Incentivizing Cyber Security Investment in the Power Sector Using An Extended Cyber Insurance Framework

By Jack Rosson, Mason Rice, Juan Lopez, and David Fass

Abstract

Collaboration between the DHS Cybersecurity and Infrastructure Security Agency (CISA) and public- sector partners has revealed that a dearth of cyber- incident data combined with the unpredictability of cyber attacks have contributed to a shortfall in first-party cyber insurance protection in the critical infrastructure community. This research explores the foundations of insurance theory and adopts behavioral manipulation methods to incentivize cyber-security investment. We validate the model by applying power industry performance data from 2013-2015 to assess risk facing the industry. Results show that the model can successfully discriminate between individual power companies as well as geographic regions on the basis of risk and can recommend cyber risk- management strategies tailored to individual risk profiles. The adoption of this framework could invite more market participation, which will create a more robust cyber- incident reporting environment, contributing directly to the DHS goal of creating a national cyber- incident data repository.

Suggested Citation

Rosson, Jack; Rice,Mason; Lopez, Juan; and Fass, David. "Incentivizing Cyber Security Investment in the Power Sector Using An Extended Cyber Insurance Framework." *Homeland Security Affairs* 15, Article 2 (May 2019). https://www.hsaj.org/articles/15082.

Introduction

Cyber incidents have bridged the divide from data compromise to physical effects. The Stuxnet worm's physical destruction of Iranian centrifuges and the recent cyber induced Ukrainian power outages provide evidence that attitudes must transition from "what if?" to "when will cyber attacks result in physical damage in the power sector?" [1] The Department of Homeland Security's (DHS) most recent fiscal year's Strategic Plan emphasizes this shift in focus by highlighting cyber security of critical infrastructure as a top priority of their cyber mission.[2] The power industry's viability, as the foundation of all other critical infrastructure's functional capability, is crucial to the national security and well-being of the United States. However, the ownership of the power enterprise remains largely private, presenting regulatory and practical challenges in implementing effective security measures across the industry.[3]

To date, the primary concern of critical infrastructure (CI) operators is to ensure system availability and reliability, while the security of their control systems is considered a secondary objective.[4] The conflict between availability and security is understandable, given that security often complicates operations. However, as more control systems are retrofitted for remote management or internetworked with enterprise business systems, they become exposed and vulnerable to cyber threats not foreseen when initially developed.[5] Convincing CI asset owners to further strain budgets by investing in security that may or may not prevent damage is a hard sell. It is difficult to balance availability and reliability with security, and this, combined with the burgeoning costs of cyber risk management, presents a hurdle for effective cyber-security implementation in industrial control system dominated sectors, especially the power sector.

Cyber insurance is beginning to garner attention as a first-party risk management method in the critical infrastructure community. However, the insurance industry is not yet mature enough to provide cost-effective risk-transfer mechanisms to critical infrastructure owners.[6] Collaboration between the DHS Cybersecurity and Infrastructure Security Agency (CISA) (formerly the National Protection and Programs Directorate), and public partners has revealed that data concerns and the unpredictability of cyber attacks contribute to the lack of robust policy options for critical infrastructure in today's market. To combat these concerns, CISA working sessions have developed three vectors to encourage more participation by insurers in the cyber- insurance arena: (1) better information sharing, (2) cyber- incident analysis, and (3) enterprise risk management (ERM).[7] The establishment of the Cyber Incident Data and Analysis Working Group (CIDAWG) has led to more working sessions between stakeholders in the insurance, cyber security, and critical infrastructure communities which have laid the groundwork for data sharing, analysis, and risk management.[8] However, while there is progress, the Government Accountability Office (GAO) reports that the lack of an overarching data-reporting structure continues to limit the effectiveness of vulnerability reporting, which remains a contributing factor to the lack of maturity in the cyber-insurance market.[9]

Practical Implications

This research proposes an extended insurance framework to assess the cyber- risk profiles of the U.S. power enterprise. The framework considers industry-provided reliability indicators, estimated loss ratios, and various insurance features to recommend an optimal insurance package that minimizes risk to both the insurance offeror and insured party. Minimizing risk through the adoption of this framework should result in a more robust cyber- insurance marketplace for critical infrastructure companies and should lead to a stronger cyber-security posture for the entire power enterprise. As the marketplace grows, insurers will begin to assume the role of a de facto regulatory authority—power companies seeking to offset risk via insurance may need to meet baseline security requirements set forth by insurers to be eligible for coverage. Furthermore, this framework exemplifies how coverage could be made more affordable by incentivizing cyber- security investment using policy structure as a tool. Finally, as competition for business increases, power companies should begin to see a growing variety of products in the market, paving the way for more coverage options and, ultimately, more participation.

Perhaps more importantly though, the adoption of the framework will contribute to CISA's working session vectors by creating a better data- sharing environment. This will further the ERM goal by providing the capability to perform comprehensive risk management for individual companies, which would also be scalable to the entire enterprise. Data collection and analysis by the insurance providers presents possibilities for the development of security policy "best practices," likely executed via minimum baselines for coverage, or through continuous improvement of coverage options themselves. Not only would data analysis become prevalent for insurance providers and their customers, but this research can directly benefit CIDAWG's goal of establishing a cyber- incident data repository.[10] There is great potential for the aggregation and analysis of cyber-incident data across the cyber-insurance industry, allowing for detection of patterns, identification of high-risk areas, and maybe even active elimination of threats, leading to a better security posture at the enterprise level.

