)\lambda - (\min(S(z, v)\lambda * D, (D * \lambda))) * C) + \varepsilon) \quad (1)$$

Where:

$$S(z, v) = \text{Expected Loss Conditioned by Security Investment} \quad (2)$$

The operationalization of wealth in a loss scenario establishes the foundation for the minimization used in the model. Insurance variables and premium calculation methods are detailed below.

### **Threat Likelihood Model**

The traditional threat likelihood mode uses an annual rate of occurrence and the expected probability of success of a single event [79]. The product of the threat likelihood model is a single loss expectancy (SLE) given an annual loss expectancy (ALE), which in this model is represented by an annual threat severity ( $\lambda$ ), vulnerability, ( $v$ ), and threat ( $t$ ). The equation for  $SLE$  is outlined in Equation (3).

$$SLE = \lambda * v * t \quad (3)$$

Table 4. Threat likelihood and reduction of threat likelihood variables.

| Variable     | Definition                                                                                                                                 |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| $\lambda$    | Estimated monetary loss caused in a single breach (SLE), also the value of the insurance policy in this model                              |
| $t$          | Probability of an attempted breach                                                                                                         |
| $v$          | Vulnerability                                                                                                                              |
| $\lambda vt$ | The expected loss conditioned on no new additional security investment                                                                     |
| $z$          | Monetary investment in additional security                                                                                                 |
| $S(z,v)$     | Security breach probability function expressing the probability that security will be breached given a monetary investment in security $z$ |
| $\alpha$     | Effectiveness of security investment                                                                                                       |
| $D$          | Deductible percentage                                                                                                                      |
| $C$          | Coinsurance percentage                                                                                                                     |

### Reduction of Threat Likelihood Model

The reduction of threat likelihood model illustrates the optimal investment for a given vulnerability and has been adopted from the Gordon-Loeb class II security investment function. In this model, the given vulnerability represents the vulnerability of the OT network used at power companies. The function illustrates a concave function which identifies an optimal point of investment, past which, the marginal costs outweigh the marginal benefits and the investor experience experiences diminishing returns [80]. The effectiveness of security controls used in this framework calculates the probability of successful attack given security investment and vulnerability ( $S(z,v)$ ), an initial vulnerability ( $v$ ), a security investment effectiveness level, ( $\alpha$ ), and a security investment, ( $z$ ). The effectiveness of security controls can be modeled as:

$$S^{II}(z, v) = v^{\alpha z + 1} \quad (4)$$

### Insurance Premium Discount Model

The insurance premium discount model uses a base rate premium and incorporates discounts based assumed value of assets; the rate of discount offered by insurance companies for security investment,  $r$ ; the attained insurance discount,  $\delta$ ; the probability of a successful cyber attacked after security investment,  $S(z,v)$ ; deductible

discounts,  $D^*$ ; and coinsurance discounts,  $C^*$  [79]. Table 4 illustrates the progression from the base rate insurance premium to the final premium paid by the insured.

**Table 5. Insurance premium discount model.**

| Variable | Definition                                  | Derivation                          |
|----------|---------------------------------------------|-------------------------------------|
| D        | Deductible percentage                       | Model recommendation                |
| C        | Coinsurance percentage                      | Model recommendation                |
| $D^*$    | Amount of loss assumed by insured           | $D^* = (\lambda * D)$               |
| $C^*$    | Amount of loss assumed by insured           | $C^* = ((\lambda - D^*) * C)$       |
| $P_0$    | Base rate insurance premium                 | $P_0 = (\lambda - D^* - C^*) * 8\%$ |
| $r$      | Rate of discount for investment in security | 50%                                 |
| $\delta$ | Attained insurance discount                 | $\delta = r (1 - S(z, v))$          |
| $P$      | Total insurance premium                     | $P = P_0 (1 - \delta)$              |

This research follows the Young et al. insurance premium discount model by using the initial loss severity to build out the insurance premiums. Moving forward, this research operates under the assumption that the insurance coverage purchased will be equal to the estimated severity. This was assumed because power companies will reasonably seek insurance up to the maximum loss that they expect to sustain. The base rate insurance premium was derived using 8% of asset value (in this case, loss severity). This figure was used as the starting point for insurance premium prices in the early era of the commercial airline industry and gradually adjusted as the industry matured [81]. Given the base rate premium,  $P_0$ , the model must now incorporate discounts offered in exchange for direct security investment and cost sharing in the form of deductibles and coinsurance:

**Deductible Discount, ( $D^*$ ):** The discount offered as a result of the insured assuming responsibility for a deductible was calculated using a straight line method,

where the amount of the deductible in dollars is subtracted from the initial coverage amount (loss severity) prior to the calculation of  $P_0$ . This method was used because the deductible reduces the amount of loss that the insurance company is responsible for and therefore should not be a factor in determining the premium.

**Coinsurance Discount, ( $C^*$ ):** The discount offered as a result of the insured assuming responsibility for a coinsurance cost was also calculated using a straight line method, where the amount of loss that the insured would assume is subtracted from the initial loss severity prior to the calculation  $P_0$ . This reduces the amount of coverage the insurance company is responsible for and therefore should not be considered as a chargeable expense in the premium.

**Security Rate of Discount, ( $r$ ):** The premium discount provided by the insurer is set by the insurer and discounts the policy premium by  $r\%$  of the reduction in vulnerability resultant from the security investment.

**Security Spending Premium Discount, ( $\delta$ ):** The insurance discount received resultant from security investment is the reduction in vulnerability multiplied by the insurance discount offered by the insurer. It is calculated as:

$$\delta = r(1 - S(z, v)) \quad (5)$$

## **Baseline Conditions**

### **Power Interruptions**

Amongst the electrical industry, there are several definitions for what could be considered a power interruption. The Institute of Electrical and Electronic Engineers

(IEEE) considers a power interruption to be the total loss of power to one or more customers connected to the electrical distribution system [82]. The IEEE also discriminates between momentary and sustained interruptions, using five minutes as the threshold between momentary and sustained [82]. The U.S. Department of Energy requires incident reports for a variety of events that may or may not result in interruptions to consumers, among which, the events is a loss of power to more than 50,000 customers for at least an hour [83]. To ensure clarity from this point forward, any reference to a power interruption will assume the IEEE standard of a sustained outage. The decision to use the IEEE standard for this research is based on the fact that reliability data collected by the Energy Information Administration uses the IEEE sustained interruption standard.

### **Model Inputs**

The baseline conditions for the model are values assigned to variables required for the model. The rationale for each variable is detailed in the following sections:

**Threat, (t):** The 2015 Critical Infrastructure Readiness Report found that nearly nine out of ten companies have experienced an attack in the last year, allowing for the use of a 90% threat estimate [84].

**Vulnerability, (v):** Also in the Critical Infrastructure Readiness Report, 55% of the companies interviewed experienced physical damage during those attacks and 33% experienced disruptions in their daily business cycles. The average of these two figures was used to estimate that 46% of the attacks resulted in success of some sort [84].

**Loss Severity Calculation, ( $\lambda$ ):** The annual loss severity used as the amount of coverage sought by the power company was calculated using power outage reliability figures and customer data reported via form EIA-861 to the Energy Information

Administration annually. The calculation method was developed by Berkeley National Lab for the Department of Energy and estimates the economic losses in the event of an outage using inputs reported by power companies described below. The calculator also accounts for regional differences by differentiating between residential and commercial customers, backup power capability at commercial customer's facilities, time of day, and time of year [85]. The inputs required for the calculator are as follows:

1. **SAIDI Index:** This index represents the average length of time customers are interrupted, it is defined as:

$$SAIDI = \frac{\text{Sum of sustained interruption durations for all customers}}{\text{Total number of customers served}} \quad (6)$$

2. **SAIFI Index:** This index represents the total number of customer interruptions per customer for a specified electric supply system and is defined as:

$$SAIFI = \frac{\text{Total number of sustained interruptions for all customers}}{\text{Total number of customers served}} \quad (7)$$

3. Number of residential customers served by the power company
4. Number of non-residential customers (i.e., manufacturing and industrial) in the populations

While the severity estimate has validity as a worst case scenario for a cyber incident, the true value of this framework is including real-world available reliability metrics to provide a first look at applicability and scalability as concurrent research continues to adjust vulnerability and threat parameters, and further refine loss estimates associated with cyber incidents.

**Operational Technology Security Budget:** The security budget of a company is estimated using the revenue of power companies reporting reliability numbers to the EIA

[86]. The EIA data is publically accessible from their web site. To develop a realistic operational technology budget, information technology budgets were used as a proxy. Private consulting firms recommend that between 3% - 7% of revenue should be used as an IT budget baseline depending on the stability of the IT budget in prior years and whether the company is experiencing rapid growth [87], [88]. The IT Security Spending Trends Survey Report by the SANS Institute suggests that companies typically spend between 7% - 9% of their IT budgets on IT security [89]. Using the spend range categories from Table 5, the average revenue calculation is used to develop a general OT security budget using 5% of revenue and 8% of the resultant IT budget using the assumption that OT budgets have been underfunded in recent years.

**Table 6. Calculated security investment effectiveness.**

| <b>Spend Range (\$M)</b> | <b>Avg. Revenue</b> | <b>Security Budget (\$K)</b> | <b>Alpha (<math>\alpha</math>)</b> |
|--------------------------|---------------------|------------------------------|------------------------------------|
| \$0-\$50                 | \$27,072.41         | \$108.29                     | 2.63908E-05                        |
| \$50-\$100               | \$70,472.33         | \$281.89                     | 1.01382E-05                        |
| \$100-\$500              | \$214,530.20        | \$858.12                     | 3.3304E-06                         |
| >\$500                   | \$1,851,776.00      | \$7,407.10                   | 3.858E-07                          |

**Productivity of Security Investment, ( $\alpha$ ):** Alpha values in Table 6 were derived by implementing conservative values assuming companies opt to implement the full security budget listed in Table 5. If the full security budget is implemented, a company (on average) can expect to experience the following outcomes: (i) 5% probability of successful attack, ( $S(z,v)$ ), (ii) 46% for  $v$  as estimated earlier, and (iii) 90% for  $t$ , as described earlier. Using Equation (4), the corresponding values for alpha under the security budget investments are listed in Table 6.

## Optimization

The minimization for the model is the expected loss conditioned on security investment multiplied by loss severity and threat, combined with the costs of the security investment, premium, deductible expenses and coinsurance expenses. The minimization seeks to minimize the amount by which the initial wealth is reduced as defined in Equation (1).

$$\text{Minimize: } [S(z, v)\lambda t + z + P + D_{Exp} + C_{Exp}] \quad (8)$$

### Decision Variables

**Deductible Percentage (D):** The percentage of loss severity that an insured will be responsible for in the event of an incident, prior to any payouts from the insurer.

**Deductible Toggle:** A binary on/off switch in the optimization that serves as a multiplier for the deductible percentage, effectively including or excluding the costs from being considered in the optimization.

**Coinsurance Percentage (C):** The percentage of loss severity, after the deductible is paid, that the insured is responsible for.

**Coinsurance Toggle:** A binary on/off switch in the optimization that serves as a multiplier for the coinsurance percentage, effectively including or excluding the costs from being considered in the optimization.

**Direct Security Investment, (z):** The dollar amount of direct self-investment by the power company in to cyber security.

### Constraints

In addition to default non-negative constraints, in order to make the optimization successful, the restraints outlined in Table 7:

**Table 7. Optimization constraints.**

| <b>Constraint</b>                   | <b>Explanation</b>                                                                                                                                                                                                                    |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| $z < \lambda$                       | If direct security investment is equal to or more than security, company should self-insure                                                                                                                                           |
| $P + z \leq \text{Security Budget}$ | The OT security budget cannot exceed budget constraints. *This can be turned on/off depending whether the model is determining an optimal budget without constraints or attempting to develop an allocation that remains under budget |
| $\text{Combined Toggle} \geq 0$     | The sum of the deductible and coinsurance toggles, this sum can also be set to $=0, \geq 1$ , or $\geq 2$ , depending on the preferences of the parties involved                                                                      |
| $\text{Deductible Toggle} \geq 0$   | This constraint can be adjusted to $=0$ , or $\geq 1$ , depending on preferences for inclusion of a deductible in the model                                                                                                           |
| $\text{Coinsurance Toggle} \geq 0$  | This constraint can be adjusted to $=0$ , or $\geq 1$ , depending on preferences for inclusion of coinsurance in the model                                                                                                            |

### Solver Settings

The optimization software used to develop this framework and run all associated optimizations is Frontline Systems, Inc. Analytic Solver Platform V2016-R2. The settings are detailed in Table 8.

**Table 8 - Analytic Solver settings**

| <b>Parameter Option</b>     | <b>Variable</b>    |
|-----------------------------|--------------------|
| Algorithm                   | GRG nonlinear      |
| Maximum Time                | 100 seconds        |
| Iterations                  | 1000               |
| Precision                   | $1 \times 10^{-6}$ |
| Convergence                 | 0.0001             |
| Multi-Start Search          | Enabled            |
| Require Bounds on Variables | Enabled            |
| Estimates                   | Tangent            |
| Derivatives                 | Forward            |
| Search                      | Newton             |
| Maximum Sub Problems        | 5000               |
| Maximum Feasible Solutions  | 5000               |

## **Data Diagnostics**

### **Model Confirmation**

To ensure that the extension of the Young et al. base model works correctly, a scenario from their published work was re-created. The extended model's deductible and coinsurance capabilities were forced to zero using the constraints previously described, and the scenario was repeated 35 times. The results were used to establish a 95% confidence interval (CI). The 95% CI intersected entirely within the Young et al. model's published results.

### **Energy Industry Reliability Data**

Organizations were established to track energy industry statistics in response to the oil market disruption of 1973, resulting in the establishment of the Energy Information Association in 1977 through the Department of Energy Organization Act [90]. The EIA collects information from a sample of industry participants via the EIA-861, "Annual Electric Power Industry Report" [86]. When considering the power industry as a whole, this research refers to any power company that is operated as a municipal, state, federal, investor owned, cooperative, political subdivision, or transmission entity. Power marketing companies were excluded, as they do not have power generation capabilities.



**Figure 3. NERC Regions North America [91].**

### **Sampling Strategy**

The sampling strategy is a stratified sample across using North American Electric Reliability Corporation's (NERC) regions as a grouping factor. The NERC regions, provided in Figure 3, are used to allocate companies to a single group. All NERC regions will contain an equal sample, which is restricted by the smallest sample available in the EIA self-reported data (see Table 9, 2013, FRCC,  $n = 10$ ). This approach provides a balanced design (e.g., equal group sizes) to minimize effects for ANOVA models. The parsing process randomly selected 10 companies from each of the eight regions. Reported data included an independent service organization (MISO) and the state of Alaska, which were excluded because they did not meet the minimum ( $n = 10$ ) threshold. Samples were drawn from three consecutive years of available self-reported EIA data, 2013 through 2015, providing a total sample size of  $n = 240$  for assessing the model. The sampling data represents over 200 companies across 42 states. The stages of the parsing process are outlined in Table 9.

**Table 9. Data parsing process.**

|                                  |               |     |      |     |      |     |     |      |      |    |
|----------------------------------|---------------|-----|------|-----|------|-----|-----|------|------|----|
| Year                             | 2015          |     |      |     |      |     |     |      |      |    |
| Available Operational Data       | 2,286         |     |      |     |      |     |     |      |      |    |
| No. Reported Reliability Metrics | 1045 (45.71%) |     |      |     |      |     |     |      |      |    |
| No. Reported All Attributes      | 487 (21.30%)  |     |      |     |      |     |     |      |      |    |
| NERC Region                      | FRCC          | MRO | NPCC | RFC | SERC | SPP | TRE | WECC | MISO | AK |
| Data Available by Region         | 11            | 80  | 23   | 98  | 138  | 44  | 13  | 70   | 7    | 3  |
|                                  |               |     |      |     |      |     |     |      |      |    |
| Year                             | 2014          |     |      |     |      |     |     |      |      |    |
| Available Operational Data       | 2,249         |     |      |     |      |     |     |      |      |    |
| No. Reported Reliability Metrics | 1231 (54.74%) |     |      |     |      |     |     |      |      |    |
| No. Reported All Attributes      | 488 (21.70%)  |     |      |     |      |     |     |      |      |    |
| NERC Region                      | FRCC          | MRO | NPCC | RFC | SERC | SPP | TRE | WECC | MISO | AK |
| Data Available by Region         | 12            | 86  | 21   | 94  | 133  | 39  | 21  | 72   | 6    | 4  |
|                                  |               |     |      |     |      |     |     |      |      |    |
| Year                             | 2013          |     |      |     |      |     |     |      |      |    |
| Available Operational Data       | 2,197         |     |      |     |      |     |     |      |      |    |
| No. Reported Reliability Metrics | 965 (43.92%)  |     |      |     |      |     |     |      |      |    |
| No. Reported All Attributes      | 456 (20.76%)  |     |      |     |      |     |     |      |      |    |
| NERC Region                      | FRCC          | MRO | NPCC | RFC | SERC | SPP | TRE | WECC | MISO | AK |
| Data Available by Region         | 10            | 79  | 22   | 82  | 130  | 36  | 15  | 72   | 6    | 4  |

**Company Scenarios**

The model will be use the baseline conditions described earlier:  $t$  at 90%, a  $v$  value of 46% and the initial base rate premium of 8%. Building on the Young et al. framework the insurance discount is based on a security investment offered by insurance companies,  $r$ , and is set to 50%. The calculated  $\alpha$  values for each company will correspond to the size of the company as calculated in Table 5. Our analysis will focus on the allocation of a cyber security budget under no constraints. This provides insight into what the optimal security budget would look like under the variety of circumstances provided by the data reported to the EIA. Additionally, the unconstrained budget was

chosen due to the inability for some of the analyzed companies to obtain insurance for the full loss severity within the estimated constrained budget described in Chapter 3. It was determined that more data under no budget constraints would be more effective in spotting trends on an industry scale versus fewer data points in the presence of a constrained budget.

### **Data Discovery and Analysis**

The sample data will be assessed for normality using quantile plots, visual aids of the sampling distributions, 2nd, 3rd, and 4th order moments, equal variance analysis using unequal variance tests and residual analysis, and if required, transformations. A nonparametric Analysis of Variance (ANOVA) equivalent test for k groups called the Kruskal-Wallis test will be considered if the sampling distributions demonstrate power issues due to non-normality (e.g., non-Gaussian), unequal variance, or extreme outliers. Since the dependent variable (EIA reliability data) is continuous and the independent variable used for grouping (NERC Region) nominal (e.g., categorical), a single-factor ANOVA is appropriate to assess if any differences exist across groups. The reliability data will be compared in pre-treatment and post-treatment conditions to test for effects by region. In this research, emphasis will be placed on assessing whether post-treatment outcomes indicate a risk reduction within any NERC region and across all regions. Post Hoc pairwise testing will be performed, if required, using the Tukey Honestly Significant Difference (HSD) test.

### **Revenue versus Loss Metric**

The annual loss expectancy and the conditioned loss post treatment were used to determine the effectiveness of the model. These numbers represent the pre-treatment,

unconditioned losses anticipated and the post-treatment expected loss as generated by the model. These losses were normalized by dividing by that company's revenue, to generate a percentage of revenue loss for the company analyzed. This generated a loss ratio that could be used for comparison between companies. The smaller the ratio, the better the performance of the company, as the losses are a smaller portion of the annual revenue earned during the time period, which in this case, is a year.

## **IV. Analysis and Results**

### **Chapter Overview**

This chapter will provide the results of testing the extended framework through the application of power industry data. The results begin with a preliminary analysis of the power industry by NERC region prior to model treatment. Factors that affected security allocation, budget recommendations and structure of insurance policy will also be identified.

### **Pre-Treatment**

Power companies within each NERC region represent a variety of sizes with respect to revenue. Visual analysis through scatter plots, frequency distributions, and summary statistics illustrated in Figure 4 confirm the data represents a wide range of revenue observations with a moderate number of extreme outlier values. Therefore, using company size (as represented by revenue) as a continuous dependent variable (e.g. small, medium, and large) based exclusively on raw revenue is not a feasible approach that can scale across such a broad range of values. Since all NERC regions contain a

wide range of company sizes, a ratio of “Actual Loss as a Percentage of Revenue” was selected for the dependent variable for pre-treatment evaluation, and “Expected Loss as a Percentage of Revenue” for post-treatment evaluation. Company assignment to a NERC region is mutually exclusive on a per year basis.

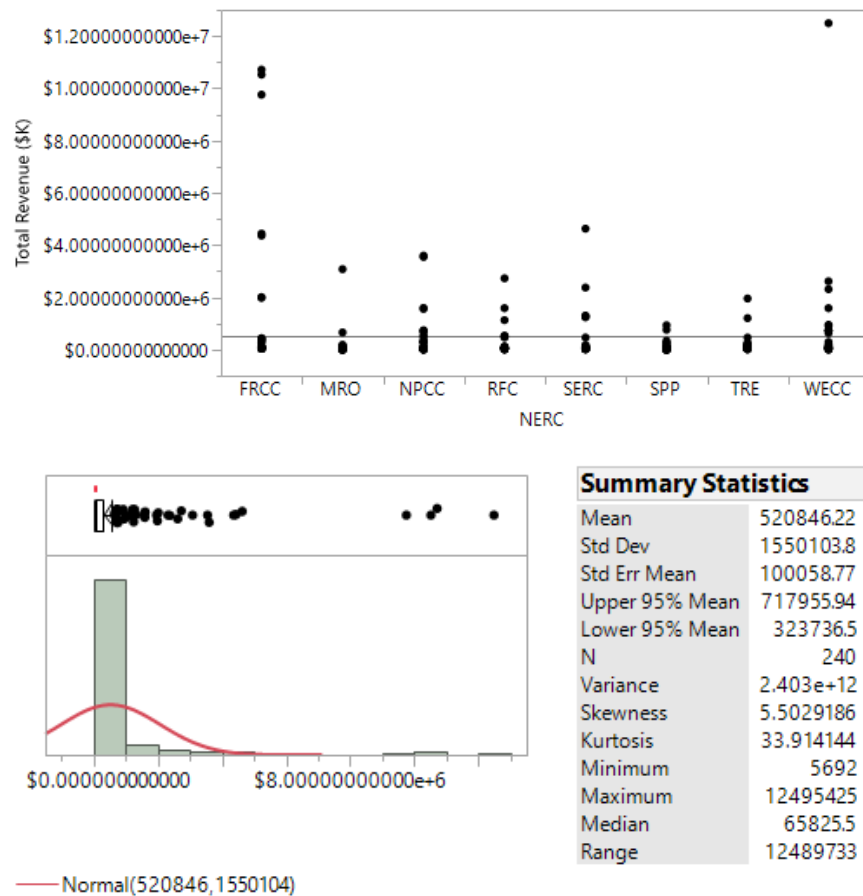
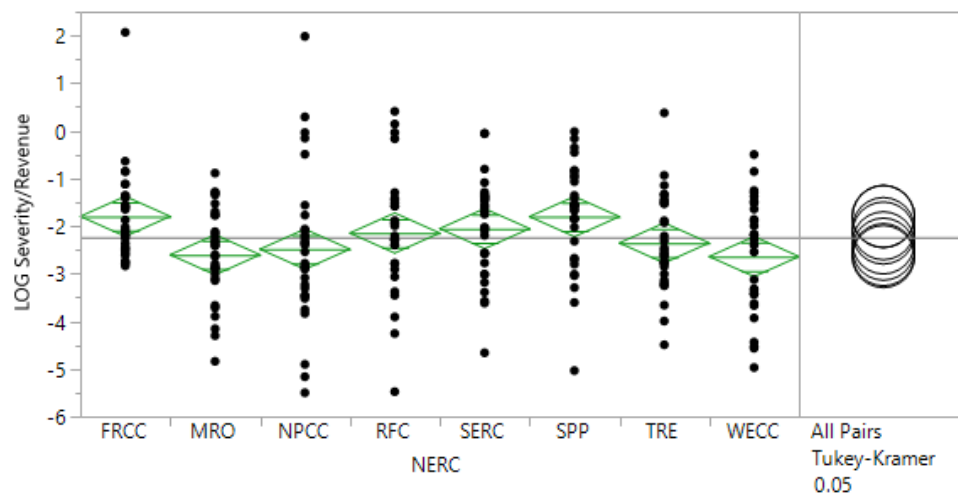


**Figure 4. Summary statistics for revenue, 2013-2015 (n = 240).**

### Major Disruptive Event (MED)

Outlier analysis also revealed some extreme values in the self-reported data set as a result of an observed phenomenon known as a Major Event Days (MED). These events are considered a low probability of occurrence with high impact and appear as extreme

outliers in the data set. The decision to retain the extreme outlier values in the data set is based on the following facts: (i) MED's are naturally occurring real events (although infrequent) that are typically unforeseen (e.g., hurricanes, earthquakes, and blackouts), (ii) impact all company sizes, and (iii) have to be addressed and mitigated by the companies affected. Furthermore, ANOVA analysis reveals that at  $\alpha = 0.05$ , no NERC region is significantly different from the other when comparing the means of loss severity as a percentage of revenue. The ANOVA and Tukey-Kramer HSD tests are displayed in Figure 5. This indicates that each region has learned to contend with interruption events peculiar to their geographic location, such as MED's. Further analysis of the SAIDI, SAIFI and customer populations indicate that there are some differences between regions in each of these categories, but as Figure 5 shows, these inputs do not have enough impact to alter the overall loss experienced by the company. Figure 6, Figure 7, Figure 8, and Figure 9 show the statistical differences between regions by customer and reliability measures.



### Connecting Letters Report

| Level  | Mean      |
|--------|-----------|
| FRCC A | -1.796099 |
| SPP A  | -1.800387 |
| SERC A | -2.053077 |
| RFC A  | -2.145816 |
| TRE A  | -2.352270 |
| NPCC A | -2.483964 |
| MRO A  | -2.600412 |
| WECC A | -2.639540 |

Levels not connected by same letter are significantly different.

### Analysis of Variance

| Source   | DF  | Sum of Squares | Mean Square | F Ratio | Prob > F |
|----------|-----|----------------|-------------|---------|----------|
| NERC     | 7   | 23.86430       | 3.40919     | 2.4927  | 0.0174*  |
| Error    | 232 | 317.30123      | 1.36768     |         |          |
| C. Total | 239 | 341.16553      |             |         |          |

**Figure 5. Pre-treatment loss severity as a percentage of revenue.**

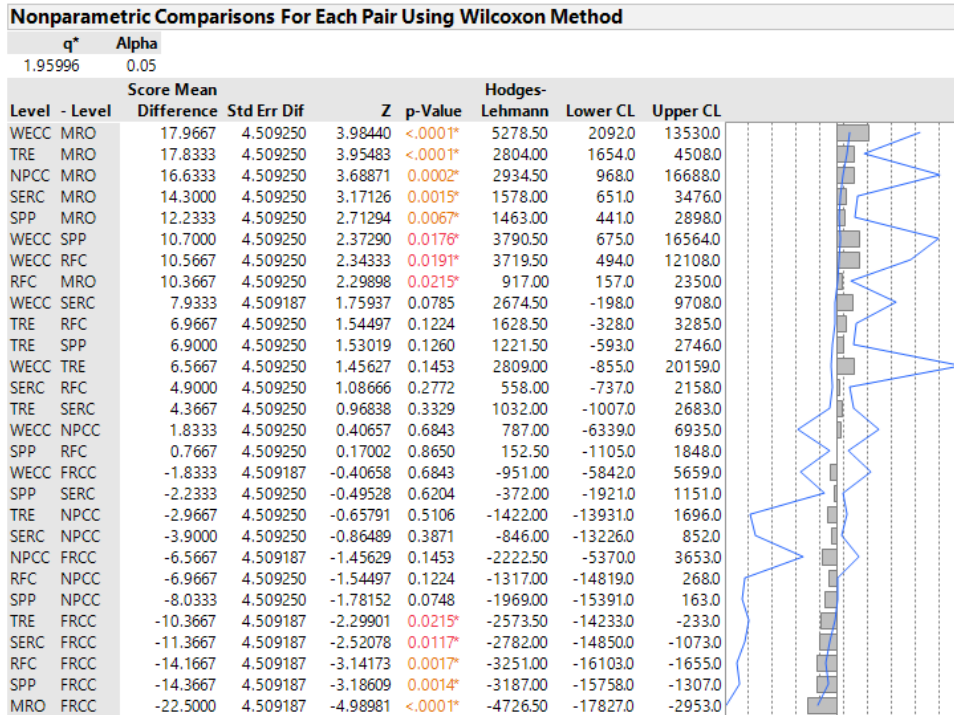


Figure 6. Commercial population comparisons between NERC regions.

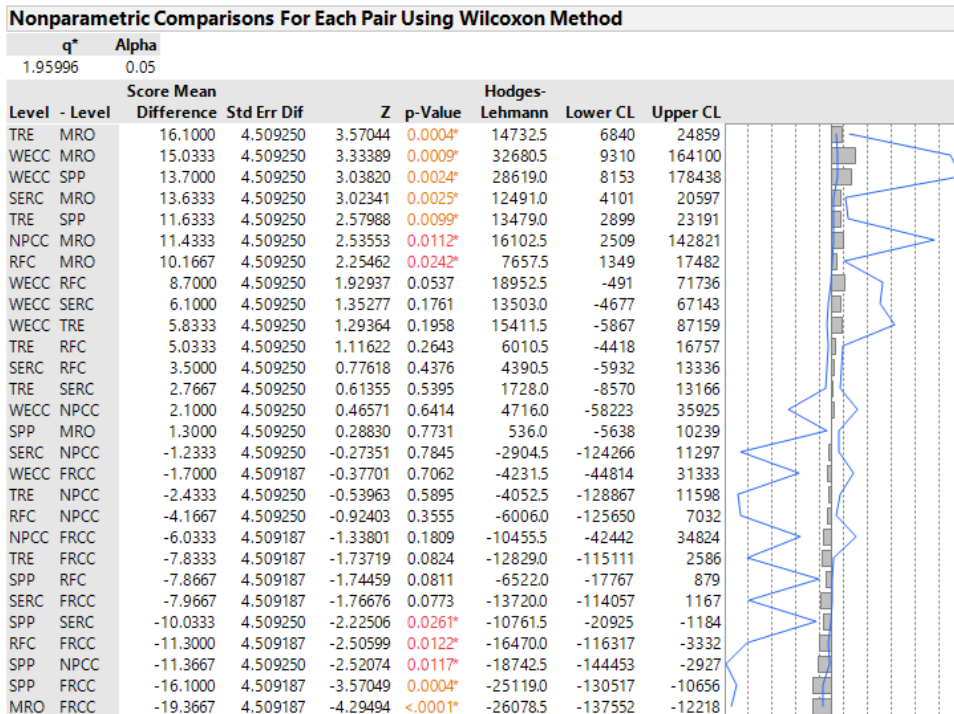


Figure 7. Residential population comparisons between NERC regions.