In accomplishing this, the framework furthers three DHS cyber-mission sub-goals: (1) strengthening security and resilience of CI, (2) advancing incident response and reporting capabilities, and (3) strengthening collaboration between government, law enforcement, private sector, and the public sector. [11]

Incentives Through Insurance

Early theoretical research in insurance economics led to the belief that self-protection could be encouraged by market insurance if the costs of insurance were inversely related to the quantity of self-protection. [12] Since then, the role of insurance has changed from a pure risk- transfer mechanism into a de facto regulatory authority. [13] The ability of the insurance industry to react quickly in a dynamic environment coupled with the desire to maximize profits naturally led to the manipulation of the insured's behavior by insurance companies through insurance contract structure. [14] Mature arms of the insurance industry—auto, earthquake, flood, and medical all feature negative and positive incentives aimed at reducing the probability that a loss event will occur. Insurance elements such as coinsurance and deductibles are applicable to cyber-insurance policies and are included in the extended cyber-insurance framework to incentivize power companies to engage in risk-reduction measures as a condition of the insurance contract offering.

Methodology

This research evaluates whether using the common insurance features of deductibles and coinsurance can incentivize self-investment in cyber security. In order to perform this evaluation, the authors extended a framework introduced by Young et al. for incorporating insurance into critical infrastructure risk strategies to include deductible and coinsurance options. [15] The research methodology consists of two stages: the first stage describes the approach used to incorporate the additional insurance components not addressed 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 self-reporting. Of particular interest is the impact of the model's effect on risks faced by a particular National Energy Reliability Corporation (NERC) region in the United States and the power industry as a whole.

Extended Cyber Insurance Framework

Young et al. proposed a quantitative cyber-insurance framework that integrated four distinct models: (1) threat likelihood and severity model, (2) reduction of threat likelihood model, which incorporated (3) Gordon and Loeb's class II security breach investment function, and (4) an insurance premium discount model. This research extended the Young et al. framework by incorporating the insurance components of coinsurance and deductibles not previously considered. Each of these models has been updated to fit the analyzed data used for this research as described below. Table 1 provides an overview of the variables used in the framework.

Table 1. Variables used in cyber insurance framework.

Variable	Definition
λ	Annual loss severity calculated using self-reported power industry data
t	Probability of an attempted breach
v	Vulnerability of the system
$\lambda v t$	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
α	Effectiveness of security investment

Operationalizing the Framework

To begin, we construct the wealth of a company in a loss scenario. Equation (1) represents this conceptualization, where the wealth in a loss event, W, was reduced by the sum of the insurance premium, P; security investment, z; the minimum of deductible, DExp or loss; coinsurance expenses, CExp; and unforeseen losses above the insurance coverage, ε. This equation will be the foundation of the optimization utilized in this research.

$$Wealth = W - (P + z + min[D_{Exp}, S(z,v)\lambda t] + C_{Exp} + \varepsilon)$$

Eq. 1. Wealth post loss event equation

Threat Likelihood Model

The threat-likelihood model uses an annual rate of occurrence and the expected probability of a successful cyber attack to derive the impact of a single event from the cost of annual losses. [16] Reliability data reported by the power industry was used to develop the annual loss severity, λ. When multiplied by vulnerability, v, and threat, t, the single loss expectancy (SLE) is derived for use as part of the measured risk ratio. The equation for SLE is provided in Equation (2).

$$SLE = \lambda * v * t$$

Eq. 2. Single loss expectancy equation

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, a given vulnerability represents weakness in the security posture of the operational technology (OT) network used at power companies. The function is concave which identifies an optimal point of investment, past which, the marginal costs outweigh the marginal benefits and the investor experiences diminishing returns. [17] The effectiveness of security controls used in this framework calculates the probability of a successful attack conditioned on security investment, S(z,v), based on an initial vulnerability, v, security investment effectiveness level, α, and amount of security investment, z. The effectiveness of security controls can be modeled as:

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

Eq.3. Gordon-Loeb Class II Security Investment Function

Insurance Premium Discount Model

The insurance premium discount model uses a base-rate premium and incorporates discounts based on the assumed value of assets; the rate of discount offered by insurance companies for security investment, r; the attained insurance discount, δ; the probability of a successful cyber attack after security investment, S(z,v); deductible discounts; and coinsurance discounts. [18] Table 2 illustrates the progression from the base-rate insurance premium to the final premium paid by the insured.

This research followed the Young et al. insurance premium discount model by using the initial loss severity to build out the insurance premiums. Moving forward, the extended insurance framework operates under the assumption that the insurance coverage purchased will be equal to the estimated annual loss severity. It is assumed that power companies will seek insurance up to the maximum loss that they expect to sustain in a given time period. The base rate insurance premium multiplier was estimated using 8% of asset value (in this case, calculated economic losses represented by loss severity). This is the same threshold used as the starting point for insurance premium prices in the early era of the commercial airline industry, which was gradually adjusted as the industry matured. [19] The similarity of maturity levels in each industry provided justification for using the early airline-insurance industry as a valid substitute.

Table 2. 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%
δ	Attained insurance discount	$\delta=r(1-S(zv))$
P	Total insurance premium	$P=P_0(1-\delta)$

Cost Sharing

The cost-sharing mechanisms of deductible and coinsurance generate premium discounts that provide the primary incentive element that differentiates this model from its predecessor. These elements position the insured to assume partial responsibility for incurred losses, increasing their risk while reducing the risk of the insurer. The result of the additional risk assumed by the insured is that they are not expected to pay as much for coverage, but are also incentivized to take additional actions to reduce losses in order to preserve their wealth.

In practice, deductibles are considered first when making a claim, where the insured will pay the minimum of the entirety of the deductible or loss amount prior to the insurer making any payments. Coinsurance is then calculated on the remaining claim and split between the insurer and insured as dictated by the policy. Table 2 shows the impact of cost sharing on the calculation of insurance premiums.

Security Rate of Discount

The insurance offeror establishes the security investment discount, r. Policy premium discounts, r%, are determined on the vulnerability reduction as a direct result of security investments. In this model, the security discount offered by an insurance company is assumed to be 50% of the reduction in losses.