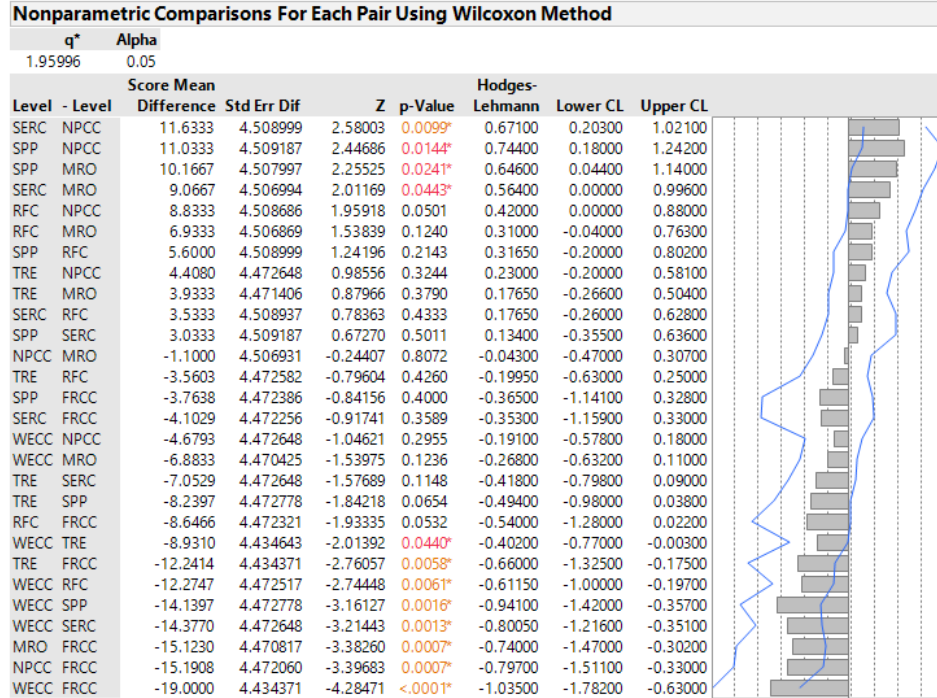


Figure 8. SAIFI comparisons between NERC regions.

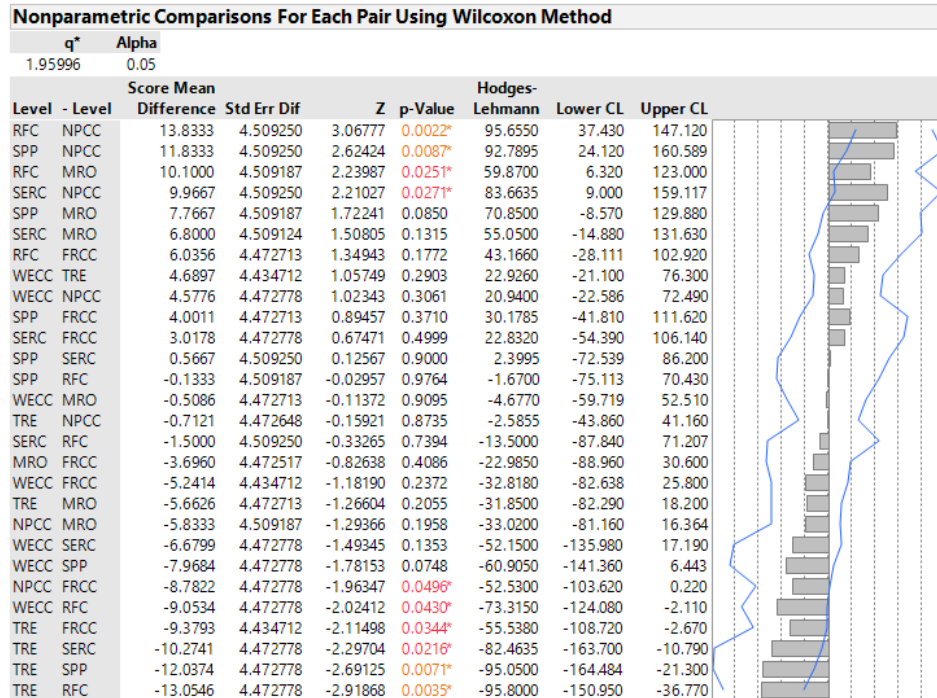


Figure 9. SAIDI comparisons between NERC regions.

### **Extended Insurance Model Policy Options**

This framework, built on the Young et al. model has the capability to represent four general policy structures. The introduction of additional economic elements in this model represent cost sharing on the part of the insured, where they will be responsible for a portion of the losses. Cost sharing in this model will come in the form of a deductible, coinsurance, both, or no cost sharing. Deductibles are structured so that the insured will be required to pay the deductible amount out of pocket prior to receiving any compensation from the insurer. Coinsurance represents a scenario where the insured will pay a portion of the losses in conjunction with the insurer simultaneously. In the case where both a deductible and coinsurance mechanism is recommended, the deductible will be paid first by the insured and the coinsurance payment will be divided as dictated by the coinsurance percentage on the remainder of the damages beyond the deductible amount. The Young et al. model represents the default structure, with no deductible or coinsurance options. Table 10 shows the type of cost sharing mechanisms available in the extended insurance model and the responsibility assumed by both the insured and insurer.

**Table 10. Types of cost sharing options included in extended insurance model.**

| Type             | Insured Responsibility                                                                                                        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Deductible Only  | Full deductible amount before insurer pays                                                                                    |
| Coinsurance Only | Percentage of covered losses in conjunction with insurer as dictated by insurance contract                                    |
| Both             | Full deductible before insurer payment and coinsurance payment in conjunction with the insurer on remainder of covered losses |
| None             | Insurer responsible for all covered losses                                                                                    |

Table 11 illustrates the responsibility by each party in a hypothetical scenario. It should be noted that when the loss experienced is less than the total coverage, the coinsurance is more advantageous to the insured. The deductible is only more advantageous to the insured when it is a fixed dollar amount and the loss is sufficient that the coinsurance expenses would exceed the fixed deductible expense.

**Table 11. Insured and insurer responsibilities given different cost sharing structures.**

| Type             | Amount                                         | Loss  | Insured Pays | Insurer Pays |
|------------------|------------------------------------------------|-------|--------------|--------------|
| Deductible Only  | 10% of Loss                                    | \$100 | \$10         | \$90         |
| Coinsurance Only | 10% of Loss                                    | \$100 | \$10         | \$90         |
| Both             | 10% of Loss, 10% of remainder after deductible | \$100 | \$10 + \$9   | \$81         |
| None             | N/A                                            | \$100 | \$0          | \$100        |

## **Assessing the Extended Insurance Model**

To assess if the model is stable and capable of providing insurance policy options that incentivize power industry asset owners to self-investment, all data points were introduced to the model. The results will be reported immediately below, and factors of the model that were found to be statistically significant will be discussed in the following section.

The extended insurance policy options model outputs are illustrated in Figure 10. The vertical bars represent the number of companies associated with a specific policy option (i) None = no deductible and no coinsurance, (ii) Coinsurance = coinsurance only, and (iii) Both = coinsurance and deductible. The horizontal connected line above the vertical bars represents the average amount in dollars of security self-investment recommended for a particular insurance policy option. Figure 10 can be interpreted as follows: (i) 50 companies should not participate in any additional cost sharing, (ii) 68 companies should engage in partial cost sharing through coinsurance only, and (iii) 122 companies should utilize the maximum amount of cost sharing available through coinsurance and deductible. No companies in the data set should opt for a deductible only policy. Addressing the deductible only policy option for the extended model will be discussed further in the limitations section.

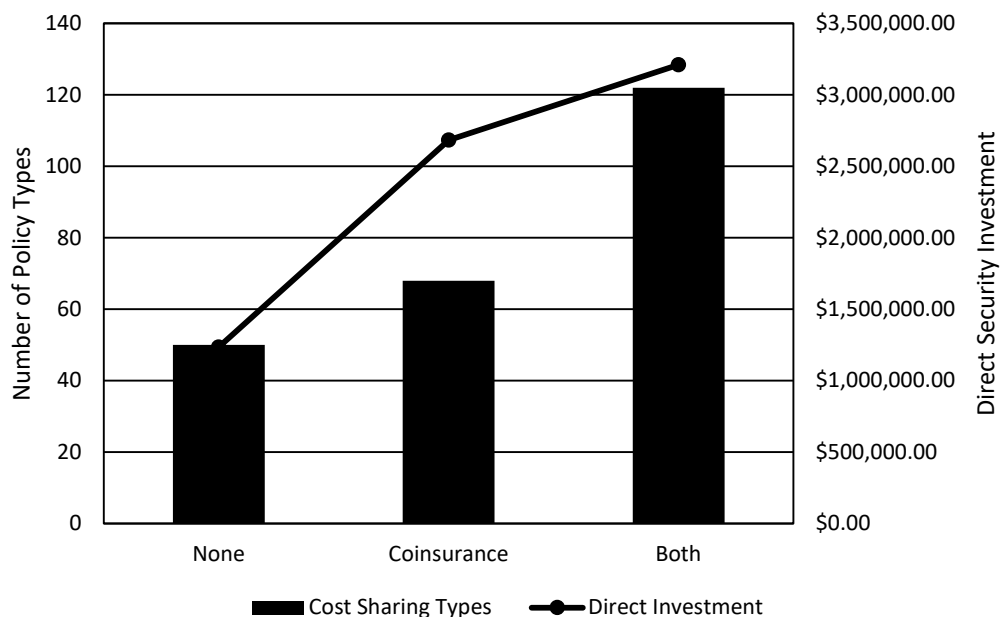


**Figure 10. Recommended insurance policy structure and security investment.**

Figure 11 describes additional characteristics of each type of insurance policy option that exhibit statistical significance. The extended insurance model recommends companies with higher pre-treatment losses, depicted by the bar chart and measured on the primary vertical axis should engage in full cost sharing practices using both coinsurance and a deductible. The recommended security budget, as a percentage of revenue is depicted by the line graph and measured on the secondary vertical axis. This budget recommendation indicates that those companies anticipating higher losses than industry peers should spend more on reducing risk via direct cyber security investment. By assuming more risk through engaging in more cost sharing, the model's recommendation to spend more on risk reduction indicates that the incentive mechanism is working.

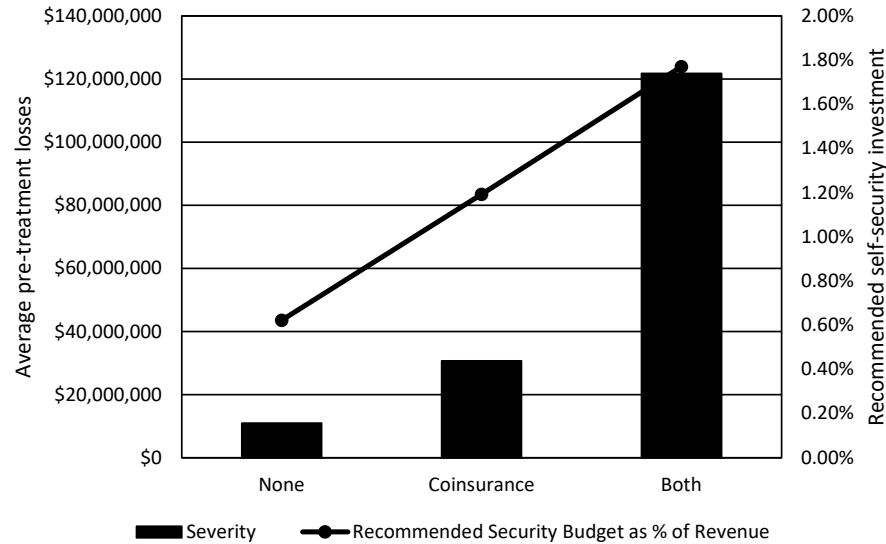


**Figure 11. Average pre-treatment losses and recommended direct self-security investment.**

Figure 12 shows the post-treatment losses as a percentage of revenue, measured on the primary axis, and the probability of a successful attack, as measured on the secondary axis sorted by recommended insurance option. A comparison of each of the elements in Figure 10, Figure 11, and Figure 12 shows how the relationship between the expected losses in pre-treatment and post-treatment conditions, direct investment, and probability of a successful attack illustrates the nature of diminishing returns on security self-investment, which is a feature of the reduction of threat likelihood model used in this framework. Companies that anticipate lower initial losses experience an apex in the effectiveness of additional security investments, after which, the value of additional investment decreases. The model can detect the threshold and therefore stops investing, which results in higher successful attack probabilities. This explains why the companies who participate in no cost sharing exhibit the lowest pre-treatment losses in Figure 11,

but have the highest post-treatment losses in Figure 12. What may seem like an anomaly is actually a result of the model determining that higher expected losses outweigh the expenses of additional security investment. In dollar terms, companies that received the recommendation not to engage in cost sharing invested about half as much in direct security investment as companies who were recommended to engage in partial cost sharing, but the expected loss are about the same.

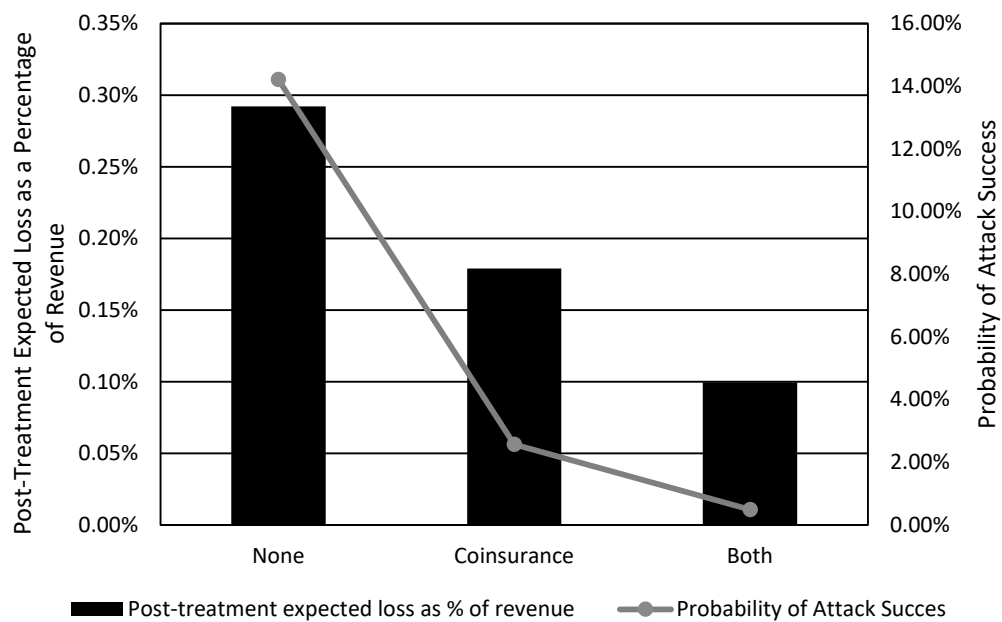


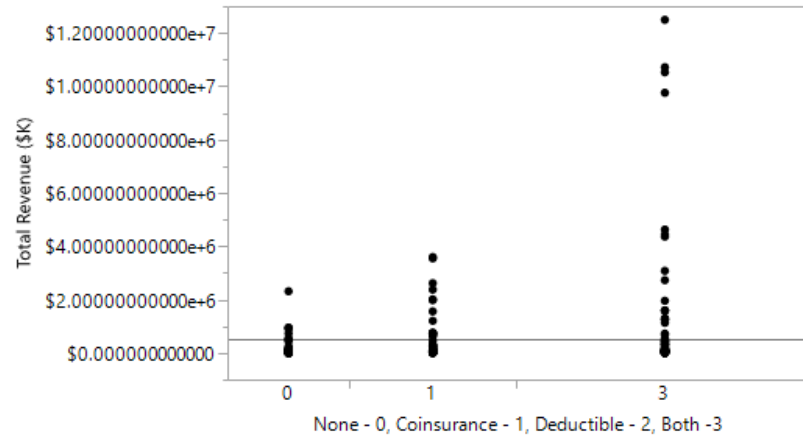
**Figure 12. Average post-treatment loss and probability of a successful attack for each insurance policy option.**

### Significant Factors in Extended Insurance Model

The factors found to be statistically different in the extended insurance model are described below.

### **Company Size**

Analysis of the extended insurance model policy options show that there is sufficient evidence to support the claim that company size is not a discriminating factor in insurance type. Failure to meet normality assumptions necessitated the use of non-parametric analysis. At  $\alpha = 0.05$ , the Kruskal-Wallis rank sums test failed to reject the null that the samples come from the same distribution with a p-value = 0.066. A comparison between each pair using the Wilcoxon method showed that at  $\alpha = 0.05$ , there is no statistical difference between no cost sharing policies and full cost sharing policies (p-value = 0.0769), nor partial cost sharing and full cost sharing (p-value = 0.3602). There is however, a statistical difference in company size between partial cost sharing with coinsurance and no cost sharing. The p-value = 0.0240. Figure 13 shows the data outputs from JMP statistical software. The limitations on sample size by NERC region preclude this area from being studied further within the scope of this research. There is data available within several of the NERC regions that could be studied at a future date to determine what factors drove the difference between non-cost sharing options and coinsurance only. This was not pursued because it was not deemed critical to the analysis of the industry as a whole, nor did it invalidate the model.



| Wilcoxon / Kruskal-Wallis Tests (Rank Sums) |       |           |          |            |            |                   |
|---------------------------------------------|-------|-----------|----------|------------|------------|-------------------|
| Level                                       | Count | Score Sum | Expected |            | Score Mean | (Mean-Mean0)/Std0 |
|                                             |       |           | Score    | Score Mean |            |                   |
| 0                                           | 50    | 5085.00   | 6025.00  | 101.700    |            | -2.151            |
| 1                                           | 68    | 8942.00   | 8194.00  | 131.500    |            | 1.542             |
| 3                                           | 122   | 14893.0   | 14701.0  | 122.074    |            | 0.356             |

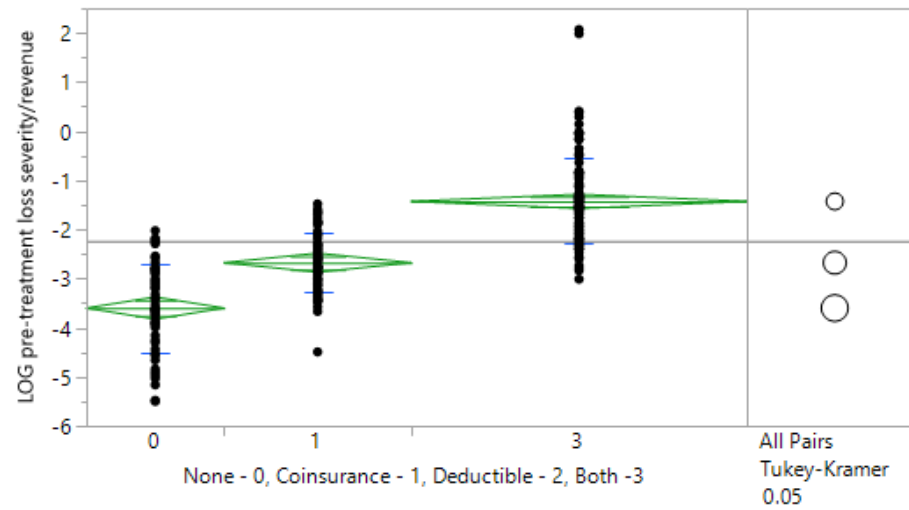
| 1-way Test, ChiSquare Approximation |    |            |
|-------------------------------------|----|------------|
| ChiSquare                           | DF | Prob>ChiSq |
| 5.4361                              | 2  | 0.0660     |

| Nonparametric Comparisons For Each Pair Using Wilcoxon Method |         |                       |             |          |         |                |          |          |
|---------------------------------------------------------------|---------|-----------------------|-------------|----------|---------|----------------|----------|----------|
| q*                                                            |         | Alpha                 |             |          |         |                |          |          |
| 1.95996                                                       |         | 0.05                  |             |          |         |                |          |          |
| Level                                                         | - Level | Score Mean Difference | Std Err Dif | Z        | p-Value | Hodges-Lehmann | Lower CL | Upper CL |
| 3                                                             | 0       | 14.7892               | 8.361726    | 1.76868  | 0.0769  | 15458.8        | -2451.3  | 34247.50 |
| 1                                                             | 0       | 14.3856               | 6.372728    | 2.25737  | 0.0240* | 26905.9        | 3390.0   | 60810.50 |
| 3                                                             | 1       | -7.6151               | 8.322337    | -0.91502 | 0.3602  | -10043.2       | -34734.0 | 10441.00 |

**Figure 13. Revenue comparison between recommended insurance policy options.**

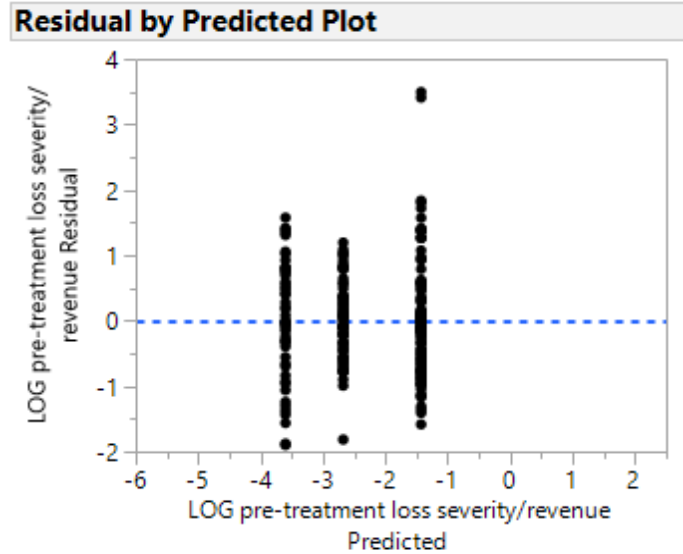
### Pre-Treatment Loss Severity as a Percentage of Revenue

Using ANOVA analysis, pre-treatment loss severity is statistically significant at  $\alpha = 0.05$  across insurance policy types with a p-value  $< 0.0001$ . The All Pairs Tukey-Kramer HSD test also shows that at  $\alpha = 0.05$ , the pre-treatment severity is statistically different, all with p-values  $< 0.0001$ . Figure 14 shows the ANOVA analysis and Figure 15 shows the residual plot along with Tukey-Kramer HSD test and connecting letters report.



| Analysis of Variance                               |     |                |             |          |          |
|----------------------------------------------------|-----|----------------|-------------|----------|----------|
| Source                                             | DF  | Sum of Squares | Mean Square | F Ratio  | Prob > F |
| None - 0, Coinsurance - 1, Deductible - 2, Both -3 | 2   | 185.81450      | 92.9073     | 141.7372 | <.0001*  |
| Error                                              | 237 | 155.35103      | 0.6555      |          |          |
| C. Total                                           | 239 | 341.16553      |             |          |          |

**Figure 14. ANOVA analysis of pre-treatment severity by insurance policy options.**



### Connecting Letters Report

| Level |   | Mean      |
|-------|---|-----------|
| 3     | A | -1.427866 |
| 1     | B | -2.675945 |
| 0     | C | -3.599658 |

Levels not connected by same letter are significantly different.

### Ordered Differences Report

| Level | - Level | Difference | Std Err Dif | Lower CL | Upper CL | p-Value |
|-------|---------|------------|-------------|----------|----------|---------|
| 3     | 0       | 2.171792   | 0.1359509   | 1.851139 | 2.492445 | <.0001* |
| 3     | 1       | 1.248079   | 0.1225252   | 0.959092 | 1.537066 | <.0001* |
| 1     | 0       | 0.923713   | 0.1508289   | 0.567969 | 1.279457 | <.0001* |

**Figure 15. Residual plot and Tukey-Kramer HSD comparison test of pre-treatment loss severity by insurance policy options.**

### Direct Security Investment as a Percentage of Revenue

As shown in Figure 11, the companies with the highest pre-treatment loss severity are recommended to use the most cost-sharing, they are also recommended to spend the most, as a percentage of their revenue, on direct self-security investment. Non-parametric analysis showed that the null must be rejected at  $\alpha = 0.05$  using the Kruskal-

Wallis test with a p-value  $< 0.0001$ . A comparison between no cost sharing and both deductible and coinsurance rejected the null that they were the same with a p-value  $< 0.0001$ . The policy options using partial cost sharing with coinsurance and both a deductible and coinsurance showed a p-value = 0.0008, and the comparison of a coinsurance only policy and no cost sharing policy generated a p-value = 0.0002, both of which reject the null that the groups are the same. All comparisons were analyzed at  $\alpha = 0.05$  level and JMP output is displayed in Figure 16.

| Wilcoxon / Kruskal-Wallis Tests (Rank Sums) |       |           |                |            |                   |
|---------------------------------------------|-------|-----------|----------------|------------|-------------------|
| Level                                       | Count | Score Sum | Expected Score | Score Mean | (Mean-Mean0)/Std0 |
| 0                                           | 50    | 3502.00   | 6025.00        | 70.040     | -5.775            |
| 1                                           | 68    | 7663.00   | 8194.00        | 112.691    | -1.095            |
| 3                                           | 122   | 17755.0   | 14701.0        | 145.533    | 5.679             |

| 1-way Test, ChiSquare Approximation |    |            |
|-------------------------------------|----|------------|
| ChiSquare                           | DF | Prob>ChiSq |
| 43.1343                             | 2  | <.0001*    |

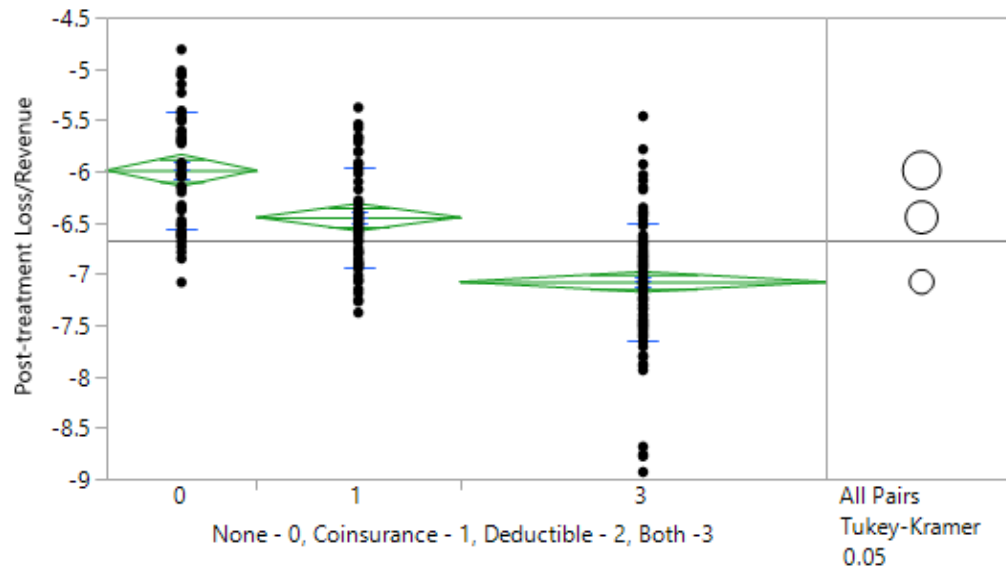
| Nonparametric Comparisons For Each Pair Using Wilcoxon Method |         |                       |             |          |         |                |           |           |                                                                                       |
|---------------------------------------------------------------|---------|-----------------------|-------------|----------|---------|----------------|-----------|-----------|---------------------------------------------------------------------------------------|
| q*                                                            |         | Alpha                 |             |          |         |                |           |           |                                                                                       |
| 1.95996                                                       |         | 0.05                  |             |          |         |                |           |           |                                                                                       |
| Level                                                         | - Level | Score Mean Difference | Std Err Dif | Z        | p-Value | Hodges-Lehmann | Lower CL  | Upper CL  |                                                                                       |
| 3                                                             | 0       | 51.55770              | 8.361726    | 6.165916 | <.0001* | 0.0042479      | 0.0031298 | 0.0054662 |  |
| 3                                                             | 1       | 28.04424              | 8.322337    | 3.369755 | 0.0008* | 0.0018975      | 0.0008084 | 0.0028834 |  |
| 1                                                             | 0       | 24.06853              | 6.372728    | 3.776801 | 0.0002* | 0.0024553      | 0.0012506 | 0.0035602 |  |

**Figure 16. Non-parametric analysis of recommended direct security investment as a percentage of revenue by insurance policy type.**

### Post-Treatment Losses as a Percentage of Revenue

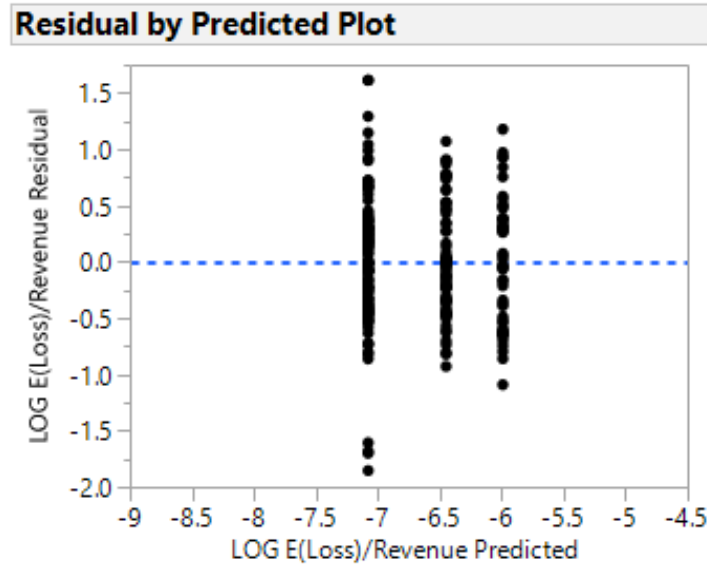
Figure 17 shows that post-treatment losses, as a percentage of revenue are significantly different by insurance policy option type at  $\alpha = 0.05$ , with a p-value  $< 0.0001$  using ANOVA analysis. Further testing using the Tukey-Kramer HSD test shows that the null hypothesis of equal expected loss percentages must be rejected at  $\alpha = 0.05$ ,

with p-values < 0.0001 in every comparison. The residual plots, statistical outputs, and connecting letters reported are detailed in Figure 18.



| Analysis of Variance                               |     |                |             |         |          |
|----------------------------------------------------|-----|----------------|-------------|---------|----------|
| Source                                             | DF  | Sum of Squares | Mean Square | F Ratio | Prob > F |
| None - 0, Coinsurance - 1, Deductible - 2, Both -3 | 2   | 46.68098       | 23.3405     | 76.4381 | <.0001*  |
| Error                                              | 237 | 72.36835       | 0.3054      |         |          |
| C. Total                                           | 239 | 119.04934      |             |         |          |

**Figure 17. ANOVA analysis of post-treatment losses as a percentage of revenue.**



### Connecting Letters Report

| Level |   | Mean      |
|-------|---|-----------|
| 0     | A | -5.990296 |
| 1     | B | -6.448392 |
| 3     | C | -7.077344 |

Levels not connected by same letter are significantly different.

### Ordered Differences Report

| Level | - Level | Difference | Std Err Dif | Lower CL  | Upper CL | p-Value |
|-------|---------|------------|-------------|-----------|----------|---------|
| 0     | 3       | 1.087048   | 0.0927896   | 0.8681947 | 1.305901 | <.0001* |
| 1     | 3       | 0.628951   | 0.0836262   | 0.4317109 | 0.826192 | <.0001* |
| 0     | 1       | 0.458096   | 0.1029442   | 0.2152928 | 0.700900 | <.0001* |

**Figure 18. Tukey-Kramer HSD comparison of post-treatment expected loss as a percentage of revenue by insurance policy type.**

### Extended Insurance Policy Options Model Summary

The results above show that model developed in this research used real data to recommend three different insurance policy options for companies. On the surface, the recommendations make sense and examination of the statistical significance of the

factors involved confirms that the model provided recommendations consistently, based on but not limited to: (i) pre-treatment loss severity, (ii) post-treatment loss severity as a percentage of revenue, and (iii) direct security investment as a percentage of revenue. The model did display significant differences between the sizes of companies in two of the three options, indicating that revenue was not a major factor in the recommendation.

The model also required that increased risk through cost sharing be associated with lower probabilities of loss by recommending that companies only engage in the highest levels of cost sharing using deductibles and coinsurance when the probability of a successful attack can be reduced to less than 1.1% or in terms of the loss/revenue ratio, less than 0.19% of the company's annual revenue. The probability of loss was not included as a statistically significant factor because it failed assumptions of normality and variance in both parametric and non-parametric analysis, respectively.