Model Confirmation

To ensure that the proposed extension to the Young et al. base model functions correctly, the authors implement a scenario from their published work. We set the extended model's deductible and coinsurance coefficients to zero and repeated the scenario 35 times. We used the results to establish a 95% confidence interval (CI). The 95% CI fell entirely within the Young et al. published results. This provides sufficient evidence that the extended framework model is stable.

Baseline Conditions

We describe the baseline conditions for each company tested within the model and data collection methods in the following sections. First, we describe the rationale used to determine the baseline security posture of each company, and then we describe the data collection methodology.

Model Inputs

Threat

The 2015 Critical Infrastructure Readiness Report surveyed 556 public and private entities operating in the finance, energy, transport and government sectors across the United Kingdom, France, Germany, and the United States. According to this data, nine out of ten companies have sustained at least one cyber attack over the preceding 12 months. [20] This data helped to inform this research by allowing threat, t, to be estimated at 90%.

Vulnerability

We estimated Vulnerability, v, to be 44% based on published data in the 2015 Critical Infrastructure Readiness Report. The vulnerability figure is an average adjusted estimate using the following figures from the same 556 companies across the finance, energy, transport, and government sectors mentioned above: (1) 55% of the companies interviewed experienced physical damage during attacks and, (2) 33% of the companies experienced disruptions in their daily business cycles. [21]

Loss-Severity Calculation

The annual loss severity, λ, is the amount of coverage sought by the power company and is calculated using power outage reliability figures and customer data reported annually via form EIA-861 to the Energy Information Administration. [22] We used a web-based calculator, developed at the Berkeley National Lab under contract for the U.S. Department of Energy (DoE), to generate the annual loss severity estimate. [23] The web-based tool estimates the economic losses of outage events during the time period of the report based on: (1) average interruption duration (SAIDI), (2) average interruption frequency (SAIFI), (3) residential customer population, and (4) the non-residential (commercial and industrial) customer population served by the reporting power company. The Institute of Electrical and Electronics Engineers (IEEE) standardizes power interruptions as sustained interruptions lasting more than five minutes. [24] We also included the measurements of major event days (MED), which indicate days where the power grid is stressed more than normally expected, (e.g. external events that caused major disruptions to the system). We describe the duration and frequency of power interruption figures below. [25]

SAIDI Index: This index represents the average length of time the average customer experienced an interruption and is defined as:

$$SAIDI = \frac{Sum\ of\ sustained\ interruption\ durations\ for\ all\ customers}{Total\ number\ of\ customers\ served}$$

Eq. 4. SAIDI Index

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

$$SAIFI = \frac{Total\ number\ of\ sustained\ interruptions\ for\ all\ customers}{Total\ number\ of\ customers\ served}$$

Eq. 5. SAIFI Index

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

Productivity of Security Investment

We derived the productivity of security investment, α, by rearranging the Gordon-Loeb class II security breach investment function. We developed the security budget used in this calculation utilizing IT security budgets as a proxy for OT budgets. Private consulting firms recommend that between 3% - 7% of revenue should be used as an IT budget baseline.[26] The IT Security Spending Trends Survey by the SANS Institute suggests that companies typically spend between 7% - 9% of their IT budgets on IT security. [27] By multiplying the mid-ranges of IT budget and IT security budget, 0.05 by 0.08, the authors developed a baseline OT security budget of 0.4% of a given company's revenue. Using the revenue ranges found in Table 3 and the assumption that the expenditure of the entire estimated OT security budget on direct security investment would result in a 5% chance of a successful cyber attack, the authors calculated a baseline alpha for different size companies. We detail the security investment effectiveness results in Table 3.

Table 3. Calculated security investment effectiveness.

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

Data Collection

When referring to the power industry, this research includes any power company that is operated as a municipal, state, federal, investor owned, cooperative, political subdivision, or transmission entity. We excluded power marketing companies from the reported data, as they do not have power-generation capabilities.

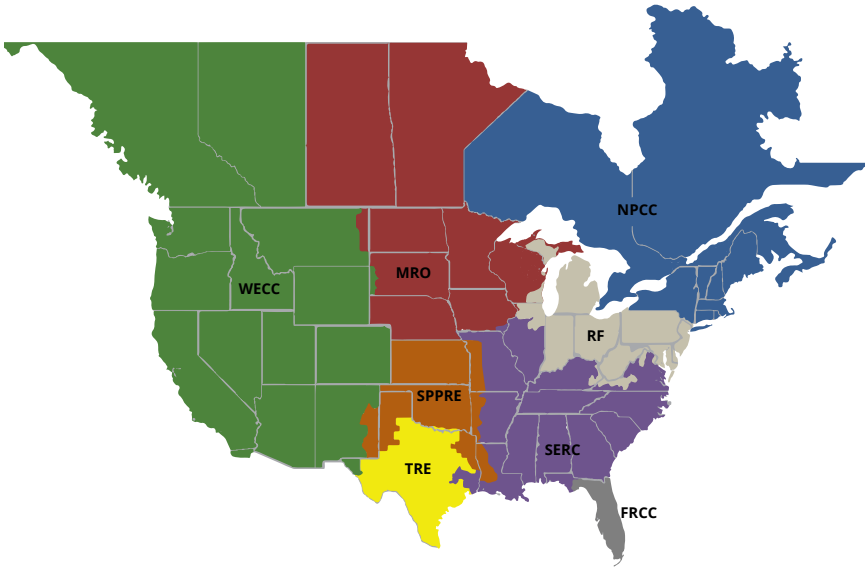

Figure 1. North American Electric Reliability Corporation regions.

Our sampling strategy was a stratified sample using North American Electric Reliability Corporation's (NERC) regions as a grouping factor. We used the NERC regions, shown in Figure 1, to allocate companies into eight groups. [28] All NERC regions will contain an equal sample, which is restricted by the smallest sample available in the EIA-861 self-reported data (see Table 4, 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. We drew samples from three consecutive years of available 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. We outline the stages of the parsing process in Table 4.

Table 4. 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	14	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

Optimization

The objective function minimized the amount by which the initial wealth would be reduced. The function also considered the expected loss despite theoretically being covered by the insurance policy. This inclusion was necessary to induce the model to consider the security posture of the company. We display the minimization in Equation (6).

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

Eq.6. Loss minimization objective function

Decision Variables

We used five decision variables in this optimization. Four of the variables concerned the inclusion of cost sharing and the amount of sharing recommended. The fifth decision variable was the amount of direct security investment recommended for the company. We outline each decision variable and its description in Table 5.

Table 5. Optimization decision variables.

Decision Variable	Description
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 serving as a multiplier for the deductible percentage, effectively including or excluding it from consideration.
Coinsurance Percentage (C)	The percentage of loss severity, after the deductible is paid, for which the insured is responsible.
Coinsurance Toggle	A binary on/off switch serving as a multiplier for the coinsurance percentage, effectively including or excluding it from consideration.
Direct Security Investment	The dollar amount of direct self-investment by the power company into cyber security.

Constraints

We detail the constraints of the optimization in Table 6. Three of the five constraints concern the cost-sharing toggles, where for the purposes of analysis, each of the elements could be included or excluded in the model based on user preference. The remaining constraints ensured that security investment was not greater than the initial loss severity or that the insurance and premiums combined were not more than the security budget, if operating under budget constraints.

Table 6. Optimization constraints.

Constraint	Explanation
$Z<\lambda$	If direct security investment is equal to or more than security, company should self-insure.
$P+z \leq$ 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.
Combined Toggle ≥ 0	The sum of the deductible and coinsurance toggles, this sum can also be set to $=0$, ≥ 1, or ≥ 2, depending on the preferences of the parties involved.
Deductible Toggle ≥ 0	This constraint can be adjusted to $=0$, or ≥ 1, depending on preferences for inclusion of a deductible in the model.
Coinsurance Toggle ≥ 0	This constraint can be adjusted to $=0$, or ≥ 1, depending on preferences for inclusion of coinsurance in the model.

Solver Settings

We used Frontline Systems, Inc. Analytic Solver Platform V2016-R2 as the optimization software to develop this framework and run all associated optimizations. We detail the settings in Table 7.

Table 7. Analytic Solver Platform settings.

Parameter Option	Variable
Algorithm	GRG nonlinear
Maximum Time	100 seconds
Iterations	1,000
Precision	$1x10^{-6}$
Convergence	0.0001
Multi-Start Search	Enabled
Require Bounds on Variables	Enabled
Estimates	Tangent
Derivatives	Forward
Search	Newton
Maximum Sub Problems	5,000
Maximum Feasible Solutions	5,000

Results

Initially, we used a pilot study to determine the best method of analysis. The dependent variables measured in this research were continuous and the independent variables—insurance type and NERC region—were nominal, allowing for the use of single-factor ANOVA for determining whether there were differences between groups. We performed post-hoc examination of the means using the Tukey-Kramer Honestly Significant Difference (HSD) test. Using quantile plots, visual aids of the sampling distributions, 2nd, 3rd, and 4th order moments, variance analysis via unequal variance tests, and residual scatterplot analysis, the authors determined that the dependent variables required a log-transformation in order to move forward with the analysis. In certain cases, where the data failed to meet the normality assumption, we performed non-parametric analysis using the Kruskal-Wallis test and post-hoc analysis using the Wilcoxon Each Pair test. We describe the method of testing significance and results below.

Insurance Policy Option Analysis

We analyzed the risk profiles of companies using a normalized loss-severity metric. In pre-treatment, we measured the annualized loss severity as a percentage of the company's annual revenue. In post-treatment conditions, we assessed the expected losses after security investment as a percentage of revenue, where a lower ratio indicated that the company

faced less risk. Using this ratio of losses to revenue ensured that different size companies could be compared.

Pre-Treatment Risk Profile of the Electric Industry

We measured the risk profile of the electric industry by comparing the means of the risks faced by companies within each NERC region prior to being treated by the model. The ANOVA results indicated that there were slight differences within the industry at $\alpha = 0.05$, with a p-value = 0.0174. However, the post- hoc Tukey-Kramer test failed to reject the null that any single region was distinct from another, indicating that there may be some variation in the industry, but not enough in any single region to make it statistically unique.

Risk Assessment of Individual Power Companies

Applying the data to the model returned results indicating that this framework has the capability to discriminate between companies using their risk profiles. The model separated the 240 data points into three insurance policy options: (1) no cost sharing, (2) partial cost sharing using coinsurance, and (3) maximum available cost sharing using deductibles and coinsurance. We excluded a deductible-only policy as an option due to the construction of the model. Deductibles as a percentage of loss will always be more expensive than coinsurance of the same percentage, up to the policy limit. Each cost-sharing element will also generate the same premium discount when used individually. For this reason, the coinsurance option was always a better value in this research. This model can be altered to reflect a flat-rate deductible, but due to the range of company sizes analyzed, a single flat-rate deductible was not viable here.