During this phase of the analysis, the second and third research questions posed in Chapter 1 were answered. The first question was designed to identify which factors contributed to insurance policy design. The statistically significant factors previously identified are good start to determining what influenced insurance policy recommendations. As cyber security threat and vulnerability assessments become more robust, the industry should gain more insight into specific policy option influencers that contribute to the factors identified in this framework. The third question exploring an optimal policy structure for the industry can be answered by examining the distribution of the companies assigned to each of the options. The recommendations, based on the variable characteristics identified above, reject the "one-size-fits-all" insurance design for

power companies within the industry. Each policy must cater to the needs of the insured and the insurer to reduce risk on both sides.

### **Post Treatment Industry Analysis**

Now that the extended model has been tested and confirmed to provide recommendations based on statistically significant criteria, the research turns to the effects on NERC regions and the entire industry. Beginning with an analysis of the individual NERC regions, ANOVA analysis showed that one region's expected losses are statistically different from the rest of the regions at  $\alpha = 0.05$ , with a p-value  $< 0.0001$ . The ANOVA output and Tukey-Kramer HSD test showing the pre-treatment and post-treatment conditions are presented in Figure 19. This however, does not shed any light on whether the industry as a whole has adopted a stronger security posture based on the recommendations made in this research. To do this, we examined the standard deviation of the losses in pre-treatment and post-treatment conditions.

Prior to launching this analysis however, it should be noted that no amount of security investment can eliminate the chance of a successful cyber attack. Investment can be made in an effort to reduce vulnerabilities, but as each security measure is developed, malicious actors find new means and methods of circumvention. This research does not propose that any framework can eliminate the cyber threat of any company, however, it is valuable in that it could contribute fewer vulnerabilities.

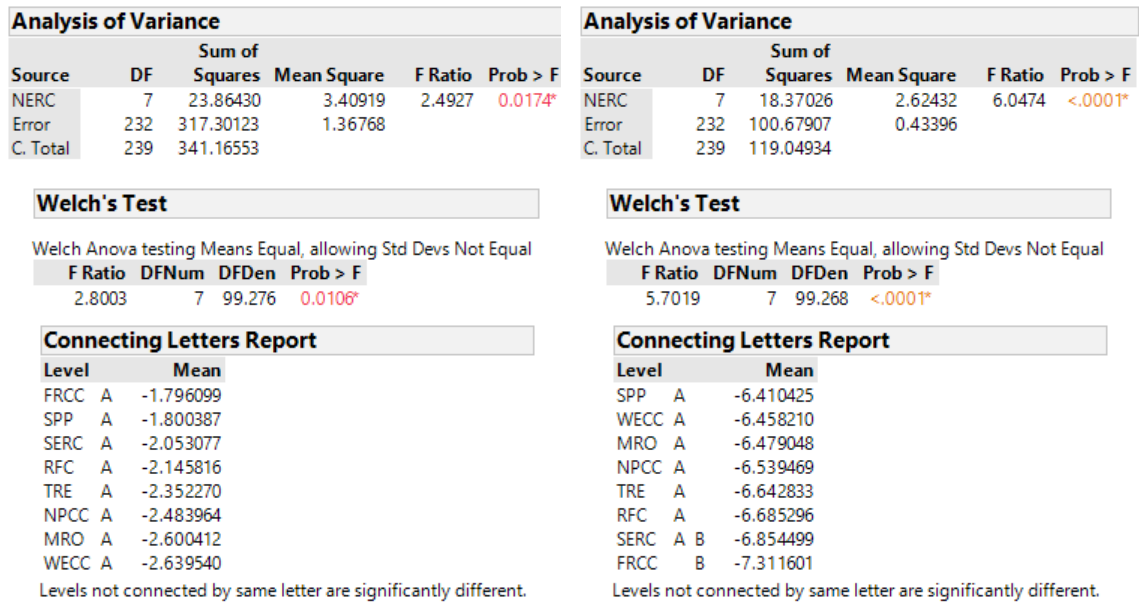


**Figure 19. ANOVA and Tukey-Kramer HSD test of pre (left) and post treatment (right) losses by region.**

Figure 20 shows the difference between the standard deviation of losses as a percentage of revenue within each NERC region in pre and post treatment conditions.

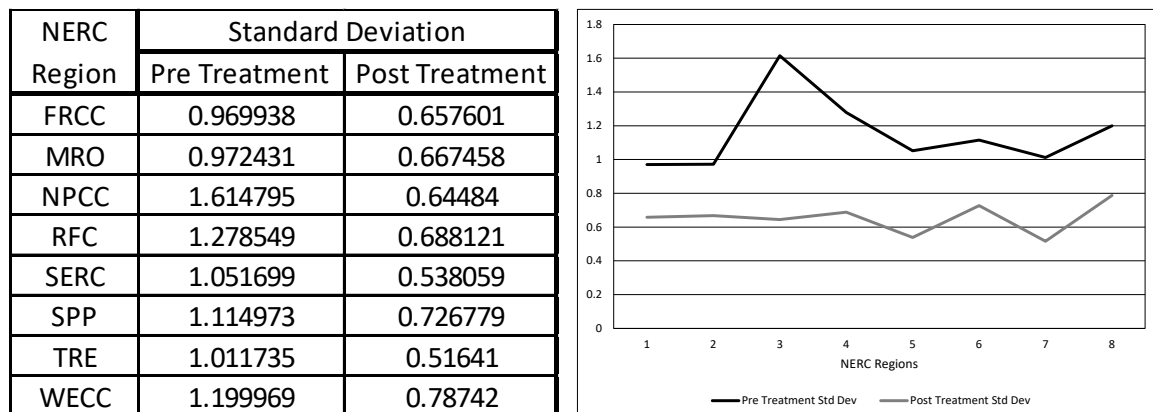


**Figure 20. Standard deviation of loss pre and post treatment.**

The two post-treatment differences in scale are clearly evident. Both ANOVA and non-parametric methods generated the same results—the ranges of standard deviation

in the post treatment state are smaller. Figure 21 shows the JMP ® depicting the standard deviations.

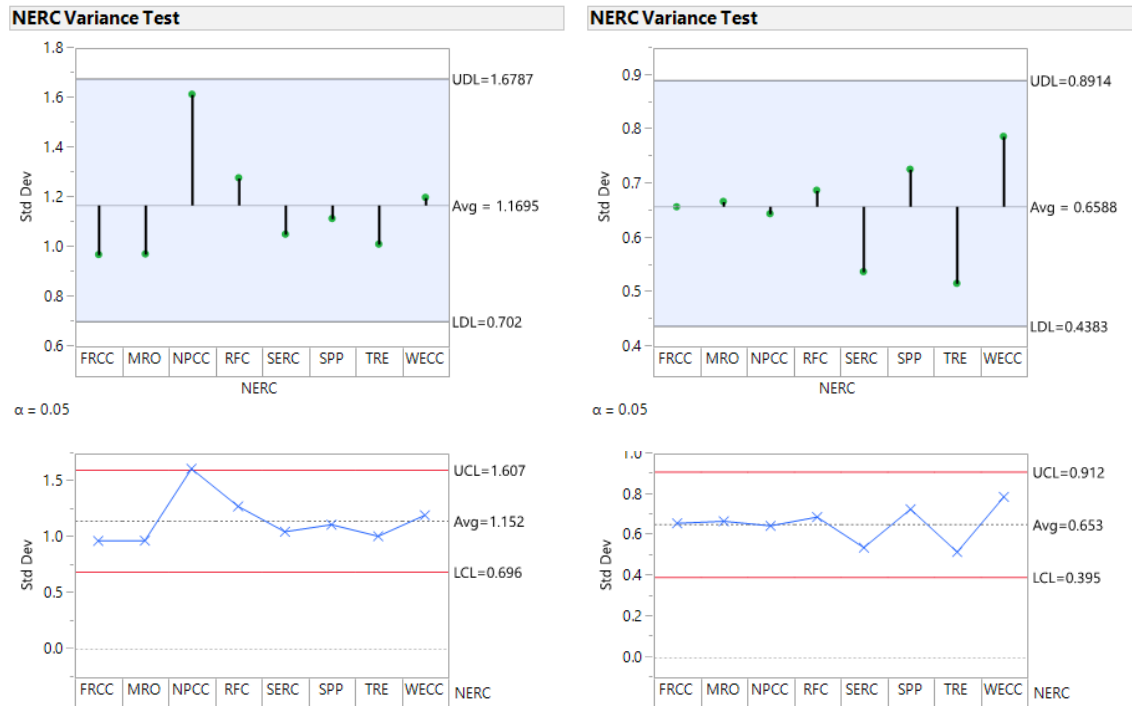


**Figure 21. Variance comparisons, pre-treatment loss (left) and post-treatment loss (right)**

The standard deviations of loss by NERC region were separated into pre-treatment and post-treatment categories and examined using ANOVA. Log transformation was used to help the data meet the normality assumptions. It was found that two outlier data points prevented the log transformed data set from being normal, as detailed in the Normal Quantile Plot and distribution in Figure 22. Removal of these outliers did allow the data to meet the normality assumption, but did not change the

results. For these reasons, the research moved forward using ANOVA, as detailed in Figure 23.

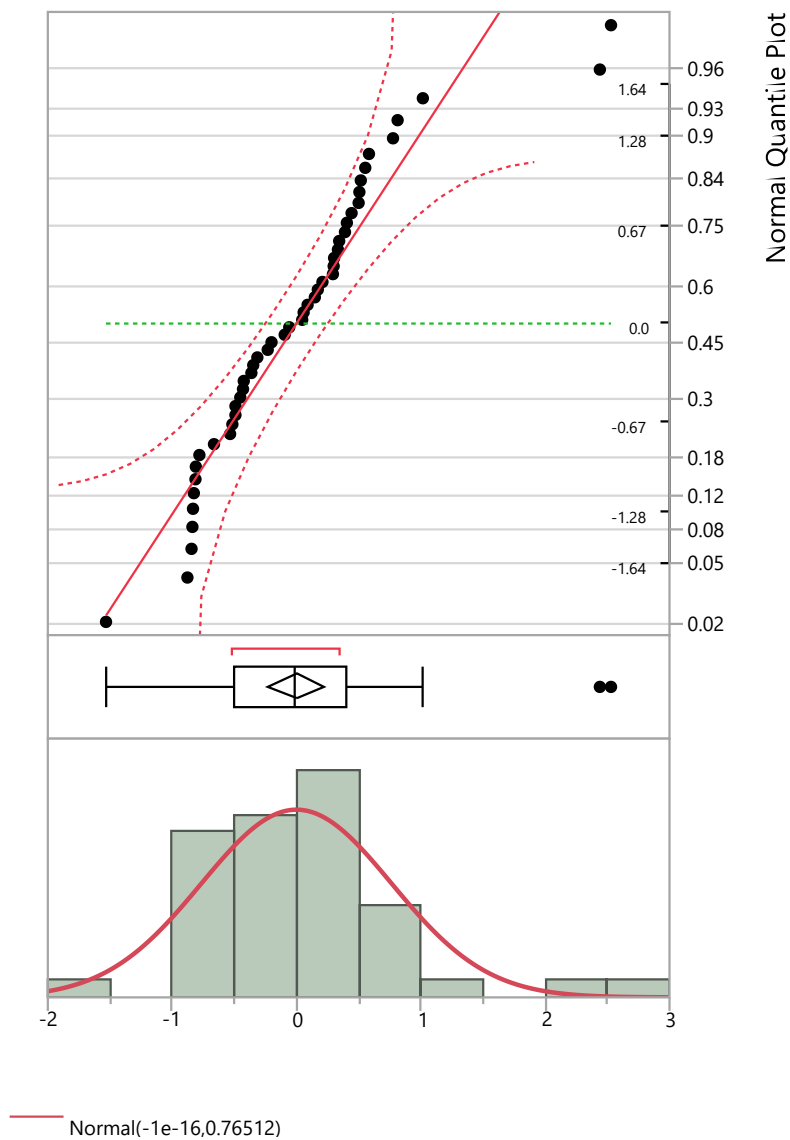
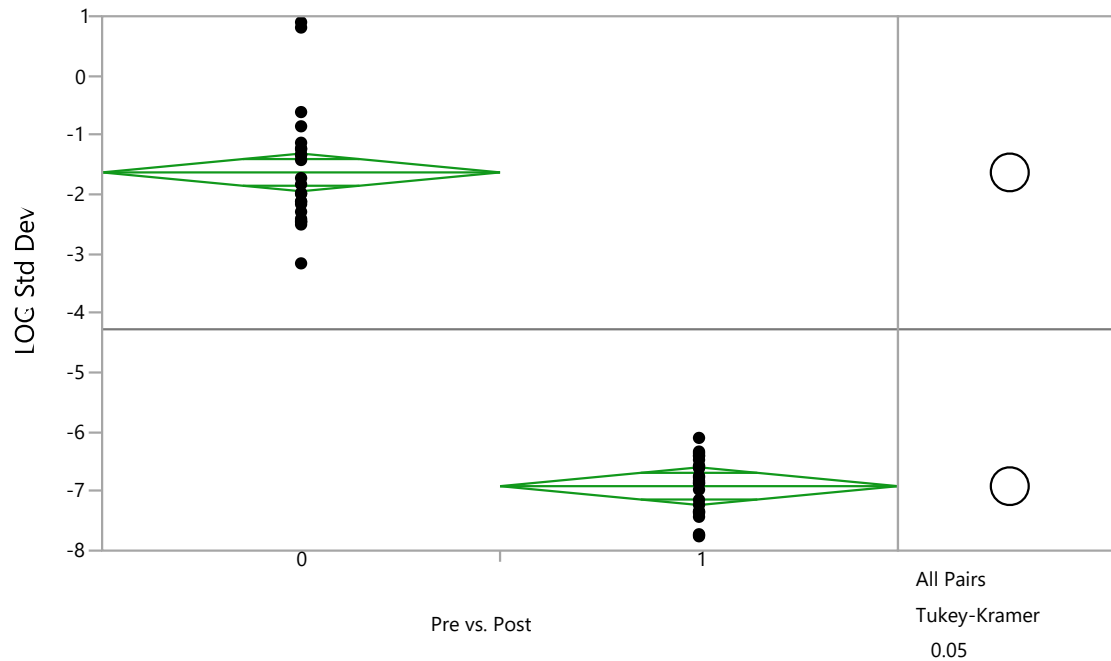


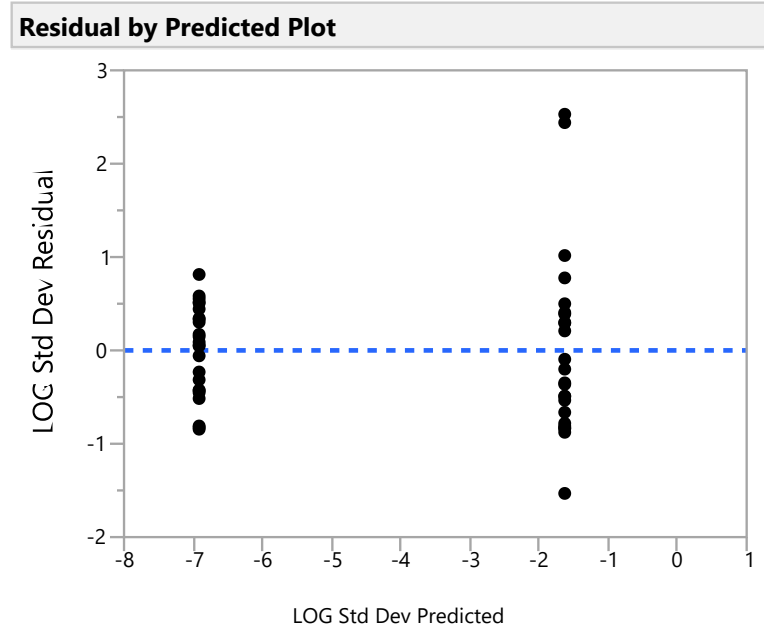
**Figure 22. Log transformed residuals of standard deviation of losses.**



| Analysis of Variance |    |                |             |          |          |
|----------------------|----|----------------|-------------|----------|----------|
| Source               | DF | Sum of Squares | Mean Square | F Ratio  | Prob > F |
| Pre vs. Post         | 1  | 335.12960      | 335.130     | 560.2897 | <.0001 * |
| Error                | 46 | 27.51427       | 0.598       |          |          |
| C. Total             | 47 | 362.64387      |             |          |          |

**Figure 23. ANOVA analysis of log transformed standard deviation in pre and post treatment categories.**

The variance assumption also presented some issues by narrowly failing the Levene test, but passing the Browne-Forsythe testing using medians, as detailed in Figure 24. Examination of the residual plot does not cause major concern with homoscedasticity as the variances look relatively similar, allowing continued use of ANOVA. At  $\alpha = 0.05$ , comparison of the pre-treatment and post-treatment conditions determined that the null that the means were the same must be rejected with a p-value  $< 0.0001$ .



| Test           | F Ratio | DFNum | DFDen | p-Value  |
|----------------|---------|-------|-------|----------|
| O'Brien[.5]    | 3.7621  | 1     | 46    | 0.0586   |
| Brown-Forsythe | 4.0469  | 1     | 46    | 0.0501   |
| Levene         | 5.7416  | 1     | 46    | 0.0207 * |
| Bartlett       | 10.2011 | 1     | .     | 0.0014 * |
| F Test 2-sided | 4.0460  | 23    | 23    | 0.0014 * |

**Figure 24. Residual plot and variance tests of standard deviation in pre and post treatment categories.**

Due to the outlier distortion of the normality and equal variance assumptions, further analysis comparing the standard deviations in pre-treatment and post-treatment conditions when separated by year was conducted. Examination of the normal quantile plots indicated that the residuals of each year's data was normally distributed. This was confirmed by the Wilks-Shapiro test, as detailed in Figure 25.