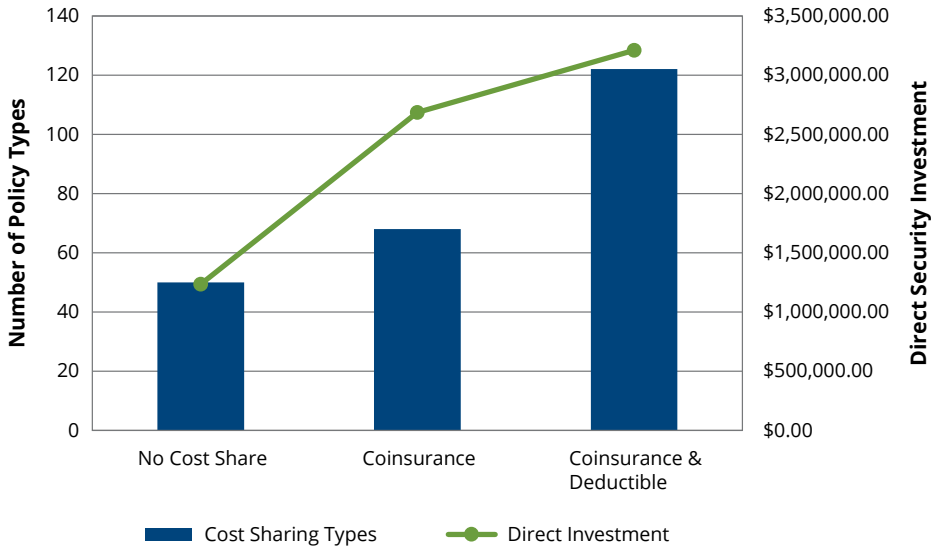

Figure 2. Insurance policy type and average direct security investment recommendation.

Figure 2 depicts the distribution of policy options, where 50 companies should not participate in any additional cost sharing, 68 companies should engage in partial cost sharing through coinsurance only, and 122 companies should utilize the maximum amount of cost sharing available through coinsurance and deductible. The line graph shows the average dollar amount of direct security investment recommended for each type of insurance policy measured on the secondary axis. Using non-parametric analysis, the Wilcoxon Each Pair test indicates that the direct security investment recommended as a percentage of company revenue was different by insurance policy option at α = 0.05. We provide The p-values in Figure 3.

Nonparametric Comparisons For Each Pair Using Wilcoxon Method

q*	Alpha
1.95996	0.05

Score Mean				Hodges-					
Level	-Level	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 3. Recommended security investment as a percentage of revenue statistical analysis.

Contributing Factors

In Figure 4 and Figure 5, the bar graphs depict the expected losses prior to treatment and after the data was treated in the model. ANOVA and Tukey-Kramer tests showed that both pre-treatment and post-treatment losses were statistically different at α = 0.05 with p-values < 0.0001. The probability of attack success, depicted by the line graph and measured on the secondary axis, shows that the increased security investment shown in Figure 2 results in lower probabilities of attack success, as depicted in Figure 4 and Figure 5. Non-parametric analysis confirmed differences between companies recommended to engage in cost sharing and those not recommended to engage in cost sharing based on dollars invested in direct self-security at α = 0.05 with p-values < 0.0001. These figures provide evidence that the model could successfully recognize risk and assign companies to homogenous groups based on that risk.

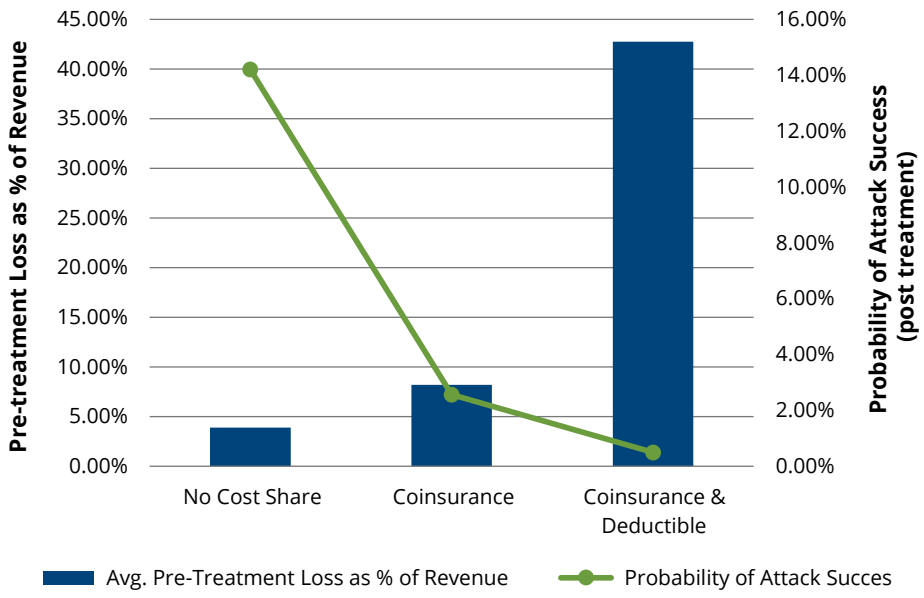

Figure 4. Average pre-treatment loss as a percentage of revenue and probability of attack success.

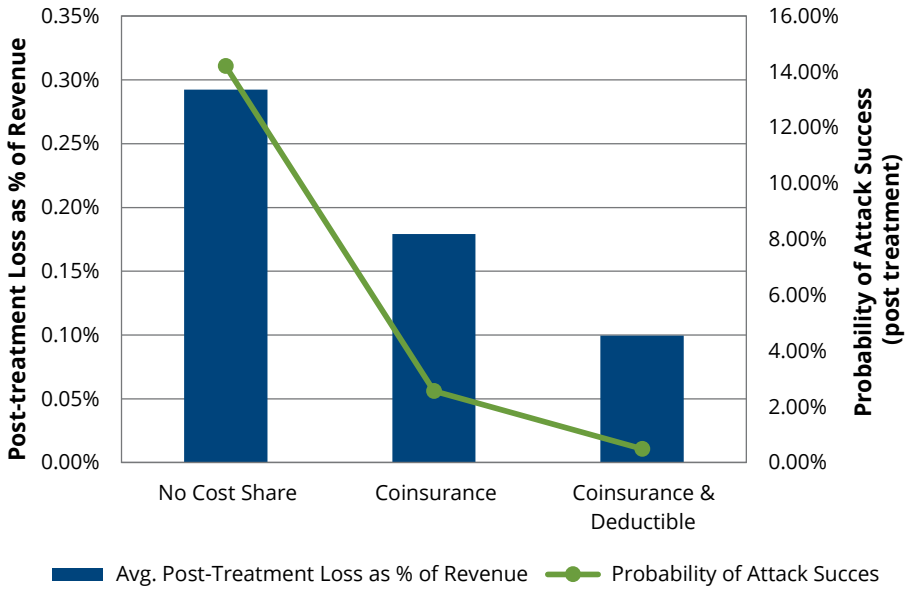

Figure 5. Average post-treatment loss as a percentage of revenue and probability of attack success.

Summary

The insurance policy recommendations prove that the model has the capability to discriminate between companies based on risk profiles at statistically significant levels. Companies with lower expected initial loss severities should not incur more risk by engaging in additional cost-sharing practices. Those with relatively higher expected initial loss severities were

recommended to engage in cost sharing of some type. Through cost sharing, companies would incur more financial responsibility in a loss event, which provided incentive to invest in risk mitigation to reduce expected losses. [29] The model's effectiveness in providing recommendations based on risk profiles provides value by eliminating a one-size-fits-all approach to insurance policy structure, which will better meet the needs of both the insured and insurer and should increase participation in the market.

Industry Impact

The authors conducted further analysis to explore the effectiveness of the extended framework and its scalability to the power enterprise. An ANOVA of the power industry's risk profile across NERC regions after the application of the model showed that at $\alpha = 0.05$, one region's risk profile was statistically different from the rest with a p-value < 0.0001. We provide a comparison of the ANOVA and connecting letters reports from the pre-treatment and post-treatment data in Figure 6, showing definitively that the Florida Reliability Coordinating Council (FRCC) is different from the rest of the NERC regions in the post-treatment condition.

Welch's Test

Welch Anova Testing Means Equal, allowing Std Devs Not Equal

F Radio	DFNum	DFDen	Prob > F
2.8003	7	99.276	0.0106*

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.

Welch's Test

Welch Anova Testing Means Equal, allowing Std Devs Not Equal

F Radio	DFNum	DFDen	Prob > F
5.7019	7	99.268	<0.0001*

Connecting Letters Report

Level			Mean
SPP	A		-6.410425
WECC	A		-6.458210
MRO	A		-6.479048
NPCC	A		-6.539469
TRE	A		-6.642833
RFC	A		-6.685296
SERC	A	B	-6.854499
FRCC		B	-7.311601

Levels not connected by same letter are significantly different.

Figure 6. Comparison of risk profiles by region in pre-treatment (left) and post-treatment (right) conditions.

The post-treatment results indicating that one region is statistically different from the other provided evidence that this extended framework is scalable to the recognition of risk across the enterprise, meaning it can differentiate effectively between the risk postures of different regions. To determine whether the model actually reduced risk, we compared the standard deviations of loss to revenue ratio between pre-treatment and post-treatment conditions. Figure 7 shows the differences in the standard deviations in each condition across all years.

Both the tabular and graphical representations show that the losses faced by companies within regions were less volatile in the post-treatment condition.

NERC Region	Standard Deviation	
	Pre-treatment	Post-treatment
FRCC	0.969938	0.657601
MRO	0.972431	0.667458
NPCC	1.614795	0.64484
RFC	1.278549	0.688121
SERC	1.051699	0.539059
SPP	1.114973	0.726779
TRE	1.011735	0.51641
WECC	1.199969	0.78742

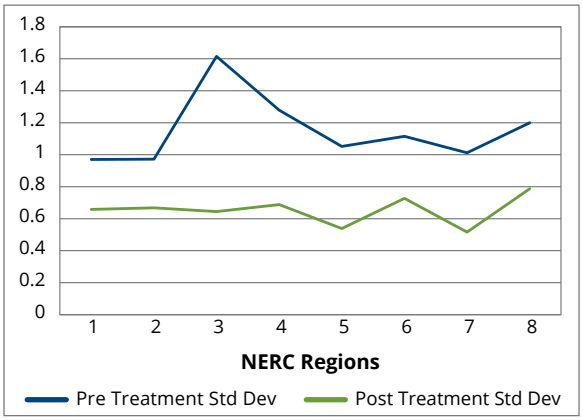

Figure 7. Standard deviation of loss to revenue ratio in pre-treatment and post-treatment conditions.

We used ANOVA of the log-transformed standard deviation data to confirm the reduction of risk across the power industry. The results showed that at $\alpha = 0.05$, both the pre-treatment and post-treatment groups were different, each with a p-value < 0.0001. However, outliers did challenge the assumptions of normality and equal variance when all years were analyzed together. The authors conducted further analysis of the pre-treatment and post-treatment conditions within years to confirm that the standard deviations were different by eliminating the possibility that any single year contributed to the measured differences across all years.

Comparing the means of the standard deviations within years at $\alpha = 0.05$ showed that there were differences between pre-treatment and post-treatment conditions. Each year's comparison resulted in a p-value < 0.0001. All years met the assumptions of normality and equal variance. Consideration of why the entire sample failed normality and homoscedasticity assumptions attributes extreme events such as super storms, polar vortices, hurricanes, droughts, et cetera to some years and not others. These types of events, measured as Major Event Days (MED), and included in the data, would have had an impact on the data collected during a given year. The fact that the assumptions are met when comparing the standard deviations within years provides support for this speculation.

The scalability of this model to the power industry writ large is represented by the reduction in the standard deviation of the risks faced within each region. By reducing the average standard deviation in each of the regions, the enterprise finds itself on firmer footing from a security perspective as the baseline security profile of each company is strengthened. A tighter range of risks faced by individual companies could lead to improved protection from cascading effects resulting from the compromise of a single system.