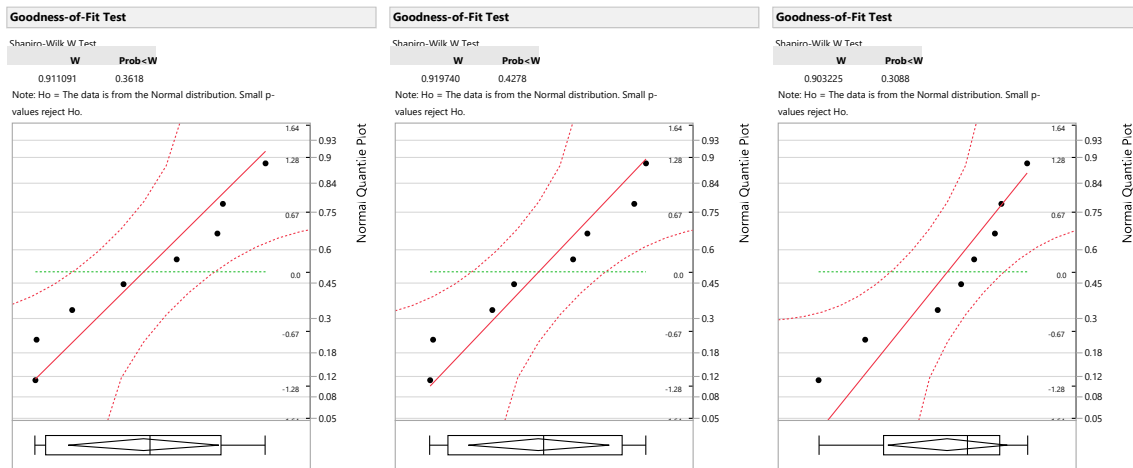
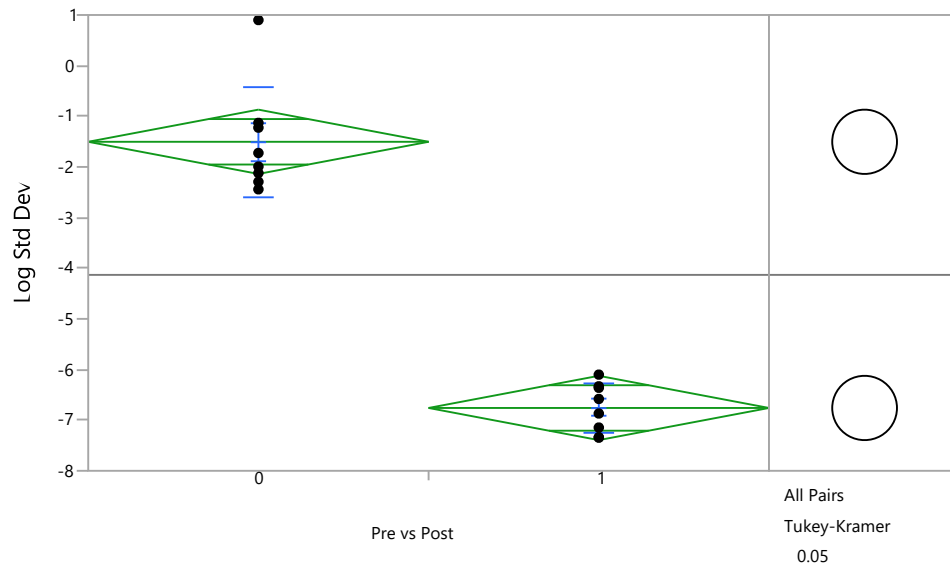


**Figure 25. Normality tests of standard deviation residuals. From left to right: 2013, 2014, and 2015.**

The subsequent ANOVA analysis and variance tests are captured in Figure 26, Figure 27, and Figure 28, where at  $\alpha = 0.05$  the p-values  $< 0.0001$  for each year indicate that the null must be rejected that the standard deviations in pre and post treatment conditions are equal.

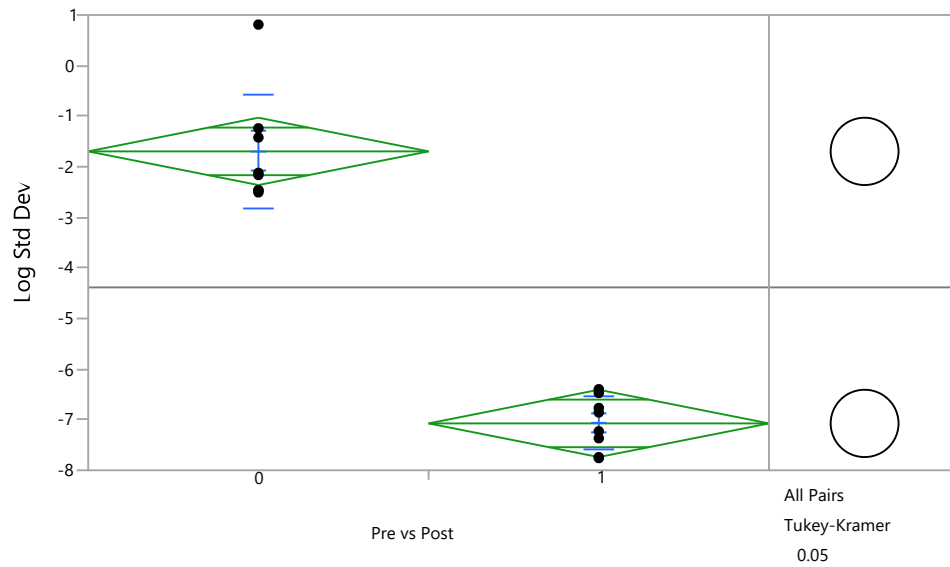


| Analysis of Variance |    |                |             |          |          |
|----------------------|----|----------------|-------------|----------|----------|
| Source               | DF | Sum of Squares | Mean Square | F Ratio  | Prob > F |
| Pre vs Post          | 1  | 110.48095      | 110.481     | 157.6196 | <.0001*  |
| Error                | 14 | 9.81308        | 0.701       |          |          |
| C. Total             | 15 | 120.29403      |             |          |          |

| Test           | F Ratio | DFNum | DFDen | p-Value |
|----------------|---------|-------|-------|---------|
| O'Brien[.5]    | 1.1930  | 1     | 14    | 0.2932  |
| Brown-Forsythe | 0.8874  | 1     | 14    | 0.3622  |
| Levene         | 1.8087  | 1     | 14    | 0.2000  |
| Bartlett       | 3.8083  | 1     | .     | 0.0510  |
| F Test 2-sided | 4.9634  | 7     | 7     | 0.0508  |

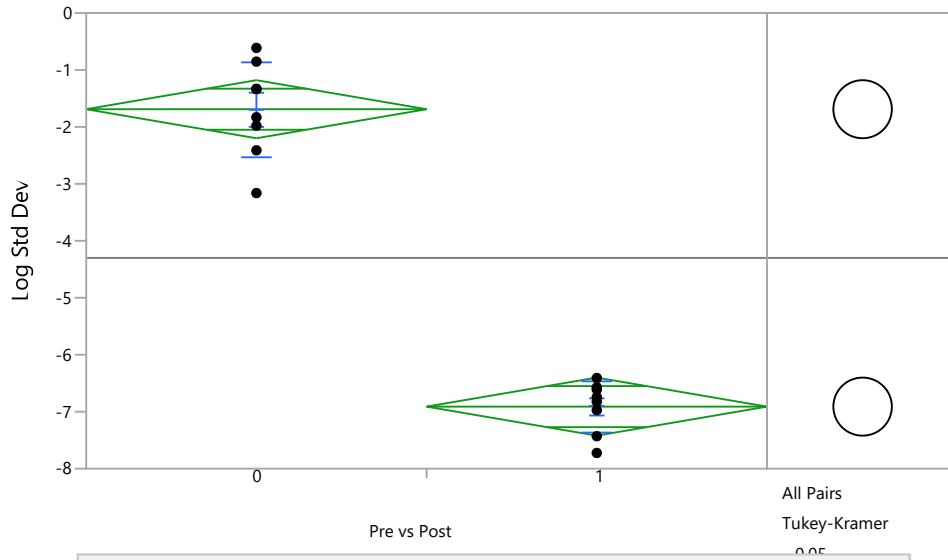
**Figure 26. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2013.**



| Analysis of Variance |    |                |             |          |          |
|----------------------|----|----------------|-------------|----------|----------|
| Source               | DF | Sum of Squares | Mean Square | F Ratio  | Prob > F |
| Pre vs Post          | 1  | 115.64836      | 115.648     | 150.0977 | <.0001*  |
| Error                | 14 | 10.78682       | 0.770       |          |          |
| C. Total             | 15 | 126.43518      |             |          |          |

| Test           | F Ratio | DFNum | DFDen | p-Value |
|----------------|---------|-------|-------|---------|
| O'Brien[.5]    | 1.1062  | 1     | 14    | 0.3107  |
| Brown-Forsythe | 0.5282  | 1     | 14    | 0.4793  |
| Levene         | 1.8444  | 1     | 14    | 0.1959  |
| Bartlett       | 3.3316  | 1     | .     | 0.0680  |
| F Test 2-sided | 4.4353  | 7     | 7     | 0.0678  |

**Figure 27. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2014.**



| Analysis of Variance |    |                |             |          |          |
|----------------------|----|----------------|-------------|----------|----------|
| Source               | DF | Sum of Squares | Mean Square | F Ratio  | Prob > F |
| Pre vs Post          | 1  | 109.05377      | 109.054     | 241.2789 | <.0001*  |
| Error                | 14 | 6.32775        | 0.452       |          |          |
| C. Total             | 15 | 115.38152      |             |          |          |

| Test           | F Ratio | DFNum | DFDen | p-Value |
|----------------|---------|-------|-------|---------|
| O'Brien[.5]    | 2.1533  | 1     | 14    | 0.1644  |
| Brown-Forsythe | 2.6888  | 1     | 14    | 0.1233  |
| Levene         | 2.7590  | 1     | 14    | 0.1189  |
| Bartlett       | 2.3421  | 1     | .     | 0.1259  |
| F Test 2-sided | 3.4334  | 7     | 7     | 0.1259  |

**Figure 28. ANOVA analysis, Tukey-Kramer HSD test, and Levene test of standard deviation in pre-treatment and post-treatment conditions sorted, 2015.**

Although there are concerns with the assumptions for normality and variance when comparing all standard deviations across all years, the year by year comparisons confirm that the standard deviations of losses in pre-treatment and post-treatment conditions are not equal. Speculation into why the year by year standard deviations fail normality and homoscedasticity assumptions could be attributed to some years

experiencing more interruptions than others due to super storms, polar vortexes, hurricanes, droughts, et cetera. These reasons may have contributed to normality and homoscedasticity issues between years. The fact that the assumptions are met when comparing the standard deviations within years supports this speculation.

### **Checking for Single Factors Disruption of Analysis**

To ensure that the reduced risk as measured by standard deviation of losses in pre-treatment and post-treatment conditions is uniform across all regions rather than just “cleaning up” one particularly bad region, we looked at a couple of factors (i.e. security spending by NERC region and the pre-treatment losses by NERC region).

Non-parametric analysis of recommended security spending by NERC region indicated that one region will spend a different amount on security, as a percentage of revenue, than some other regions, as detailed in Figure 29. But Figure 30 shows that Kruskal-Wallis test fails to reject the null that there is a statistical difference in amongst regions at  $\alpha = 0.05$ , calculating a p-value = 0.1636. Since pre-treatment losses as a percentage of revenues were not statistically different, as discussed above and displayed in Figure 5, and the recommended security spending as a percentage of revenue was not significantly different between regions, which indicated that no single region could have single handedly caused the enterprise wide reduction in the average standard deviation of losses. The model’s recommendations resulted in a uniform reduction in the average standard deviation of losses across the entire industry, which can be interpreted as an industry wide reduction in risk.

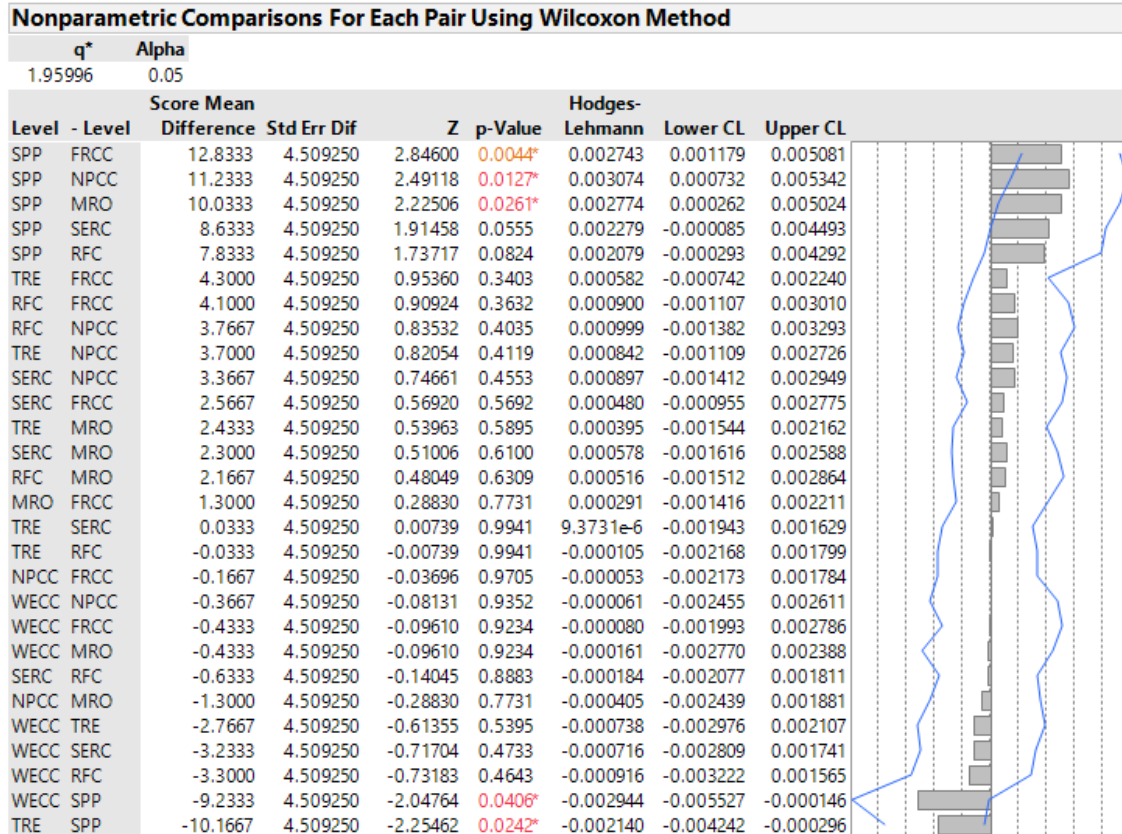


Figure 29. Recommended security budget as a percentage of revenue.

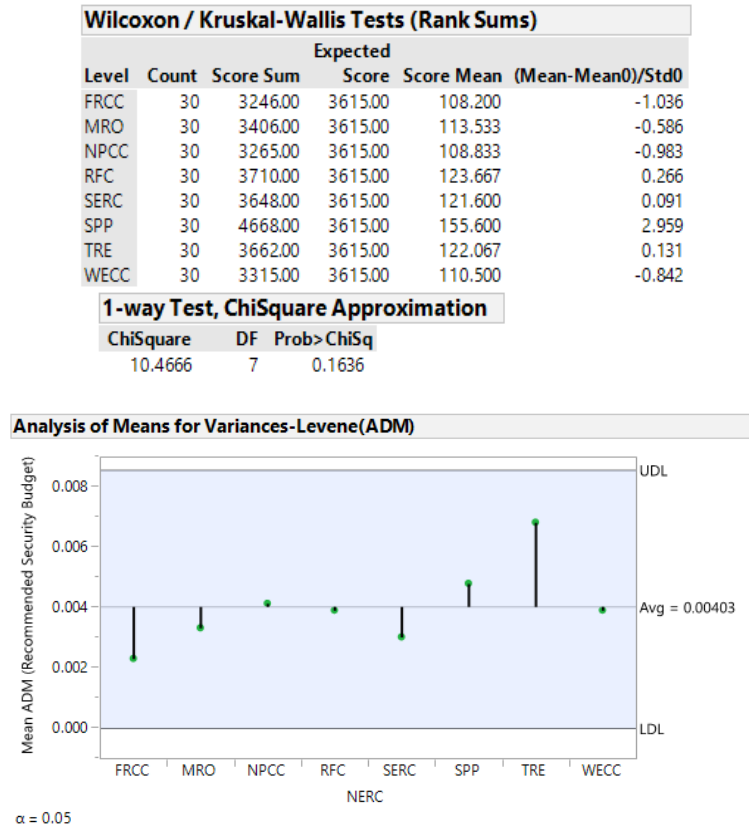


**Figure 30. Security spending as a percentage of revenue, post-treatment.**

## Summary

The uniformity among NERC regions in the pre-treatment scenario indicates that post-treatment results, effected each region with relatively the same magnitude. These results indicate that the extended insurance model successfully recommended different insurance policy options for companies based on the initial loss severity, as a percentage of revenue, investment levels as a percentage of revenue, post-treatment loss severity, and even considered diminishing returns of investment in security. When looking for industry wide risk reduction impact, the model demonstrated the ability to reduce the risk across the enterprise by narrowing the range of standard deviation of the expected losses

from pre-treatment to post-treatment scenarios. The impact of these findings will be discussed in the next chapter.

## **V. Conclusions and Recommendations**

### **Chapter Overview**

This chapter will discuss the implications of the results and analysis from the previous chapter, provide answers to the research questions not discussed within first four chapters, and determine whether the stated hypothesis should be accepted or rejected. It will also cover limitations of the study and avenues for future research.

### **Conclusions of Research**

This research has proven that extending Young et al.'s framework with the inclusion of the economic elements of coinsurance and a deductible will result in increased security investment. The recommendations based on statistically significant criteria, if implemented across industry, will result in a reduction in risk enterprise wide. Given the efficacy of the model, this research can provide value in a variety of applications:

- 1) Recommend cyber security budgets.
- 2) Recommend an allocation strategy for a cyber security budget.
- 3) Use the economic elements to create trade-space in the presence of constrained budgets.

The fourth and fifth research questions posed in Chapter 1 can now be answered. A key attribute of this framework is that each of the elements within the model are assessable and measurable. Insurers can use this framework and its elements to develop

insurance designs that meet the needs of the insured. In a constrained environment, cost sharing mechanisms create trade-space for a company that can provide the capability to remain under budget by reducing the initial obligation from the insured. These discounts can be reinvested back into additional security investment, further reducing premiums and ideally reducing the probability of a successful attack. In this case, the insurer will have reduced its losses and potentially increased its net gain by discounting premiums. From the perspective of the insured, the reduction in premiums will make the investment in risk transfer more appealing and would result in risk reduction if investment were a condition of entering into the insurance contract in the first place.

This framework provides a path forward for incentivizing cyber security investment using insurance. Its widespread adoption will lead to a more secure power industry. The interdependence of network systems dictates that all parties play a role in ensuring the safety of the group. Industry-wide cyber insurance that incentivizes investment will reduce risk by achieving greater participation in the market. This will contribute to security through increased data collection and information sharing. Insurers will have influence over their customers, but the insurers may begin to participate in the programs such as the aforementioned government information-sharing program sponsored by the DHS. They will continue to use their newfound plethora of data to further reduce their own risk.

## **Limitations**

There are two primary limitations associated with this research: (i) the method in which deductibles were implemented within this model; and (ii) the variables associated with the framework.

The results used by the modeling indicated that in no circumstances would a deductible only insurance policy be optimal. This outcome is not erroneous based on how the model was structured, however, in practice, deductibles may be offered in a way that would make them more prevalent in the field. This model was built with deductibles considered as a percentage of the coverage sought in the policy. The rationale behind this was that setting a flat-rate deductible as a baseline would create issues within the model due to the range of loss severity and company sizes analyzed. A flat rate deductible representing 10% of the losses sustained by the median company in the sample would have represented an 1800% deductible for a company seeking coverage at the 25% percentile. For this reason, a deductible as a percentage of loss severity was used, and since deductibles are paid out of pocket by the insured prior to receiving any reimbursement from the insurer, coinsurance will always serve as the optimal choice because in the event of any loss, the insured is guaranteed to receive some reimbursement from the insurer.

The variables associated with the model are an avenue for future research and a limitation for the accuracy of the model today. Current research shows that there are methods of quantifying vulnerabilities in systems. However, many of those capabilities are not available to those who do not have access directly to the system itself. The

attractiveness of this model is that users can determine these variables and then applied to this model to generate recommendations that are tailored to their specific situations.

These limitations are peculiar to the way that this model was run and can be overcome in future applications of this framework and future research.

## **Hypotheses**

Using the hypotheses outlined in Table 2 to validate the proposed research's model and analyze the impact of the extended framework on the industry yielded interesting results. H1's null was rejected for the alternative that the insurance policy options recommended by the extended model contained different characteristics in terms of coinsurance and deductible structure, and/or security investment. Rejection of this hypothesis proved that the model made recommendations based on specific criteria, in this case, the risk profiles of each company.

The second hypothesis, H2, analyzed whether the risk profiles of NERC regions were different from one another. Analysis of the risk facing the companies within each region, as measured by estimated loss severity divided by revenue, did not prove to be statistically significant. Therefore, H2 was not rejected and it was determined that the power industry had developed methods of combating risks associated with a particular geographic region, which had a normalizing effect across the industry.

The final hypothesis, H3, analyzed the differences in the risk profiles across NERC regions after the application of all data to the model. It was found that one region differed significantly from the others in risk. This difference indicated that the model

could distinguish the difference in risks faced by NERC region and could therefore be effective differentiating the risks between companies and regions in the power industry.

The hypotheses addressed in this research proved that the extended framework would be effective in segregating companies based on risk characteristics, such as pre-treatment and post-treatment loss severity, and direct security investment. The analysis of the industry in pre-treatment and post-treatment conditions confirmed that the model had the capability to recognize differences in the risk profiles facing each region across the industry.

### **Recommendations for Future Research**

Research must be conducted on cyber incidents occurring at power companies in the United States. More focused research into specific cyber incidents and the associated damage would provide more insight into the economics that drive this framework and make it more responsive to the needs of the market. There is also potential to identify areas that generate the most effective target of investment. In dissecting the variables in this model, companies could learn a great deal about what vulnerabilities they have and how to best utilize their resources.

This model is also applicable to other industries. Future research aimed at other critical infrastructures will provide valuable insight into that particular industry, but given the nature of OT networks, could also be shared across industry lines to develop more comprehensive threat and vulnerability information for use in the defense of all of our critical networks.

## Summary

This research is relevant because critical infrastructure companies are vulnerable. Aging operational technology is reliable, but much of it was not conceived in this century and lacks the security measures required to deal with worldwide interconnectivity. As processes become more efficient and remote monitoring and management more the norm, operational technology becomes more exposed. Cyber incidents are increasing in the United States and critical infrastructure is no exception. In order to bring security to the forefront of the critical infrastructure operator's priorities, there must be incentive. Insurance may provide the answer, as transferring risk is an attractive option, and if it can be used to incentivize risk reduction, then it is attractive to both the insured and insurer.

This research began by examining the fundamental theories behind risk management and insurance. Using these theories as a foundation, we searched mature insurance markets for evidence of behavior manipulation by insurance companies. The incentives built into insurance contracts today, whether negative or positive reinforcement, have a profound effect on our behavior. These incentives are transferrable across industries and can be adopted into cyber insurance. The extension of Young et al.'s framework using coinsurance and deductibles are not only grounded in insurance economics theory but they are practiced in the real world.

The model presented in this research provided recommendations using real data that discriminated companies by their performance and direct investment in cyber security. The results were statistically significant and can provide insight into what factors have an impact on cyber security budget formulation and allocation. The recommendations revealed that there is no cyber insurance policy that best meets the

needs of any given company. Each situation requires its own analysis. Cyber insurance companies, insured companies, and the population stand to benefit from increased security investment. By encouraging risk reduction, more consumers will be drawn to the market and the costs of doing business will continue to decrease, stabilizing the industry and helping to secure the future.

## Bibliography

- [1] D. Harp and B. Gregory-Brown, "The State of Security in Control Systems Today," Bethesda, MD, 2015.
- [2] O. Andreeva *et al.*, "INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS," Woburn, MA, 2016.
- [3] E. Nakashima and J. Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, 02-Jun-2012. [Online]. Available: [https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U\\_story.html](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html). [Accessed: 15-Jul-2016].
- [4] B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strateg. Insights*, vol. 10, no. 1, pp. 15–25, 2011.
- [5] Office of Management and Budget, "Federal Information Security Modernization Act Report: 2015," Washington, DC, 2016.
- [6] Government Accountability Office, "Agencies Need to Correct Weaknesses and Fully Implement Security Programs Agencies Need to Correct Weaknesses and Fully Implement Security Programs Why GAO Did This Study What GAO Recommends," Washington, DC, 2015.
- [7] Department of Homeland Security, "NCCIC / ICS-CERT Year in Review FY15," 2015.
- [8] J. Vijayan, "Simulated attack points to vulnerable U.S. power infrastructure," *Computerworld*, 2007. [Online]. Available: <http://www.computerworld.com/article/2541225/security0/simulated-attack->

- points-to-vulnerable-u-s--power-infrastructure.html. [Accessed: 10-Jan-2017].
- [9] K. Zetter, “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever,” *WIRED*, 2015. [Online]. Available: <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>. [Accessed: 15-Jul-2016].
- [10] S. Bridges, “Emerging cyber risk, cyber attacks, and property damage: will insurance respond?,” *BusinessInsurance.com*, 2014. [Online]. Available: [http://conferences.businessinsurance.com/uploads/conference\\_admin/JLT\\_Cyber\\_Attacks\\_and\\_Property\\_Damage1.pdf](http://conferences.businessinsurance.com/uploads/conference_admin/JLT_Cyber_Attacks_and_Property_Damage1.pdf). [Accessed: 12-Jul-2016].
- [11] K. Zachman, “Risk in Historical Perspective: Concepts, Contexts, and Conjunctions,” in *Risk - A Multidisciplinary Introduction*, C. Klüppelberg, D. Straub, and I. M. Welpé, Eds. Springer International Publishing, 2014, pp. 1–34.
- [12] C. Everett, “Cyberwar and protecting critical national infrastructure,” *Comput. Fraud Secur.*, vol. 2015, no. 11, pp. 11–14, Nov. 2015.
- [13] Allianz, “Allianz Risk Barometer 2016,” 2016.
- [14] Trend Micro, “Report on Cybersecurity and Critical Infrastructure in the Americas,” Washington, DC, 2015.
- [15] “Emerging Threat: Dragonfly / Energetic Bear – APT Group | Symantec Connect Community.” [Online]. Available: <http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group>. [Accessed: 15-Jul-2016].
- [16] “Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT.” [Online]. Available: <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>. [Accessed:

18-Jul-2016].

- [17] P. Polityuk, "Ukraine investigates suspected cyber attack on Kiev power grid," *Reuters*, 2016. [Online]. Available: <http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF>. [Accessed: 17-Jan-2017].
- [18] R. P. Hartwig and C. Wilkinson, "Threat and opportunity," New York, 2015.
- [19] L. Berk, "PERSPECTIVES: Today's digital risks require broad cyber insurance coverage," *Business Insurance*, 2014. [Online]. Available: <http://www.businessinsurance.com/article/20140427/ISSUE0401/140429898/perspectives-today-s-digital-risks-require-broad-cyber-insurance>. [Accessed: 26-Jan-2017].
- [20] P. Neray, "Key Takeaways from the 2016 ICS Cyber Security Conference," *CyberX*, 2016. [Online]. Available: <https://cyberx-labs.com/en/blog/top-takeaways-2016-ics-cyber-security-conference/>. [Accessed: 26-Jan-2017].
- [21] M. Ward, "Energy firm cyber-defence is 'too weak', insurers say - BBC News," *BBC News*, 2014. [Online]. Available: <http://www.bbc.com/news/technology-26358042>. [Accessed: 26-Jan-2017].
- [22] J. Finkle, "U.S. utilities worry about cyber cover after Ukraine grid attack," *Reuters*, 2016. [Online]. Available: <http://www.reuters.com/article/us-cyber-insurance-utilities-idUSKCN0V628N>. [Accessed: 26-Jan-2017].
- [23] N. Choucri, S. Madnick, and P. Koepke, "Institutions for Cyber Security: International Responses and Data Sharing Initiatives," Cambridge, MA, 2016–10, 2016.
- [24] J. M. Nicholas and H. Steyn, *Project Management For Engineering, Business and*

*Technology*, 4th ed. New York, NY: Routledge, 2012.

- [25] U.S. Department of Energy, “Electricity subsector cybersecurity capability maturity model,” 2014.
- [26] D. L. Ungarelli, “Insurance and Prevention: Why and How?,” *Libr. Trends*, vol. 33, no. 1, pp. 57–67, 1984.
- [27] H. Loubergé, “Developments in Risk and Insurance Economics : The Past 40 Years,” G. Dionne, Ed. Geneva, Switzerland: Springer Science, 2013, pp. 1–40.
- [28] S. A. Talesh, “Insurance and the Law,” *Int. Encycl. Soc. Behav. Sci.*, vol. 11, no. Forthcoming, 2015.
- [29] J. Kehne, “Hazardous Wastes Encouraging Safety Through Insurance- Based Incentives: Financial Responsibility for Hazardous Wastes,” *Yale Law J.*, vol. 96, no. 2, pp. 403–427, 1986.
- [30] O. Ben-Shahar and K. D. Logue, “Outsourcing Regulation: How Insurance Reduces Moral Hazard,” 593, 2012.
- [31] M. Rothschild and J. Stiglitz, “Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information,” in *Foundations of Insurance Economics*, G. Dionne and S. Harrington, Eds. Springer Netherlands, 1976, pp. 355–375.
- [32] D. Rowell and L. B. Connelly, “A History of the Term ‘Moral Hazard,’” *J. Risk Insur.*, vol. 79, no. 4, pp. 1051–1075, 2012.
- [33] J. M. Marshall, “Moral Hazard,” *Am. Econ. Rev.*, vol. 66, no. 5, pp. 880–890, 1976.
- [34] R. A. Winter, “Moral Hazard and Insurance Contracts,” *Contrib. to Insur. Econ.*,

pp. 61–96, 1992.