Conclusions and Implications

Prior to interpreting the results of the data and considering the implications for its effect on the power enterprise, the disclaimer must be made that in critical infrastructure, no amount of security investment can eliminate completely the risk presented by cyber threats

and vulnerabilities. Security in any arena can only hope to reduce probability of a loss and the size of a loss through effective risk management. Reality dictates that as soon as an effective deterrent is created, malicious actors will figure out how to circumvent these security measures. This research proposes a method for reducing risks across industry by incentivizing investment through insurance at individual companies. There can be no single sweeping reform that fixes the security issues of any industry; this is especially true with cyber security. But better risk management at individual companies implemented in an incremental fashion will create a stronger security posture across the industry in the long term.

Benefits to Individual Power Companies

The benefits of this model from the perspective of individual power companies can be quantified through multiple lenses. If this model is adopted across the cyber-insurance industry, insurance companies will become a partner in reducing cyber risk. From the standpoint of cyber-security budgets, the model has the capability to recommend an optimal budget and allocation strategy between risk reduction and risk transfer. The incentive measures of coinsurance and deductibles embedded within the insurance policy will reward those companies who have shown a track record of successful cyber-risk management and aid companies with less than stellar records. This will be achieved by using a combination of cost sharing and security investment to make coverage affordable. In the presence of constrained budgets, preliminary analysis indicates that recommendations would change in order to obtain a desired level of coverage within prescribed limits. Further analysis of constrained budgets and trade space options was not within the scope of this research and should be explored further in the future.

The partnership between the insured and insurer will open the door to minimum requirements imposed by insurers serving as de facto industry regulations. These regulations will take the form of "best practices." Furthermore, the analysis driven by the assessment could identify the most efficient avenues of investment in cyber security. That is, the insurance company, applying its knowledge gained through the broader market's participation could identify the most efficient cyber-investment options for individual companies, which will ultimately translate to the industry.

Individual power companies stand to gain greatly through the effective implementation of this model from the perspective of affordability, risk reduction, partnerships, and securing a risk transfer agent in the event of a low-probability, high-loss event.

Benefits to the Insurance Industry

The framework proposed in this research provides the capability to fill a gap in the insurance industry. As critical infrastructure companies struggle to find policies that meet their needs and to meet eligibility requirements for obtaining currently-available policies, this model will aid the pairing of the right insurer to the insured. The framework provides the ability for insurance companies to recognize risks more effectively and recommend the best methods of reducing those risks. If necessary, insureds will assume more of the financial burden of

a loss event, leading to increased self-investment to reduce risk, which could increase the profits of the insurance industry.

This model also paves the way for significantly more data collection that will allow for better analysis and the development of better cyber-security practices. As more companies in the power industry adopt insurance, information availability and the development of better policy practices will follow, allowing for further reduction of risk.

Impact on Power Industry and Critical Infrastructure

The cycle of adoption of effective cyber insurance in critical infrastructure has the potential to lead not only to a more secure power industry, but also to improve cyber security across all industrial- control-system regulated sectors of critical infrastructure. This framework's risk assessment capability will aid power companies in finding the right mix of risk transfer and risk mitigation strategies. As these methods are adopted, the insurance market will respond by reducing premiums and making cyber insurance more affordable, which will invite more market participation. As premiums continue to fall, a larger risk pool, better data, and the buildup of a broader information base should result in a normalization of risk into a less variable environment. This further reduces risk, potentially, by preventing catastrophic failure of one system from impacting other interconnected systems.

National Security Implications

As the insurance industry builds a library of cyber-security and cyber-incident data, the capabilities of a private/public partnership, such as the data repository envisioned by the CIDAWG, will be significantly enhanced. An increase in monitoring of individual power companies by insurance companies will lead to more effective reporting of cyber-security incidents. Widespread information sharing would occur within the cyber-security industry at large that could have positive returns by focusing on high-risk areas, confounding emerging threats, detecting patterns of intrusion, or even developing forecasting capabilities. All of this will lead to a better security baseline for use across the public and private cyber domains.

Future Research

The avenues of research most relevant to this cyber-security framework involve gaining more fidelity of cyber risks facing critical infrastructure. This framework substituted actual power-performance metrics for vulnerability and threat parameters used to assess losses. Continued research focused on identifying vulnerabilities and threats specific to the power industry could have a major impact on the application of this model in the real world, making it more effective and paving the way for a continuously improving critical infrastructure risk profile. The ability of this framework to be tailored to any specific company is only as strong as the assessment methods available in estimating vulnerabilities and threats.

About the Authors

U.S. Air Force Captain John Rosson is currently working as a cost estimator at the Air Force Cost Analysis Agency, Joint Base Andrews, MD. His experience as a Financial Management Officer in the Air Force includes serving as a budget analyst, financial services officer, and cost estimator. He earned his BS in Finance at St. John's University in 2008 and his MS in Cost Estimating from the Air Force Institute of Technology in 2017. He may be reached at jackrosson@gmail.com.

Dr. Mason Rice earned his BS in Electrical Engineering with Honors from the Florida Institute of Technology and was commissioned as a Second Lieutenant in the U.S. Army through ROTC in July 1995. During his time in the Army, he earned a MS in Electrical and Computer Engineering from the University of Florida, a PhD in Computer Science from the University of Tulsa, and certification as a Certified Information Systems Security Professional (CISSP). He holds a patent and has published over 30 scientific papers in professional journals and books. Mason is honored to be included in the U.S. Army ROTC Hall of Fame. Following retirement from the Army in 2017, he accepted a position with Oak Ridge National Laboratory as the Cyber-Physical R&D Manager. He may be reached at ricemj@ornl.gov.