- [35] K. J. Arrow, “Economic Welfare and the Allocation of Resources for Invention,” in *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton, NJ: Princeton University Press, 1962, pp. 609–626.
- [36] K. J. Arrow, “Uncertainty and the Welfare Economics of Medical Care,” *Am. Econ. Rev.*, vol. LIII, no. 5, pp. 941–973, 1963.
- [37] I. Ehrlich and G. Becker, “Market Insurance, Self-Insurance, and Self-Protection,” *J. Polit. Econ.*, vol. 80, no. 4, pp. 623–648, 1972.
- [38] H. Schlesinger and E. Venezian, “Insurance markets with loss-prevention activity: profits, market structure, and consumer welfare,” *RAND J. Econ.*, vol. 17, no. 2, pp. 227–238, 1986.
- [39] P. R. Kleindorfer and H. Kunreuther, “The Complementary Roles of Mitigation and Insurance in Managing Catastrophic Risks,” *Risk Anal.*, vol. 19, no. 4, pp. 727–738, 1999.
- [40] C. Dijksterhuis, B. Lewis-Evans, B. Jelijs, D. De Waard, K. Brookhuis, and O. Tucha, “The impact of immediate or delayed feedback on driving behaviour in a simulated Pay-As-You-Drive system,” *Accid. Anal. Prev.*, vol. 75, pp. 93–104, 2015.
- [41] T. Vukina and D. Nestić, “Do people drive safer when accidents are more expensive: Testing for moral hazard in experience rating schemes,” *Transp. Res. Part A Policy Pract.*, vol. 71, pp. 46–58, 2015.
- [42] J. L. Wang, C.-F. Chung, and L. Y. Tzeng, “An Empirical Analysis of the Effects of Increasing Deductibles on Moral Hazard,” *J. Risk Insur.*, vol. 75, no. 3, pp.

551–566, 2008.

- [43] G. Dionne, P.-C. Michaud, and M. Dahchour, “SEPARATING MORAL HAZARD FROM ADVERSE SELECTION AND LEARNING IN AUTOMOBILE INSURANCE: LONGITUDINAL EVIDENCE FROM FRANCE,” *J. Eur. Econ. Assoc.*, vol. 11, no. 4, pp. 897–917, Aug. 2013.
- [44] M. Dementyeva and E. T. Verhoef, “Miles, speed, and technology: Traffic safety under oligopolistic insurance,” *Transp. Res. Part B Methodol.*, vol. 86, pp. 147–162, 2016.
- [45] California Earthquake Authority, “Our History.” [Online]. Available: <http://www.earthquakeauthority.com/whoweare/Pages/history.aspx>. [Accessed: 10-Dec-2016].
- [46] California Earthquake Authority, “Annual Report To The Legislature And The California Insurance Commissioner On CEA Program Operations: Report for the Year 2015,” 2015.
- [47] Insurance Information Institute, “National Flood Insurance Program,” *Flood Insurance*, 2016. [Online]. Available: <http://www.iii.org/fact-statistic/flood-insurance>. [Accessed: 12-Dec-2016].
- [48] “National Flood Insurance Program Community Rating System,” *National Flood Insurance Program Community Rating System*, 2016. [Online]. Available: <https://www.fema.gov/national-flood-insurance-program-community-rating-system>. [Accessed: 16-Dec-2016].
- [49] “Can I get a discount on my flood insurance premium?,” *FloodSmart.gov*, 2016. [Online]. Available: <https://www.floodsmart.gov/floodsmart/pages/faqs/can-i-get->

a-discount-on-my-flood-insurance-premium.jsp. [Accessed: 16-Dec-2016].

- [50] M. J. Browne and R. E. Hoyt, “The Demand for Flood Insurance: Empirical Evidence,” *J. Risk Uncertain.*, vol. 20, no. 3, pp. 291–306, 2000.
- [51] P. Hudson, W. J. W. Botzen, L. Feyen, and J. C. J. H. Aerts, “Incentivising flood risk adaptation through risk based insurance premiums: Trade-offs between affordability and risk reduction,” *Ecol. Econ.*, vol. 125, pp. 1–13, 2016.
- [52] A. M. Fendrick, J. J. Martin, and A. E. Weiss, “Value-based insurance design: More health at any price,” *Health Serv. Res.*, vol. 47, no. 1 PART 2, pp. 404–413, 2012.
- [53] M. E. Chernew, A. M. Fendrick, and B. Kachniarz, “Value Based Insurance Design,” *Encycl. Heal. Econ.*, vol. 3, pp. 446–453, 2014.
- [54] M.-J. Sepúlveda, M. C. Roebuck, P. Fronstin, P. Vidales-Calderon, A. Parikh, and K. Rhee, “Elimination of the Out-of-Pocket Charge for Children’s Primary Care Visits: An Application of Value-Based Insurance Design,” *J. Pediatr.*, vol. 175, pp. 195–200, 2016.
- [55] D. D. Maeng, J. M. Pitcavage, S. R. Snyder, and D. E. Davis, “The Value of Value-Based Insurance Design: Savings from Eliminating Drug Co-Payments,” *Am. J. Manag. Care*, vol. 22, no. 2, pp. 116–121, 2016.
- [56] N. K. Choudhry *et al.*, “Five features of value-based insurance design plans were associated with higher rates of medication adherence,” *Health Aff.*, vol. 33, no. 3, pp. 493–501, 2014.
- [57] J. Lee, M. Maciejewski, S. Raju, W. Shrank, and N. K. Choudhry, “Value-Based Insurance Design: Quality Improvement But No Cost Savings,” *Health Aff.*, vol.

32, no. 7, pp. 1251–1257, 2013.

- [58] Advisen, “Information Security and Cyber Liability Risk Management,” 2015.
- [59] Chubb Corporation, “U.S. public companies’ perceptions of risk, and their risk mitigation strategies,” Warren, NJ, 2012.
- [60] Willis, “Cyber Disclosure Report,” 2013.
- [61] Willis, “Willis Fortune 1000 Cyber Disclosure Report,” 2011.
- [62] K. Kirkpatrick, “Cyber policies on the rise,” *Commun. ACM*, vol. 58, no. 10, pp. 21–23, Sep. 2015.
- [63] R. Lenihan, “Cyber insurance market to see rapid growth through 2022,” *Business Insurance*, 2016. [Online]. Available:  
<http://www.businessinsurance.com/article/20161207/NEWS06/912310865/Cyber-insurance-market-to-grow-says-Allied-Market-Research>. [Accessed: 17-Jan-2017].
- [64] A. Wells and S. Jones, “Growth in Cyber Coverage Expected as Underwriting Evolves,” *Insurance Journal*, 2016. [Online]. Available:  
<http://www.insurancejournal.com/magazines/features/2016/04/04/403439.htm>. [Accessed: 17-Jan-2017].
- [65] A. Hahn and M. Govindarasu, “Cyber Attack Exposure Evaluation Framework for the Smart Grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.
- [66] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA security in the light of Cyber-Warfare,” *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, Jun. 2012.
- [67] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, “A survey of cyber security management in industrial control systems,” *Int. J. Crit. Infrastruct.*

*Prot.*, vol. 9, pp. 52–80, Jun. 2015.

- [68] Z. Mohajerani *et al.*, “Cyber-related risk assessment and critical asset identification within the power grid,” in *IEEE PES T&D 2010*, 2010, pp. 1–4.
- [69] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, “CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures,” *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.
- [70] Cyber Incident Data and Analysis Working Group, “Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository,” 2015.
- [71] Cyber Incident Data and Analysis Working Group, “Enhancing Resilience through Cyber Incident Data Sharing and Analysis: The Value Proposition for a Cyber Incident Data Repository,” 2015.
- [72] Cyber Incident Data and Analysis Working Group, “Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository,” 2015.
- [73] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao, “Why IT managers don’t go for cyber-insurance products,” *Commun. ACM*, vol. 52, no. 11, p. 68, Nov. 2009.
- [74] J. Bolot and M. Lelarge, “Cyber Insurance as an Incentive for Internet Security,” in *Managing Information Risk and the Economics of Security*, M. Eric Johnson, Ed. Boston, MA: Springer US, 2009, pp. 269–290.
- [75] A. Marotta, F. Martinelli, and A. Yautsiukhin, “A Survey on Cyber-Insurance,” Pisa, Italy, 2015.
- [76] C. Biener, M. Eling, and J. H. Wirfs, “Insurability of Cyber Risk: An Empirical

- Analysis,” *Geneva Pap. Risk Insur. Issues Pract.*, vol. 40, no. 1, pp. 131–158, 2015.
- [77] H. Herath and T. Herath, “Copula-based actuarial model for pricing cyber-insurance policies,” *Insur. Mark. Co. ...*, 2011.
- [78] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan, “Cyber-risk decision models: To insure IT or not?,” *Decis. Support Syst.*, vol. 56, pp. 11–26, Dec. 2013.
- [79] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney, “A framework for incorporating insurance in critical infrastructure cyber risk strategies,” *Int. J. Crit. Infrastruct. Prot.*, Apr. 2016.
- [80] L. A. Gordon and M. P. Loeb, “The Economics Of Information Security Investment,” *Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.
- [81] K. H. Borch, A. Sandmo, and K. K. Aase, *Economics of Insurance*. Elsevier Science, 2014.
- [82] R. Robinson and J. McDaniel, “IEEE Guide for Electric Power Distribution Reliability Indices,” 2012.
- [83] U.S. Department of Energy, “Electric Emergency Incident and Disturbance Report - Form OE-417,” Washington, DC, 2012.
- [84] Intel Security and The Aspen Institute, “Critical Infrastructure Readiness Report: Holding the Line Against Cyberthreats,” Washington, DC and Santa Clara, CA, 2015.
- [85] M. J. Sullivan, M. Mercurio, J. Schellenberg, and S. & C. Freeman, “Estimated Value of Service Reliability for Electric Utility Customers in the United States,”

Berkeley, CA, 2015.

- [86] Electricity Data Experts, “Form EIA-861,” *Electric power sales, revenue, and energy efficiency Form EIA-861 detaile data files*, 2016. [Online]. Available: <https://www.eia.gov/electricity/data/eia861/>.
- [87] TechTarget, “How Company Size Relates to IT Spending,” *CIO Magazine*, 2016. [Online]. Available: <http://searchcio.techtarget.com/magazineContent/How-Company-Size-Relates-to-IT-Spending>. [Accessed: 02-Dec-2016].
- [88] Optimal Networks, “How (and How Much) are Organizations Spending on IT?,” 2016. [Online]. Available: <http://www.optimalnetworks.com/how-and-how-much-it-spending/>. [Accessed: 02-Dec-2016].
- [89] B. Filkins, “IT Security Spending Trends,” 2016.
- [90] U.S. Department of Energy, “About EIA - U.S. Energy Information Administration (EIA).” [Online]. Available: [http://www.eia.gov/about/mission\\_overview.php](http://www.eia.gov/about/mission_overview.php). [Accessed: 25-Jan-2017].
- [91] “Regional Entities.” [Online]. Available: <http://www.nerc.com/AboutNERC/keyplayers/Pages/Regional-Entities.aspx>. [Accessed: 25-Jan-2017].

## **Vita**

John Patrick Rosson was born in Baltimore, MD in March, 1986. He graduated from The Severn School in 2004. He earned his B.S. in Finance at St. John's University, New York, in 2008. He enlisted in the United States Air Force in March, 2010 as a Cyber Transport Airman. After three years of service at Keesler AFB, MS and Joint Base Elmendorf-Richardson, AK, his application to Officer Training School was accepted. The newly minted Lt. Rosson was assigned to Whiteman AFB, MO in May of 2013, where he served as a finance officer until his enrollment at the Air Force Institute of Technology in August, 2015.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                         |                                          |                                         | Form Approved<br>OMB No. 074-0188                                       |                                                                                                                                                     |
| <p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
| <b>1. REPORT DATE (DD-MM-YYYY)</b><br>23-03-2017                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                         | <b>2. REPORT TYPE</b><br>Master's Thesis |                                         | <b>3. DATES COVERED (From - To)</b><br>August 2015 - March 2017         |                                                                                                                                                     |
| <b>TITLE AND SUBTITLE</b><br>An Expanded Cyber Insurance Framework to Mitigate Cyber Induced Economic Losses of the U.S. Power Industry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |                                          |                                         | <b>5a. CONTRACT NUMBER</b>                                              |                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         | <b>5b. GRANT NUMBER</b>                                                 |                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         | <b>5c. PROGRAM ELEMENT NUMBER</b>                                       |                                                                                                                                                     |
| <b>6. AUTHOR(S)</b><br>Rosson, John P., 1st Lt, USAF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                         |                                          |                                         | <b>5d. PROJECT NUMBER</b><br>17G310                                     |                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         | <b>5e. TASK NUMBER</b>                                                  |                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         | <b>5f. WORK UNIT NUMBER</b>                                             |                                                                                                                                                     |
| <b>7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)</b><br>Air Force Institute of Technology<br>Graduate School of Engineering and Management (AFIT/EN)<br>2950 Hobson Way, Building 640<br>WPAFB OH 45433-8865                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                         |                                          |                                         | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b><br>AFIT-ENY-MS-17-M-219 |                                                                                                                                                     |
| <b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>Department of Homeland Security ICS-CERT<br>POC: Neil Hersh, DHS ICS-CERT Technical Lead<br>ATTN: NPPD/CSC/NCSD/US-CERT Mailstop: 0635<br>245 Murray Lane, SW, Bldg 410, Washington, DC 20528<br>Email: <a href="mailto:ics-cert@dhs.gov">ics-cert@dhs.gov</a> phone: 1-877-776-7585                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                         |                                          |                                         | <b>10. SPONSOR/MONITOR'S ACRONYM(S)</b><br>DHS ICS-CERT                 |                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                          |                                         | <b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>                           |                                                                                                                                                     |
| <b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b><br>DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
| <b>13. SUPPLEMENTARY NOTES</b><br>This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
| <b>14. ABSTRACT</b><br>Cyber incidents are increasing in the United States and critical infrastructure is no exception. Aging operational technology is reliable, but much of it was not conceived in this century and lacks the security measures required to deal with worldwide interconnectivity. In order to bring security to the forefront of the critical infrastructure operator's priorities, there must be incentive. Insurance may provide the answer, as transferring risk is an attractive option which can be used to incentivize risk reduction, making it more attractive to both the insured and insurer. The incentives built into insurance contracts today, whether negative or positive reinforcement, have a profound effect on our behavior. This research explores the foundations of insurance theory and adopts behavioral manipulation methods used by mature insurance industries into cyber insurance. This cyber security framework builds on established research to incentivize security investment via insurance contracts by including coinsurance and deductible options. The model is validated by applying power industry performance data from 2013 through 2015. The results show how the addition of coinsurance and deductibles can serve as risk reduction incentives that create trade space in constrained budgets and ultimately make the power industry more secure from a cyber perspective if adopted. |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
| <b>15. SUBJECT TERMS</b><br>Cyber Insurance, power industry, cyber security strategy, security framework                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         |                                          |                                         |                                                                         |                                                                                                                                                     |
| <b>16. SECURITY CLASSIFICATION OF:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                         |                                          | <b>17. LIMITATION OF ABSTRACT</b><br>UU | <b>18. NUMBER OF PAGES</b><br>107                                       | <b>19a. NAME OF RESPONSIBLE PERSON</b><br>LTC Mason Rice, AFIT/ENG                                                                                  |
| <b>a. REPORT</b><br>U                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>b. ABSTRACT</b><br>U | <b>c. THIS PAGE</b><br>U                 |                                         |                                                                         | <b>19b. TELEPHONE NUMBER (Include area code)</b><br>(937) 255-3636, ext 4620<br>Email: <a href="mailto:mason.rice@afit.edu">mason.rice@afit.edu</a> |