Dr. Juan Lopez Jr., USMC (ret) is a cyber-physical R&D program manager at Oak Ridge National Laboratory located in Oak Ridge, TN. He leads research in Critical Infrastructure Protection, Supervisory Control and Data Acquisition (SCADA) systems, and Electromagnetic Interference (EMI) modeling. He served as the technical lead in SCADA/ICS research at the Air Force Cyberspace Technical Center of Excellence located at the Air Force Institute of Technology at Wright-Patterson AFB, OH. Dr. Lopez earned a PhD in Computer Science at the Air Force Institute of Technology, a BS from the University of Maryland, a MS from Capitol College, and a MS from the Air Force Institute of Technology under the NSA's Information Assurance Scholarship Program. Dr. Lopez is an IEEE Senior Member, Co-Chair for the Industrial Society of Automation's Work Group 4, Task Group 7 (Security of ICS Sensors), Certified Information Systems Security Professional (CISSP), Certified SCADA Security Architect (CSSA), and Certified Scrum Master. He may be reached at lopezj@ornl.gov.

R. David Fass, PhD is an Assistant Professor in the Department of Systems Engineering and Management at the Air Force Institute of Technology (AFIT). He received his BA in Economics, his MBA from the University of New Mexico, and his PhD in Business Administration & Management from New Mexico State University. His research interests include cost analysis, decision analysis, risk analysis, operations research, behavioral economics, organizational behavior, organizational change, and government acquisition policy. He may be reached at Robert.Fass@afit.edu.

Notes

1 Stamatis Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-physical System Security," in IECON Proceedings – 37th Annual Conference on IEEE Industrial Electronics Society, 2011, pp. 4490–4494, doi: 10.1109/IECON.2011.6120048; R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Washington, DC, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

2 Department of Homeland Security, "Fiscal Years 2014-2018 Strategic Plan," Washington, DC, 2014, https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

3 Department of Energy, "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," 2010, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

4 Derek Harp and Bengt Gregory-Brown, "The State of Security in Control Systems Today," Bethesda, MD, 2015, https://pdfs.semanticscholar.org/4ab7/f69cbf6c8bf72b7d2d24e880cb5fabbf5b50.pdf.

5 Oxana Andreeva et al., "Industrial Control Systems Vulnerabilities Statistics," Woburn, MA, 2016; ICS-CERT, "Environmental Systems Corporation Data Controllers Vulnerabilities (Update B)," 2016.

6 National Protection and Programs Directorate, "Insurance Industry Working Session Readout Report," Washington, DC, 2014, https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf.

7 Ibid.

8 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, https://www.dhs.gov/sites/default/files/publications/Overcoming%20Perceived%20Obstacles%20White%20Paper_1.pdf; 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, https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf; 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, https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf.

9 Chris Currie, "Critical Infrasturcture Protection," Washington, DC, 2016, https://www.gao.gov/assets/690/682547.pdf.

10 Ibid.

11 Department of Homeland Security, "Fiscal Years 2014-2018 Strategic Plan," Washington, DC, 2014, https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

12 Issaac Ehrlich and Gary Becker, "Market Insurance, Self-Insurance, and Self-Protection," *Journal of Political Economy*, vol. 80, no. 4, pp. 623–648, 1972.

13 Shauhin Talesh, "Insurance and the Law," *International Encyclopedia Of Social and Behavioral Science* 11, no. Forthcoming, (2015), https://ssrn.com/abstract=2611762.

14 J. Kehne, "Hazardous Wastes Encouraging Safety Through Insurance- Based Incentives: Financial Responsibility for Hazardous Wastes," *Yale Law Journal* l 96, no. 2, (1986). 403–427; Omri Ben-Shahar and Kyle Logue, "Outsourcing Regulation: How Insurance Reduces Moral Hazard," (2012)593, https://repository.law.umich.edu/mlr/vol111/iss2/2.

15 D. Young et al., "A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies," *International Journal of Critical Infrastructure Protection*, Apr. 2016.

16 Ibid.

17 L. A. Gordon and M. P. Loeb, "The Economics Of Information Security Investment," *Transactions on Information and System Security*, Vol. 5, no. 4, pp. 438–457, 2002.

18 D. Young, et al. , "A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies," *International Journal of Critical Infrastructure Protection*, Apr. 2016.

19 Karl Borch, Aase Sandmo, and Knut Aase, *Economics of Insurance*, Elsevier Science, 2014.

20 Intel Security and The Aspen Institute, "Critical Infrastructure Readiness Report: Holding the Line Against Cyberthreats," Washington, DC and Santa Clara, CA, 2015, https://www.thehaguesecuritydelta.com/media/com_hsd/report/43/document/Critical-Infrastructure-Readiness-Report---Holding-the-Line-against-Cyberthreats.pdf.

21 Ibid.

22 Electricity Data Experts, "Form EIA-861," Electric Power Sales, Revenue, and Energy Efficiency Form EIA-861 detailed data files, 2016, https://www.eia.gov/electricity/data/eia861/.

23 Michael Sullivan, Josh Schellenberg, and Marshall Blundell, "Updated Value of Service Reliability Estimates for Electric Utility Customers in the United States," Berkeley, CA, 2015, https://emp.lbl.gov/sites/all/files/lbnl-6941e.pdf.

24 Rodney Robinson and John McDaniel, "IEEE Guide for Electric Power Distribution Reliability Indices," 2012, doi: 10.1109/IEEESTD.2012.6209381.

25 Ibid.

26 TechTarget, "How Company Size Relates to IT Spending," *CIO Magazine*, 2016, http://searchcio.techtarget.com/magazineContent/How-Company-Size-Relates-to-IT-Spending. [Accessed: 02-Dec-2016]; Optimal Networks, "How (and How Much) are Organizations Spending on IT?," 2016, http://www.optimalnetworks.com/how-and-how-much-it-spending/.

27 Barbara Filkins, "IT Security Spending Trends," 2016, Available: https://www.sans.org/reading-room/whitepapers/leadership/paper/36697.

28 "Regional Entities," https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx.

29 R. Bojanc and B. Jerman-Blazic, "An Economic Modeling Approach to Information Security Risk Management," *International Journal of Information Management* 28, no. 5, (2008): .413–422.